Report No. DODIG-2017-076

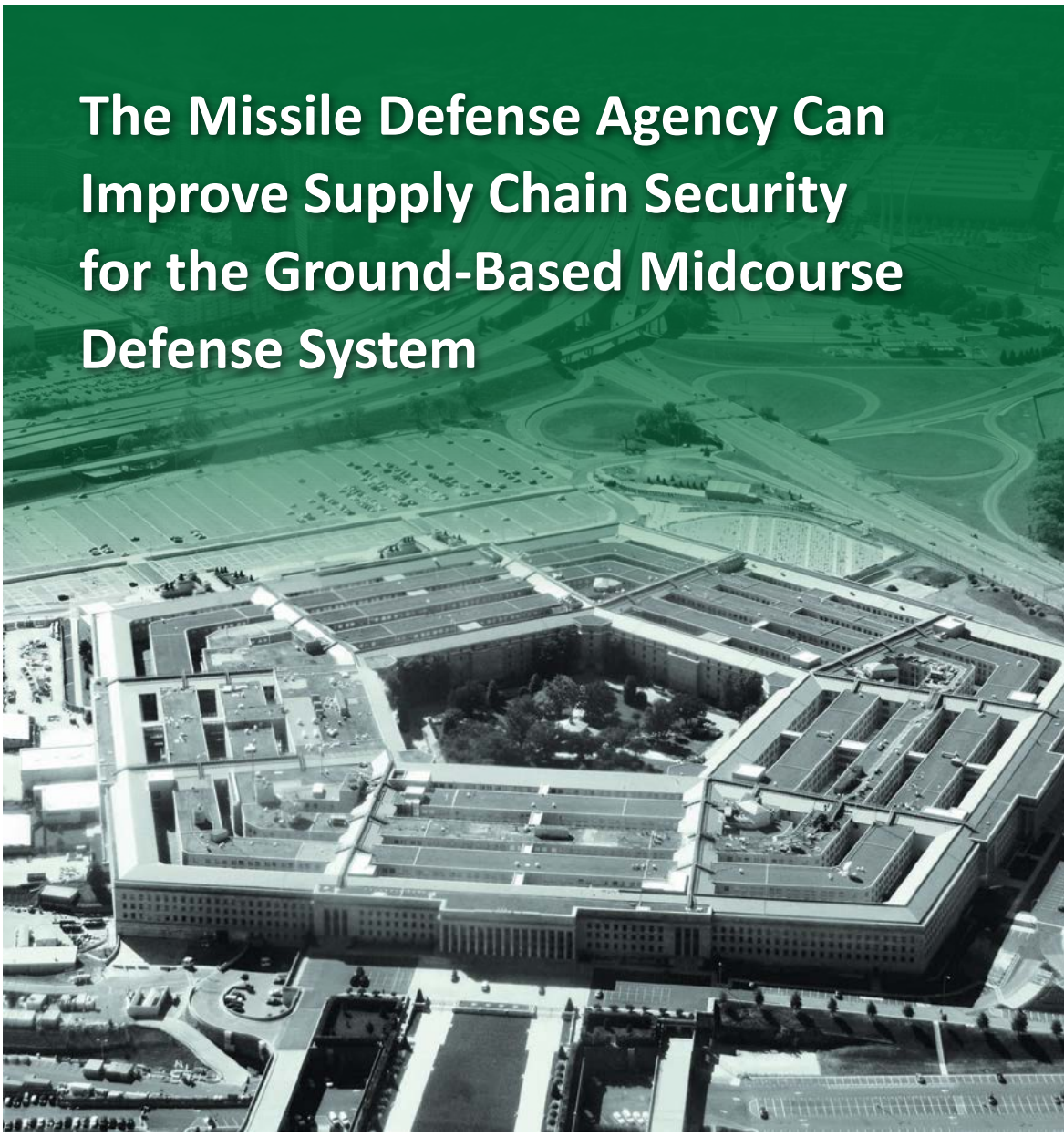
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

APRIL 27, 2017

The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System

April 27, 2017

Objective

We determined whether the Missile Defense Agency implemented an adequate supply chain risk management program for the Ballistic Missile Defense System. Specifically, we evaluated the supply chain risk management program for the Ground-based Midcourse Defense System. The Missile Defense Agency identified the Ground-based Midcourse Defense System as one of the most critical Ballistic Missile Defense System elements.

