

**Executive Summary and Addendum**

**Report on Trusted Defense Systems**

**In Response To**

**National Defense Authorization Act, Section 254**



**22 December 2009**

**Prepared by**

**The Under Secretary of Defense for Acquisition, Technology, and Logistics**

**And**

**The Assistant Secretary of Defense for Networks and Information Integration/  
DoD Chief Information Officer**

*The body of this report is For Official Use Only. The Executive Summary and other front matter are Unclassified when separated from the body of the report.*

Executive Summary and Addendum: Approved for unlimited distribution.



## Executive Summary

---

*In accordance with Section 254 of Public Law 110-417, “Duncan Hunter National Defense Authorization Act for Fiscal Year 2009” (FY09 NDAA Section 254), the Department of Defense (DoD) completed three vulnerability assessments on selected covered acquisition programs, completed a study of techniques for verifying trust in integrated circuits (IC), validated and continued to implement the Department’s Strategy for Systems Assurance and Trustworthiness using the results from the assessments and study, and issued policy and conducted activities designed to assure trust in integrated circuits, software, and other electronic components. This report describes this work.*

### The Globalization Challenge

The Department relies heavily on customized and commercial off-the-shelf (COTS) computers, communications equipment, ICs, application software, and other information communications technology (ICT)<sup>1</sup> to stay on the cutting edge of technology development and fulfill mission-critical operations. With increasing frequency, the Department and its commercial supplier base rely on foreign companies to produce the most advanced technology solutions. Once dominated by domestic manufacturing, today’s ICT manufacturing is largely conducted outside the United States. Product development (from design through manufacturing, integration, and delivery) typically involves an array of developers and suppliers around the world, many of whom the end user does not know. Even companies headquartered in the United States conduct substantial research, manufacturing, and other services in other countries.

Although the globalization of the ICT sector has accelerated the pace of technological innovation, it has also raised national security concerns. Mission-critical functionality of the Department’s systems and networks extensively leverages commercial, globally interconnected, globally sourced ICT. Consequently, adversaries have more opportunities to corrupt technologies, introduce malicious code into the supply chain, and otherwise gain access to the Department’s military systems and networks. There is no way to return to a supplier base of “all-American” companies for the Department’s ICT. Although some programs to protect classified information use cleared facilities and cleared personnel when developing technology for sensitive government use, this approach is neither ideal nor financially feasible on a large scale for a majority of the purposes for which ICT is intended.

Recognizing the emerging risk, the Department initiated a series of studies concerning hardware and software assurance beginning in 2003 to advance the development of appropriate risk management solutions. The Department also initiated the Trusted Foundry Program in 2003,

---

<sup>1</sup>ICT includes, but is not limited to, information technology (IT) as defined in title 40, U.S. Code (U.S.C.), section 11101. This term reflects the convergence of IT and communications. ICT includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, mobile telephony, satellite communications and networks). ICT that is a critical component is defined as Critical Program Information (CPI) under DoD Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 16, 2008.

which resulted in immediate access to leading edge IC foundry technology at IBM, and more than 50 additional microchip-related services at 27 other trusted suppliers.

Today, the Department is implementing a Strategy for Systems Assurance and Trustworthiness that will enable program and system managers to conduct supply chain risk management (SCRM) throughout the system lifecycle. This strategy builds on past studies and programs to provide program and system managers with tools to manage risk in a manner commensurate with the criticality of, and threats to, the system. Implementation of this comprehensive strategy began in February 2009 with a series of pilot programs and the establishment of the DoD Supply Chain Risk Management Threat Analysis Center (DoD SCRM TAC) within the Defense Intelligence Agency (DIA).<sup>2</sup>

Activities conducted in response to FY09 NDAA Section 254 have validated the Department's approach to supply chain risk. They also have produced important data about the Department's vulnerabilities, as well as techniques for verifying the trust of semiconductors procured from commercial sources that will inform the Department's SCRM efforts in important ways. The following subsections summarize these activities.

### **(a) Vulnerability Assessments Required**

The Department conducted three vulnerability assessments regarding selected covered acquisition programs. These assessments included not only command and control (C2) systems, but also an intelligence, surveillance, and reconnaissance program of record (ISR POR). The technology supporting these systems comprises many non-military specific components, exposing the Department to the globalization of components manufacturers, and thereby creating supply chain risk. Although expanding the universe of cases would undoubtedly provide more data points for this report, such an approach would not likely change the validity of the findings. For each program, the Department analyzed the systems engineering practices, systems design, threats related to suppliers and supply end items, and program protection planning activities.

The assessments identified three high-level vulnerabilities:

- Systems engineering and program protection practices in design and development do not fully address supply chain threats associated with the expanded definition of critical program information (CPI).<sup>3</sup>

---

<sup>2</sup> Directive-Type Memorandum (DTM) 08-048, *Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems*, February 19, 2009.

<sup>3</sup> DoDI 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 16, 2008, defines CPI as: "Elements or components of [a research, development, and acquisition] program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability." DoDI 5200.39 further provides that this definition includes "information about applications, capabilities, processes, and end-items"; "elements or components critical to a military system or network mission effectiveness"; and "technology that would reduce the U.S. technological advantage if it came under foreign control."

- Current procurement practices limit control of vendor and subcontractor selection and significantly limit the level of supply chain visibility necessary to make strategic risk management decisions.

Although awareness is improving, program managers do not fully mitigate potential supply chain threats because supporting processes, supporting resources, and formal training have yet to be established.

Note that there are programs that—because of their unique criticality, special access protection, or proximity to intelligence community assets—do understand and take steps to manage supply chain risk. However, these activities are not similarly robust across the full scope of mission-critical programs within the Department.

A theme identified through these assessments was a trend toward developing and implementing final systems with Field Programmable Gate Array (FPGA) technology. Compelling cost, schedule, and design agility considerations are driving this trend. These systems, unlike prior generations that may have leveraged Application-Specific Integrated Circuits (ASIC) as a production strategy (because of ASIC's power, performance, and security characteristics), are now starting and staying with FPGAs. Consequently, the Department must preserve FPGAs as a viable technology while ensuring commensurate trustworthiness.

The Department confirmed the need for broad implementation of its Strategy for Systems Assurance and Trustworthiness to address supply chain vulnerabilities in mission-critical systems; it clarified strategic recommendations to improve the tools, discipline, and processes required to assess the criticality of system components and appropriately protect the supply chain of these components; and it identified technical recommendations to address the application of information assurance (IA) and network defense countermeasures. The Department will continue to refine the strategy based on lessons learned while piloting this strategy in FY09 and FY10, expanding the type and breadth of mission-critical systems assessed to ensure policies and processes are sufficiently broad based to be effective. In accordance with DoD policy, the Department will roll out its Strategy for Systems Assurance and Trustworthiness for all mission-critical systems over the Future Years Defense Program (FYDP). The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) will continue to jointly lead the implementation of the Department's integrated strategy for mitigating supply chain vulnerabilities.

## **(b) Assessment of Methods for Verifying the Trust of Semiconductors Procured From Commercial Sources**

The Department assessed methods for verifying the trustworthiness of semiconductors procured from commercial sources. The study identified several low-cost and readily available methods for managing many IC supply chain threats. A majority of these are supplier prequalification and past performance assessment programs. Such programs can mitigate, but will not eliminate, risk associated with counterfeit and tampered ICs.

The study also determined that hiding the end use can provide a degree of anonymity and therefore inhibit an adversaries' ability to target a defense system for malicious activity. However, this method also limits communication with the end-supplier base, may inhibit early

Executive Summary and Addendum: Approved for unlimited distribution.

detection of a component's performance issues, and can be short lived if the marketplace identifies the end user after a few purchases. Among the more promising techniques were technical measures for identifying and authenticating ICs. These measures, although not generally the lowest cost, would help prevent unauthorized ICs from entering the supply chain.

Comparison techniques (in which ICs are compared against designs or products of known pedigree) and destructive physical analyses can be costly and time prohibitive, which presents challenges for broad applicability. These sophisticated techniques are currently the subject of the Defense Advanced Research Projects Agency (DARPA) TRUST in IC program, the results of which may affect this equation. Currently, electrical testing is not sufficiently comprehensive to detect many types of subversion. In addition, it is generally cost prohibitive, and can degrade product reliability and service life. Visual inspection and low-cost testing techniques are suitable for addressing many counterfeit threats. However, they are less effective against more sophisticated forms of counterfeiting and cannot detect whether a circuit contains malicious code.