The Ground-based Midcourse Defense System uses multiple sensors, communications systems, fire control capabilities, and ground-based interceptors that are capable of detecting, tracking, and destroying intermediate and long-range ballistic missiles during the midcourse phase of flight.

We conducted this audit in response to a reporting requirement contained in House Report 114-537, to accompany the National Defense Authorization Act for Fiscal Year 2017.[1] This is the first in a series of audits on DoD strategic capabilities supply chain risk management.

The supply chain is the sequence of activities necessary to provide an end user with a finished product or system (from raw material to finished product). The activities include design, manufacturing, production, packaging, handling, storage, transportation, mission operation, maintenance, and disposal.

[1] See Appendix B for the reporting requirement in its entirety.

Objective (cont'd)

The Missile Defense Agency acquires critical information and communication technology components for the Ground-based Midcourse Defense System through its supply chain.

Supply chain risk is the vulnerability that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise compromise the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system. The adversary may take these actions to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system.

DoD supply chain risk management policy[2] requires Defense agencies to identify critical information and communications technology components, purchase those components from trusted suppliers, and test and evaluate critical components for malicious threats.

Finding

The Missile Defense Agency established several initiatives to manage supply chain risk for the Ground-based Midcourse Defense System and is piloting a DoD software assurance program to improve the supply chain security for its critical software. However, the Missile Defense Agency did not fully implement DoD supply chain risk management policy for the Ground-based Midcourse Defense System. This occurred because the Missile Defense Agency did not take the steps and establish the controls and oversight necessary to:

- (~~FOUO~~) maintain an accurate critical components list to manage risks to the Ground-based Midcourse Defense System throughout its life cycle and prioritize the list for supplier threat assessment requests for the [redacted] to vet critical component suppliers;
- identify the suppliers of all critical components for the Ground-based Midcourse Defense System; or

[2] DoD Instruction 5200.44 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 1, Effective August 25, 2016).

Results in Brief

The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System

Finding (cont'd)

- use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within critical components for the Ground-based Midcourse Defense System.

As a result, the Missile Defense Agency faces an increased risk that an adversary could infiltrate the supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the Ground-based Midcourse Defense System critical hardware, software, and firmware.

Recommendations

We recommend that the Director, Missile Defense Agency, develop a plan of action, with milestones, for the Ground-based Midcourse Defense program to comply with DoD Instruction 5200.44. The plan should establish controls and oversight of Ground-based Midcourse Defense System critical components and require Missile Defense Agency personnel to develop internal procedures or establish contract requirements to:

- improve the accuracy of the critical components list to manage risks to the Ground-based Midcourse Defense System and maintain an accurate and updated list throughout the system's life cycle;
- identify the suppliers of all critical components for the Ground-based Midcourse Defense System; and
- use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within critical components of the Ground-based Midcourse Defense System.

Management Comments and Our Response

The Director, Missile Defense Agency, agreed with the recommendations and stated that the Missile Defense Agency would evaluate the type of work being considered for the extension of the Ground-based Midcourse Defense System Development and Sustainment Contract, and determine if additional changes are required for the Tailored Parts, Materials, and Processes. The Director detailed additional steps that the Missile Defense Agency would take to improve supply chain risk management efforts for another Ground-based Midcourse Defense System contract.