The findings confirm the need to consider expanding trusted supplier program services for custom chips, in which suppliers develop chips in an accredited, trustworthy environment (*e.g.*, Trusted Foundry Program), including other types of technologies. However, any analysis must balance the need for cutting edge technologies against the risk those technologies pose to the system and the availability of other mitigations to effectively address that risk. Additional research is needed regarding detection techniques. The Department is establishing a countering counterfeits effort to review counterfeit and trust issues associated with logistics and sustainment. Its work will include consideration of the forgoing issues, techniques, and assessments.

### (c) Strategy Required

The Department has developed a Strategy for Systems Assurance and Trustworthiness to achieve trusted mission-critical systems and networks. This strategy has been validated by DoD working groups led by the Office of the Secretary of Defense (OSD), Defense Science Board studies, and SCRM Initiative activities conducted under the Comprehensive National Cybersecurity Initiative (CNCI). The National Security Council Deputies Committee also has approved the strategy. The Department is taking steps to adjust the strategy in light of the results of the vulnerability assessments and verification study conducted under FY09 NDAA Section 254, and to institutionalize the strategy across the Department. Progressively over the FYDP, the Department will develop and implement the necessary policies, processes, guidance, and training in place to empower program managers to manage ICT supply chain risk whenever they acquire, integrate, or maintain high-priority systems. Core elements of the strategy are as follows:

- **Prioritize Scarce Resources Based on Mission Dependence**—Establish a repeatable analytical process for analyzing mission dependencies on systems; apply systems assurance.
- **Conduct Comprehensive Program Protection Planning for Mission-Critical Systems and Networks, to Achieve SCRM and Protect Defense-Critical Technologies**—Employ program protection planning to identify and protect CPI, including critical components within critical weapons systems and information networks; assess threats to CPI; and

mitigate risk using the full range of cost-effective best practices, including SCRM key practices and system security engineering.

- **Detect and Respond to Vulnerabilities in Programmable Logic Elements**—Invest in enhanced vulnerability detection research and development (*e.g.*, DARPA TRUST in ICs program, Center for Assured Software of the National Security Agency (NSA), and Air Force Application Software Assurance Center of Excellence (ASACoE)), and transition such analytical capabilities to support acquisition.

**Partner With Industry**—Collaborate with industry to protect the information environment supporting critical systems, use the Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Program, and address risks related to global sourcing through various channels, including United States Munitions List (USML) supplier management.

## (d) Policies and Actions for Assuring Trust in Integrated Circuits

DoD policies to assure trust in ICs, software, and other information technology are as follows:

- **DoD Directive (DoDD) 5230.25, *Withholding of Unclassified Technical Data From Public Disclosure, November 6, 1984***—The application of the DoDD is limited to only such technical data that disclose critical technology with military or space application. Critical technology consists of arrays of design and manufacturing know-how, including technical data.
- **Deputy Secretary of Defense Memorandum, *Defense Trusted Integrated Circuits Strategy (DTICS), October 10, 2003***—Establishes a strategy to ensure access to leading edge, trusted commercial suppliers and critical ICs for use in sensitive defense weapons, intelligence, and communication systems.
- **USD(AT&L) and ASD(NII)/DoD CIO Memorandum, *Interim Guidance on Trusted Suppliers for Application Specific Integrated Circuits (ASIC), January 27, 2004***—Requires that all custom-designed ICs for high mission assurance category (MAC) and confidential environments be obtained from an accredited trusted IC supplier.
- **DoD Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense, July 16, 2008***—Expands the definition of CPI to include “elements or components critical to a military system or network mission effectiveness” and requires that counterintelligence, intelligence, security, systems engineering, and other measures be used to protect CPI. Introduces supply chain risk management as a key facet of program protection.

**Directive-Type Memorandum (DTM) 08-048, *Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems, February 19, 2009***—Requires that supply chain risk be addressed across the entire system lifecycle and that a SCRM capability be instituted incrementally, beginning with pilot programs in FY09 and FY10; also reestablishes DTICS policy within the context of SCRM and program protection planning. Establishes SCRM as DoD policy.

DoD policy related to systems assurance and trustworthiness will be revised based on the vulnerability assessments and verification study and the pilot tests and will include the following:

- Department of Defense Manual (DoDM) 5200.39 will replace DoD 5200.1-M as the implementing guidance for program protection planning.
- DoDI 5240.11 will support implementation of key elements of DTM 08-048 and refine roles, responsibilities, and processes for assessing vendor threat and risk within the Department.

Best practices for trust, system security engineering, and SCRM, will be incorporated into these and other issuances, as appropriate.

### Summary and Way Ahead

The Department has been working to address program vulnerabilities in an evolving cyber environment and globalized economy for several years and will continue on this path. The vulnerability assessments and verification study required by Section 254 added impetus to the Department's activities and validated its strategy for addressing supply chain risk. The Department also identified strategic and implementation gaps that should be addressed.

The Department will continue building a Department-wide capability to achieve trusted mission-critical systems and networks that will include robust systems engineering, use of all-source threat information, rigorous program protection planning, SCRM, highly focused information systems security engineering (ISSE), and further expansion of the trusted IC supplier industrial base. The Department also will continue to pursue advanced verification and validation technologies that provide better insight into the pedigree of components acquired for DoD mission-critical systems and networks. Pilot activities will continue in FY10 and will inform a broadly based FY12 budget and planning to institutionalize the resources, processes, and policies for Systems Assurance and Trustworthiness in mission-critical systems, with full operating capability for all mission-critical systems over the FYDP.

The Department also will establish necessary working groups to address strategic and implementation gaps required for full rollout of the strategy. For example, the working groups involving the OUSD(AT&L), the OASD(NII)/DoD CIO, the Joint Staff, and DoD Components will collaborate to prioritize implementation of SCRM through an understanding of mission dependence on DoD systems and networks and standardize the process for conducting criticality analyses. In addition, the groups will help strengthen decision and oversight processes for managing risk associated with global sourcing of key components that support critical functionality in mission-critical systems and networks. Where appropriate, these efforts will be achieved through partnership with industry, including our contractors that develop our systems, our vendors that supply components, and industry leaders who design and develop leading information and communications technology.

## Table of Contents

<b>Executive Summary</b> .....	<b>i</b>
The Globalization Challenge .....	i
(a) Vulnerability Assessments Required.....	ii
(b) Assessment of Methods for Verifying the Trust of Semiconductors Procured From Commercial Sources .....	iii
(c) Strategy Required .....	iv
(d) Policies and Actions for Assuring Trust in Integrated Circuits .....	v
Summary and Way Ahead .....	vi
<b>Fiscal Year 2009 National Defense Authorization Act: Section 254 Trusted Defense     Systems</b> .....	<b>ix</b>
<b>1. Introduction</b> .....	<b>1</b>
1.1 The Globalization Challenge.....	1
1.2 Trust and Integrated Circuits.....	2
1.3 Strategy for Systems Assurance and Trustworthiness .....	2
<b>2. Vulnerability Assessments (Section 254 (a))</b> .....	<b>6</b>
2.1 Methodology .....	7
2.2 Findings of the Vulnerability Assessments .....	7
2.3 Other Vulnerabilities .....	10
2.3.1 IC Production Vulnerabilities .....	10
2.3.2 Counterfeiting Vulnerabilities .....	12
2.3.3 FPGA and Commercial Device Vulnerabilities.....	13
2.4 Prioritization of Vulnerabilities.....	14
2.5 Recommendations Under Consideration.....	14
2.6 Leadership .....	15
<b>3. Verification Study (Section 254 (b))</b> .....	<b>16</b>
3.1 Methodology .....	16
3.2 Identification of Verification Methods.....	17
3.3 Determination of Suitability of Verification Methods .....	17
3.4 Other Matters.....	17
3.5 Summary .....	18
<b>4. Strategy (Section 254 (c))</b> .....	<b>20</b>

Executive Summary and Addendum: Approved for unlimited distribution.