However, the Director's comments did not describe how the Missile Defense Agency would improve the accuracy of the critical components list, improve the identification of suppliers of all critical components, and use rigorous test and evaluation capabilities to test for malicious threats and detect vulnerabilities within critical components. Therefore, the recommendations remain unresolved, and we request that the Director, Missile Defense Agency, provide details on addressing our specific recommendations by May 30, 2017. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, Missile Defense Agency	1.a.1, 1.a.2, 1.a.3, 1.b, 1.c.1, 1.c.2, 1.c.3	None	None

Please provide Management Comments by May 30, 2017.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

April 27, 2017

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
DIRECTOR, MISSILE DEFENSE AGENCY

SUBJECT: The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System (Report No. DODIG-2017-076)

We are providing this report for review and comment. The Missile Defense Agency established several initiatives to manage supply chain risk for the Ground-based Midcourse Defense System. However, the Missile Defense Agency did not fully implement DoD supply chain risk management policy, and the Missile Defense Agency faces an increased risk that an adversary could infiltrate the supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the Ground-based Midcourse Defense System critical hardware, software, and firmware. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. The Director, Missile Defense Agency, agreed with the recommendations, however, the Director's comments did not describe corrective actions the Missile Defense Agency will take to address the recommendations. Therefore, the recommendations remain unresolved, and we request additional comments on all the recommendations by May 30, 2017. The recommendations can be resolved by detailing the specific actions the Missile Defense Agency will take to implement the recommendations.

Please send a PDF file containing your comments to audcolu@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to Mr. Patrick Nix at (703) 604-9332 (DSN 664-9332).

Troy Meyer
Principal Assistant Inspector General
for Audit

Contents

Introduction

Objective

We determined whether the Missile Defense Agency (MDA) implemented an adequate supply chain risk management (SCRM) program for the Ballistic Missile Defense System (BMDS). Specifically, we evaluated the SCRM for the Ground-based Midcourse Defense (GMD) System.

We conducted this audit in response to a reporting requirement contained in House Report 114-537, to accompany the National Defense Authorization Act for Fiscal Year 2017. This is the first in a series of audits on SCRM for DoD strategic capabilities. See Appendix A for scope, methodology, and prior audit coverage. See the Glossary for specialized terms used throughout the report.

Background

The House Armed Services Committee's Request

The House Committee on Armed Services, Subcommittee on Strategic Forces, expressed concerns in House Report 114-537, stemming from a recent Government Accountability Office report,[3] that it appeared the DoD possessed "very little real data about the supply chain associated with certain critical systems." The committee was also concerned that the DoD "largely relies on assurances it receives from prime contractors, but oftentimes those prime contractors rely on subcontractors and others for information."

The committee directed the DoD Office of Inspector General (OIG) to "conduct an audit to evaluate supply chain security and assurance of one network or system deemed critical in each of the MDA, the Air Force Space Command, the nuclear command and control system, and a delivery system or platform for U.S. nuclear weapons."[4] Specifically, the committee directed the DoD OIG to report on the supply chain security and assurance evaluation of the networks or systems. The committee also identified specific matters that the DoD OIG should address. The matters included MDA's reliance on contractors, verification and validation of suppliers, identification of the name and nationality of software and firmware developers, and diligence over second- and third-tier suppliers.[5]

[3] Report No. GAO-16-236, "DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," February 2016.