4.1	Core Strategic Elements .....	21
4.1.1	Prioritize Resources Based on Mission Dependence.....	21
4.1.2	Plan for Comprehensive Program Protection for Mission-Critical Systems and Networks to Achieve SCRM and to Protect Defense Critical Technologies.....	21
4.1.3	Detect and Respond to Vulnerabilities in Programmable Logic Elements.....	26
4.1.4	Partner With Industry.....	27
4.2	Enhancing the Strategy.....	28
<b>5.</b>	<b>Policies and Actions for Assuring Trust in Integrated Circuits (Section 254 (d)).....</b>	<b>30</b>
5.1	DoD Policies.....	30
5.1.1	DoD Directive (DoDD) 5230.25, Withholding of Unclassified Technical Data From Public Disclosure, November 6, 1984.....	30
5.1.2	Defense Trusted Integrated Circuits Memo, October 10, 2003 .....	31
5.1.3	Interim Guidance on Trusted Suppliers for Application-Specific Integrated Circuits, January 27, 2004 .....	31
5.1.4	DoD Instruction 5200.39, Critical Program Information Protection Within the Department of Defense, July 16, 2008.....	31
5.1.5	Directive-Type Memorandum 08-048, Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems, February 19, 2009.....	32
5.2	Addressing FY09 NDAA Section 254 Requirements .....	32
<b>6.</b>	<b>Way Ahead.....</b>	<b>35</b>
<b>Appendix A: Acronyms and Abbreviations .....</b>		<b>A-1</b>
<b>Appendix B: Vulnerability Assessments Methodology .....</b>		<b>B-1</b>
<b>Appendix C: Verification Study Methodology and Findings .....</b>		<b>C-1</b>
<b>Appendix D: Verification Study Industry Participants .....</b>		<b>D-1</b>
<b>Appendix E: Verification Study Identified Methods.....</b>		<b>E-1</b>
<b>Appendix F: Vulnerability Detection and Response Programs and Mechanisms.....</b>		<b>F-1</b>

# Fiscal Year 2009 National Defense Authorization Act: Section 254 Trusted Defense Systems

---

## **SEC. 254. TRUSTED DEFENSE SYSTEMS.**

(a) **VULNERABILITY ASSESSMENT REQUIRED.**—The Secretary of Defense shall conduct an assessment of selected covered acquisition programs to identify vulnerabilities in the supply chain of each program’s electronics and information processing systems that potentially compromise the level of trust in the systems. Such assessment shall—

- (1) identify vulnerabilities at multiple levels of the electronics and information processing systems of the selected programs, including microcircuits, software, and firmware;
- (2) prioritize the potential vulnerabilities and effects of the various elements and stages of the system supply chain to identify the most effective balance of investments to minimize the effects of compromise;
- (3) provide recommendations regarding ways of managing supply chain risk for covered acquisition programs; and
- (4) identify the appropriate lead person, and supporting elements, within the Department of Defense for the development of an integrated strategy for managing risk in the supply chain for covered acquisition programs.

(b) **ASSESSMENT OF METHODS FOR VERIFYING THE TRUST OF SEMICONDUCTORS PROCURED FROM COMMERCIAL SOURCES.**—The Under Secretary of Defense for Acquisition, Technology, and Logistics, in consultation with appropriate elements of the Department of Defense, the Intelligence Community, private industry, and academia, shall conduct an assessment of various methods of verifying the trust of semiconductors procured by the Department of Defense from commercial sources for use in mission-critical components of potentially vulnerable defense systems. The assessment shall include the following:

- (1) An identification of various methods of verifying the trust of semiconductors, including methods under development at the Defense Agencies, government laboratories, institutions of higher education, and in the private sector.
- (2) A determination of the methods identified under paragraph (1) that are most suitable for the Department of Defense.
- (3) An assessment of the additional research and technology development needed to develop methods of verifying the trust of semiconductors that meet the needs of the Department of Defense.
- (4) Any other matters that the Under Secretary considers appropriate.

(c) **STRATEGY REQUIRED.**—

(1) **IN GENERAL.**—The lead person identified under subsection (a)(4), in cooperation with the supporting elements also identified under such subsection, shall develop an integrated strategy—

- (A) for managing risk—
  - (i) in the supply chain of electronics and information processing systems for covered acquisition programs; and
  - (ii) in the procurement of semiconductors; and
- (B) that ensures dependable, continuous, long-term access and trust for all mission-critical semiconductors procured from both foreign and domestic sources.

(2) **REQUIREMENTS.**—At a minimum, the strategy shall—

- (A) address the vulnerabilities identified by the assessment under subsection (a);
- (B) reflect the priorities identified by such assessment;
- (C) provide guidance for the planning, programming, budgeting, and execution process in order to ensure that covered acquisition programs have the necessary resources to implement all appropriate elements of the strategy;

(D) promote the use of verification tools, as appropriate, for ensuring trust of commercially acquired systems;

(E) increase use of trusted foundry services, as appropriate; and

(F) ensure sufficient oversight in implementation of the plan.

(d) **POLICIES AND ACTIONS FOR ASSURING TRUST IN INTEGRATED CIRCUITS.**—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall—

(1) develop policy requiring that trust assurance be a high priority for covered acquisition programs in all phases of the electronic component supply chain and integrated circuit development and production process, including design and design tools, fabrication of the semiconductors, packaging, final assembly, and test;

(2) develop policy requiring that programs whose electronics and information systems are determined to be vital to operational readiness or mission effectiveness are to employ trusted foundry services to fabricate their custom designed integrated circuits, unless the Secretary specifically authorizes otherwise;

(3) incorporate the strategies and policies of the Department of Defense regarding development and use of trusted integrated circuits into all relevant Department directives and instructions related to the acquisition of integrated circuits and programs that use such circuits; and

(4) take actions to promote the use and development of tools that verify the trust in all phases of the integrated circuit development and production process of mission-critical parts acquired from non-trusted sources.

(e) **SUBMISSION TO CONGRESS.**—Not later than 12 months after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees—

(1) the assessments required by subsections (a) and (b);

(2) the strategy required by subsection (c); and

(3) a description of the policies developed and actions taken under subsection (d)

Table 1 lists requirements from FY09 NDAA Section 254 and associated report sections.

**Table 1. Requirements From FY09 NDAA Section 254 and Associated Report Sections**

Requirement	Report Section
<b>(a) Vulnerability Assessment Required. Such assessment shall—</b>	2. Vulnerability Assessments (p. 6)
(1) Identify vulnerabilities at multiple levels of the electronics and information processing systems of the selected programs, including microcircuits, software, and firmware	2.2 Findings of Vulnerability Assessments (p. 7)
(2) Prioritize the potential vulnerabilities and effects of the various elements and stages of the system supply chain to identify the most effective balance of investments to minimize the effects of compromise	2.4 Prioritization of Vulnerabilities (p. 14)
(3) Provide recommendations regarding ways of managing supply chain risk for covered acquisition programs	2.5 Recommendations Under Consideration (p. 14)
(4) Identify the appropriate lead person, and supporting elements, within the Department for the development of an integrated strategy for managing risk in the supply chain for covered acquisition programs	2.6 Leadership (p. 15)
<b>(b) Assessment of Methods for Verifying the Trust of Semiconductors Procured from Commercial Sources. The assessment shall include the following:</b>	3. Verification Study (p. 16)
(1) An identification of various methods of verifying the trust of semiconductors, including methods under development at the defense agencies, government laboratories, institutions of higher education, and in the private sector	3.1 Identification of Verification Methods (p. 16)
(2) A determination of the methods identified under paragraph (1) that are most suitable for DoD	3.2 Determination of Suitable Methods (p. 17)
(3) An assessment of the additional research and technology development needed to develop methods of verifying the trust of semiconductors that meet the needs of DoD	Appendix C: Verification Study Methodology and Findings (p. C-6)
(4) Any other matters that the USD(AT&L) considers appropriate	3.5 Other Matters (p. 17)
<b>(c) Strategy Required—</b>	4. Strategy (p. 20)
(1) In General. The lead person identified under subsection (a)(4), in cooperation with the supporting elements also identified under such subsection, shall develop an integrated strategy— (A) For managing risk (B) That ensures dependable, continuous, long-term access and trust for all mission-critical semiconductors procured from both foreign and domestic sources	(A) 4.1. Core Strategic Elements (p. 21)  (B) 4.1.2.2. Assess Threats and Vulnerabilities to CPI (p. 23) 4.1.2.3.1. Supplier Management (p. 24) 4.1.3. Detect and Respond to Vulnerabilities (p. 26) 4.2. Enhancing the Strategy (p. 28)