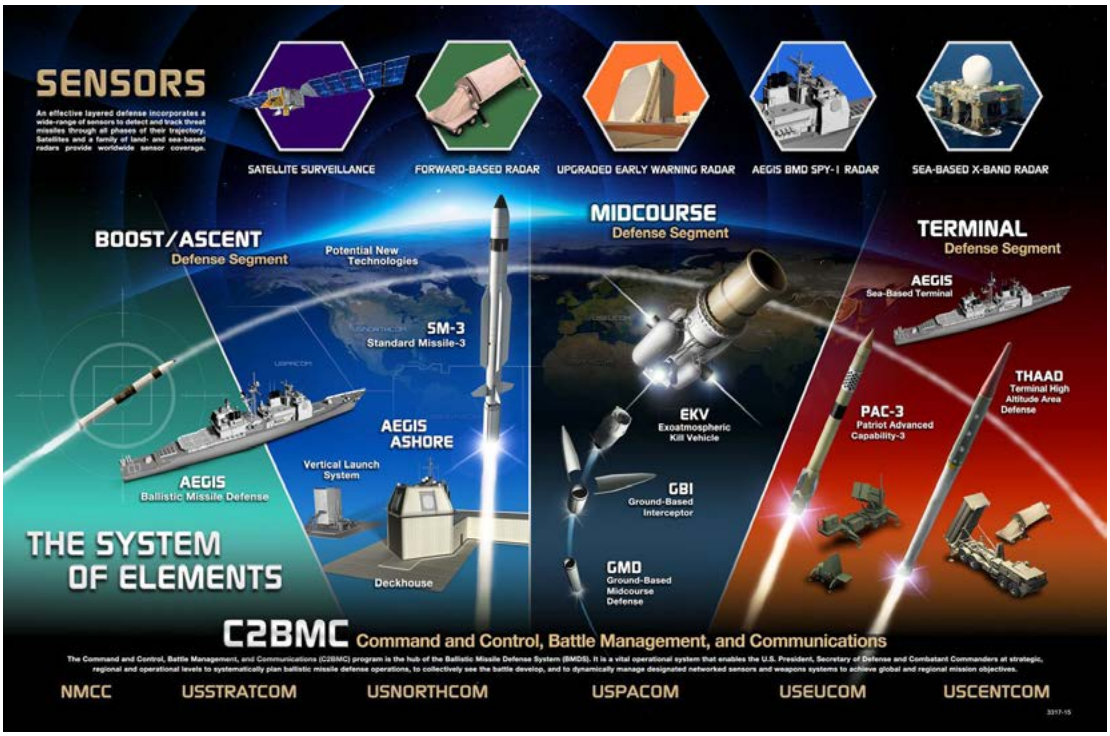
[4] Based on an agreement made with the subcommittee staffers, the audits would be done in a series, and the first audit would focus on the MDA.

[5] See Appendix B for the complete request, including the specific matters the committee asked to be addressed and our responses.

The Missile Defense Agency

The MDA is a research, development, and acquisition agency within the DoD, whose mission is to develop, test, and deploy a BMDS capable of defending the United States, its deployed forces, and allies against enemy ballistic missiles. The BMDS consists of multiple interoperable subsystems, with a mission to provide homeland and regional defense against ballistic missile threats of all ranges. The system follows the phased flight path of an incoming ballistic missile—boost/ascent (launch to atmosphere edge), midcourse (exoatmospheric), and terminal (atmosphere reentry to target). Figure 1 identifies the various BMDS components within the phased flight path.

Figure 1. BMDS Components



Source: MDA.

The MDA identified the GMD System as one of the most critical BMDS subsystems. The GMD System uses multiple sensors, communications systems, fire control capabilities, and ground-based interceptors that are capable of detecting, tracking, and destroying intermediate and long-range ballistic missiles during the midcourse phase of flight. The three major GMD components are:

- **Ground Systems** – systems that receive data from satellites and ground-based radar sources then use the data to support the intercept of ballistic missiles.

- **Exoatmospheric Kill Vehicle** – a sensor and propulsion package used to destroy an incoming ballistic missile target outside the earth's atmosphere.
- **Orbital Boost Vehicle** – A multi-staged, solid fuel booster used to launch and transport the exoatmospheric kill vehicle to its target.

The MDA awarded a 7-year Development and Sustainment Contract to a prime contractor in December 2011 to develop new capabilities and support the manufacture, testing, and operation of the GMD System (GMD contract). The prime contractor contracted with separate subcontractors for each of the three major GMD components.

DoD Supply Chain Risk and Risk Management Policy

DoD Instruction (DoDI) 5200.44 defines the DoD supply chain, supply chain risk, and risk management.[6] The DoD supply chain is the sequence of activities necessary to provide an end user with a finished product or system (from raw material to finished product). The activities include design, manufacturing, production, packaging, handling, storage, transportation, mission operation, maintenance, and disposal. The MDA acquires critical information and communication technology components for the GMD System through its supply chain.

DoDI 5200.44 defines supply chain risk as the vulnerability that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise compromise the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system. The adversary takes these actions to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system.

DoDI 5200.44 defines SCRM as a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain. SCRM involves developing mitigation strategies to combat those threats, whether presented by the supplier, the supplied product and its subcomponents, or the supply chain. SCRM is necessary throughout all phases of the supply chain, including initial production, packaging, handling, storage, transport, mission operation, and disposal.

[6] DoDI 5200.44 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 1, Effective August 25, 2016).

DoDI 5200.44 establishes DoD SCRM policy and assigns responsibilities to minimize the risk that the DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission-critical functions or critical components by foreign intelligence, terrorists, or other adversaries. DoDI 5200.44 requires DoD organizations to:

- Conduct a criticality analysis to identify mission-critical functions and critical components and reduce the vulnerability of these functions and components to system design or sabotage or subversion. It is DoD's policy that mission-critical functions and components are provided assurance consistent with their role within the system and with the criticality of the system.
- Document the results of the criticality analysis and associated planning and implementation activities in a program protection plan (PPP).
- (~~FOUO~~) Coordinate and prioritize requests for threat analysis of critical component suppliers from the [redacted][7] and use the [redacted] analysis as a basis for risk management decisions.
- Manage the risks to applicable systems throughout their entire life cycle from acquisition through sustainment. Risk management must include processes, tools, and techniques to:
    - Reduce vulnerabilities in the system design through system security engineering.
    - Control the quality, configuration, software patch management, and security of software, firmware,[8] hardware, and systems throughout their life cycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponents (for example, integrated circuits, field-programmable gate arrays, printed circuit boards) when they are identifiable to the supplier as having a DoD use.
    - Detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions.
    - Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats.

[7] Per DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011 (Incorporating Change 1, Effective October 15, 2013).

[8] Firmware is a software program or set of instructions programmed on a hardware device that provides the necessary instructions for how the device communicates with the other computer hardware.

- Purchase integrated circuit-related products from a trustworthy supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA)[9] when the products are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits).

Review of Internal Controls

DoDI 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[10] We identified an internal control weakness where the MDA did not fully implement DoD SCRM policy for the GMD System. We will provide a copy of the report to the senior official responsible for internal controls in the MDA.

[9] The DMEA was established and continuously evolved by the Office of the Secretary of Defense to jointly act as the DoD center for microelectronics technology, acquisition, transformation, and support.

[10] DoDI 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

Opportunities Exist for Improved GMD System SCRM

The MDA established several initiatives to manage supply chain risk for the GMD System and is piloting a DoD software assurance program to improve the supply chain security for its critical software. However, the MDA did not fully implement DoD SCRM policy for the GMD System. This occurred because the MDA did not take the steps and establish the controls and oversight necessary to:

- (~~FOUO~~) maintain an accurate critical components[11] list to manage risks to the GMD System throughout its life cycle and prioritize the list for supplier threat assessment requests to the [redacted]
- identify suppliers of all critical components for the GMD System; or
- use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within critical components for the GMD System.

As a result, the MDA faces an increased risk that an adversary could infiltrate the supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the GMD System critical hardware, software, and firmware.

MDA Established Initiatives to Manage Supply Chain Risks

The MDA established several initiatives to manage risks throughout the various tiers of the GMD supply chain. For the GMD System, the prime contractor would be the first tier, the subcontractor for a GMD component would be the second tier, and its purchases from the next level of suppliers would be the third tier, and so forth. The initiatives established included MDA Quality, Safety, and Mission Assurance (QS) Directorate initiatives, issuance of MDA policy on SCRM, piloting a DoD software assurance program, establishment of contract requirements, and completion of a criticality analysis.

[11] The term "critical components" refers to critical hardware, software, and firmware identified by a criticality analysis. These components generally consist of programmable and logic-bearing integrated circuit-related products.