<p>(2) Requirements. At a minimum, the strategy shall—</p> <p>(A) Address the vulnerabilities identified by the assessment under subsection (a)</p> <p>(B) Reflect the priorities identified by such assessment</p> <p>(C) Provide guidance for the planning, programming, budgeting, and execution process to ensure that covered acquisition programs have the necessary resources to implement all appropriate elements of the strategy</p> <p>(D) Promote the use of verification tools, as appropriate, for ensuring trust of commercially acquired systems</p> <p>(E) Increase use of trusted foundry services, as appropriate</p> <p>(F) Ensure sufficient oversight in implementation of the plan</p>	<p>(A) 4. Strategy (page 20) 4.1 Core Strategic Elements (p. 21)</p> <p>(B) 4.1.1. Prioritize Resources (p. 21) 4.1.2.1. Identify CPI (p. 22)</p> <p>(C) 4.1.2.3.2 SCRM Key Practices (p. 24) 5.1.5.DTM 08-048 (p. 32)</p> <p>(D) 4.1.3 Detect and Respond to Vulnerabilities (p. 26) 4.2 Enhancing the Strategy (p. 28)</p> <p>(E) 4.2 Enhancing the Strategy (p. 28) 5.1.5.DTM 08-048 (p. 32)</p> <p>(F) 5.1.5.DTM 08-048 (p. 32)</p>
<p><b>(d) Policies and Actions for Assuring Trust in Integrated Circuits. Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall—</b></p>	<p>5. Policies and Actions for Assuring Trust in Integrated Circuits (p. 30)</p>
<p>(1) Develop policy requiring that trust assurance be a high priority for covered acquisition programs in all phases of the electronic component supply chain and integrated circuit development and production process, including design and design tools, fabrication of the semiconductors, packaging, final assembly, and test</p>	<p>5.2 Addressing FY09 NDAA Section 254 Requirements (p. 32)</p>
<p>(2) Develop policy requiring that programs whose electronics and information systems are determined to be vital to operational readiness or mission effectiveness are to employ trusted foundry services to fabricate their custom designed integrated circuits, unless the Secretary specifically authorizes otherwise</p>	<p>5.2 Addressing FY09 NDAA Section 254 Requirements (p. 32)</p>
<p>(3) Incorporate the strategies and policies of the Department of Defense regarding development and use of trusted integrated circuits into all relevant Department directives and instructions related to the acquisition of integrated circuits and programs that use such circuits</p>	<p>5.2 Addressing FY09 NDAA Section 254 Requirements (p. 32)</p>
<p>(4) Take actions to promote the use and development of tools that verify the trust in all phases of the integrated circuit development and production process of mission-critical parts acquired from non-trusted sources</p>	<p>5.2 Addressing FY09 NDAA Section 254 Requirements (p. 32)</p>

# Addendum to Report on Trusted Defense Systems, January 2010–November 2012

---

The Department of Defense (DoD) continues to implement the strategy described in its Report on Trusted Defense Systems, submitted to Congress in January 2010. The four tenets remain in place:

1. Prioritize scarce resources based on mission dependence.
2. Conduct comprehensive program protection planning for mission-critical systems and networks, to achieve supply chain risk management (SCRM) and to protect defense-critical technologies.
3. Detect and respond to vulnerabilities in programmable logic elements.
4. Partner with industry.

DoD has strengthened its policy for trusted defense systems and has made significant progress implementing the policy since January 2010.

## Program Protection Planning – Mission-Critical Functions and Components

DoD continues to focus on securing mission-critical functions and components and critical program information (CPI)<sup>1</sup>. In addition to processes to identify CPI, DoD has developed a complementary process to identify and manage risk to critical components (which can be and often are commercial off-the-shelf elements) through Trusted Systems and Networks policy and program protection planning, described further below.