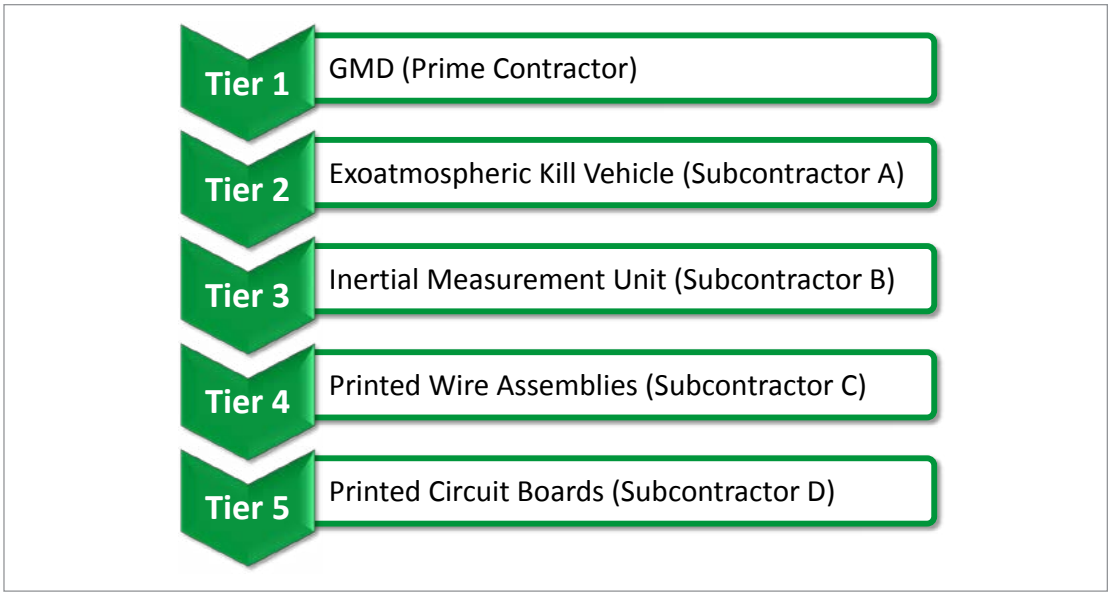
MDA's Quality, Safety, and Mission Assurance Directorate Provided Oversight

The MDA's QS Directorate is responsible for carrying out the agency's mission assurance strategy. The QS Directorate is a stand-alone organization that reports directly to the Director, MDA, on matters relating to quality, safety, and mission assurance. The QS Directorate maintained a supplier road map to track mission-critical suppliers, had mission assurance representatives who conducted engagements at contractor facilities, and conducted audits and technical assessments of BMDS contractors.

Supplier Road Map Identified Mission-Critical Suppliers

(~~FOUO~~) The supplier road map is a listing of suppliers of BMDS safety and mission critical components down to the fifth tier of the supply chain. The QS Directorate updates the supplier road map twice a year based on information obtained from the MDA program offices and contractors. The supplier road map contains basic information about the suppliers, including name and address, commercial and government entity code, the specific or type of critical component supplied, the supply chain tier, and the applicable BMDS program the supplier supports. The June 30, 2016, supplier road map identified [redacted] suppliers for the GMD System. QS Directorate officials informed us that there is an inherent risk that the supplier road map may be incomplete because contractors may be reluctant to provide information on all of their suppliers for competitive reasons. Figure 2 provides a portion of the supplier road map for selective exoatmospheric kill vehicle critical components down to the fifth tier.

Figure 2. Supplier Road Map for Exoatmospheric Kill Vehicle Critical Components



Source: MDA.

As a GMD contract deliverable, the prime contractor was responsible for providing the MDA with a mission-critical supplier list, which lists the major suppliers and their products identified as mission-critical to the effective and safe operation of the GMD System. The prime contractor's mission-critical supplier list identified:

- (~~FOUO~~) [redacted] subcontractors for ground systems,
- (~~FOUO~~) [redacted] subcontractors for the exoatmospheric kill vehicle, and
- (~~FOUO~~) [redacted] subcontractors for the orbital boost vehicle.

MDA Assurance Representatives Conducted Limited Scope Supplier Engagements

The QS Directorate established an MDA assurance representative regional plan to provide the agency insight into lower tier suppliers. The directorate maintains a permanent resident office within selective BMDS supply chain critical supplier facilities. In addition to covering their primary facilities, MDA assurance representatives evaluate other suppliers within the MDA supply chain. MDA assurance representatives perform limited-scope supplier engagements, designed to ensure implementation of MDA safety, quality, and mission assurance provisions. Although these engagements provide the MDA with insight into lower tier suppliers, QS Directorate personnel informed us that because of their limited scope, the engagements do not adequately assess compliance with the DoD SCRM requirements.