## Policy Updates

Since publishing the report, DoD has published and developed several policies for managing supply chain and system design risk in mission-critical systems:

- **DoD Instruction O-5240.24<sup>2</sup>, “Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA),”** provides for threat analysis to support SCRM and directs the integration of a technology-targeting risk assessment with appropriate analytical products to address foreign-collection threats to programs with CPI.
- **Committee on National Security Systems (CNSS) Directive 505<sup>3</sup>, “Supply Chain Risk Management (SCRM),”** requires U.S. Government departments and agencies to protect the confidentiality, integrity, and availability of national security systems from supply chain risks.
- **2011 National Defense Authorization Act (NDAA) Section 806, “Requirements for Information Relating to Supply Chain Risk,”** clarifies the Department’s authority to use intelligence within its procurement decisions while protecting the basis of its decision making from disclosure. The Defense Acquisition Regulation Council is implementing Section 806 through case number

---

<sup>1</sup> At the time of the writing of the Report, Critical Components were conceived as a variety of CPI. Since that time, DoD envisions critical components and CPI as unique types of DoD assets requiring protection.

<sup>2</sup> Available to authorized users at [http://www.dtic.mil/whs/directives/corres/pdf/O524024p\\_placeholder.pdf](http://www.dtic.mil/whs/directives/corres/pdf/O524024p_placeholder.pdf)

<sup>3</sup> Available to authorized users by request from the Committee on National Security Systems.

2012-D050, "Supply Chain Risk," and, when the regulatory changes are complete, the Department will pilot use of these new authorities within its trusted systems and networks processes.

- **DoD Instruction 5200.44<sup>4</sup>, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN),"** establishes policy to minimize the risk that DoD's warfighting mission capability will be impaired because of vulnerabilities in system design or because of sabotage or subversion of a system's mission-critical functions or critical components by foreign intelligence, terrorists, or other hostile elements.
- **Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics (AT&L) Memorandum, "Expected Business Practice: Document Streamlining – Program Protection Plan" (July 18, 2011)<sup>5</sup>,** requires every acquisition program to complete a Program Protection Plan (PPP) and provides an outline and guidance for the content of the plan. This outline and guidance includes planning requirements for software assurance, SCRM, trusted microelectronics, counterfeit avoidance, and other key aspects of the strategy.
- **Draft Program Protection Enclosure to DoD Instruction 5000.02, "Operation of the Defense Acquisition System,"** provides top-level program protection requirements to acquisition program managers and establishes a clear policy relationship between technology protection issuances (e.g., DoD Instruction 5200.39) and trusted defense systems issuances (e.g., DoD Instruction 5200.44). This enclosure is under review and will be coordinated with the next version of DoD Instruction 5000.02.
- The **Defense Acquisition Guidebook Chapter 13, Program Protection<sup>6</sup>** provides guidance regarding the program protection process as well as development, classification guidance, review/approval, management, and implementation of the PPP. It also provides expectations for major activities associated with program protection including CPI, mission critical functions and components, intelligence and counterintelligence (CI) support, vulnerability assessment, risk assessment, countermeasures, horizontal protection, foreign involvement, contracting, and detailed systems security engineering (SSE).

## Implementation Status

USD(AT&L) and the DoD Chief Information Officer (CIO) have partnered to support implementation of system security engineering and SCRM in more than 50 major defense acquisition programs. DoD continues to strengthen its partnership with the acquisition executive, chief information officer, and security elements in the Military Departments and has begun similar engagements with 9 defense agencies in the past year. In the coming months, DoD will be developing programming and budgeting guidance with these partners to ensure DoD achieves its full operating capability for trusted defense systems FY16.

---

<sup>4</sup> Available on the DoD Issuances Website: <http://www.dtic.mil/whs/directives/>

<sup>5</sup> Available on the Office of the Deputy Assistant Secretary of Defense for Systems Engineering Website: <http://www.acq.osd.mil/se/pg/index.html>

<sup>6</sup> Available on the Defense Acquisition Guidebook Website: <https://acc.dau.mil/dag13>  
Executive Summary and Addendum: Approved for unlimited distribution.