Audits and Technical Assessments Addressed Some SCRM Requirements

QS Directorate officials informed us that SCRM is only a small subset of the scope of the QS Directorate audits and assessments.

The QS Directorate conducts audits and technical assessments to determine the effectiveness of the BMDS developers and suppliers' quality, safety, and mission assurance systems. The audits and assessments determine the degree of compliance of the supplier to contractual requirements, internal requirements, or other approved documentation including industry or MDA best practices. The primary SCRM-related processes included in the scope of the QS Directorate audits and assessments involve counterfeit parts avoidance but not testing for malicious threats. However, QS Directorate officials informed us that SCRM is only a small subset of the scope of the QS Directorate audits and assessments.

MDA Issued Policy to Implement the DoD's SCRM Requirements

The MDA updated its Parts, Materials, and Processes Mission Assurance Plan (PMAP), and issued a policy memorandum[12] to address the minimum requirements for the MDA products and systems and to implement the DoD's SCRM policy.

PMAP Addressed Some SCRM Requirements

The MDA's PMAP defines parts, materials, and processes requirements for all new or modified safety and mission-critical products and systems developed for the MDA. The PMAP documents a coordinated approach to using part review boards at the program and agency levels to maintain the availability, high quality, and reliability of the MDA's products and systems. The PMAP requires suppliers to purchase parts from authorized sources or to appropriately test parts from unauthorized sources to mitigate the potential risks that counterfeit parts may infiltrate the BMDS. The MDA issued a revised PMAP (Revision B) in March 2012, which added the following related to SCRM.[13]

- The requirement that integrated circuit products be procured from a trusted supplier accredited by the DMEA when the integrated circuit products are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (paragraph 3.2.7).
- Enhanced procedures to minimize the risk of procuring or using counterfeit parts and materials for new, modified, and existing mission and safety critical hardware (paragraph 3.6.7).
- The requirement that supplier selection and surveillance methodology at a minimum include processes to verify critical function components received from suppliers to ensure that components are free from malicious code (seals, inspection, secure shipping, testing) in accordance with "National Security Agency Guidance for Addressing Malicious Code Risk," dated September 10, 2006 (paragraph 3.7.1).
- The requirement that commercial off-the-shelf (COTS) information assurance products (routers, switches, servers, communication equipment) used in MDA hardware for entering, processing, storing, displaying, or transmitting national security information be limited only to those that have been evaluated and validated jointly by the MDA program office and the National Security Agency in accordance with specified criteria,

[12] MDA Policy Memorandum No. 70, "Supply Chain Risk Management," April 10, 2014 (certified current October 20, 2015).
[13] MDA "Parts, Materials, and Processes Mission Assurance Plan," Revision B, March 2, 2012.

schemes, or programs. In addition, validation of COTS information assurance products will be conducted by accredited commercial laboratories, or the National Institute of Standards and Technology (paragraph 3.10).

MDA Issued a Policy Memorandum on SCRM

The MDA issued Policy Memorandum No. 70 in April 2014. The memorandum tasked the MDA Director of Technical Intelligence to lead SCRM implementation, coordination, and monitoring through a chartered MDA SCRM/Trusted System and Networks Integration Council (MSTIC). The MSTIC was to meet at least twice yearly, and the MDA Director of Engineering was to report twice yearly to the Director, MDA, on the progress of the MDA SCRM initiatives and compliance.

The memorandum required all BMDS program managers and program directors to coordinate efforts with the MDA Technical Intelligence Directorate and to identify critical components that support the significant functions of their respective BMDS components. The memorandum also required the program managers and program directors to document the results of their criticality analysis in a PPP in accordance with DoD SCRM requirements. According to its charter, the MSTIC was responsible for overseeing the MDA's SCRM implementation and reviewing and approving all critical components lists derived from program-level criticality analyses.

The policy memorandum also required the QS Director to coordinate with the MDA Director of Technical Intelligence to audit the compliance of vendors and sub-tier vendors for all logic-bearing components (a component with embedded logic; for example, a program) identified through SCRM criticality analysis.

MDA is Piloting a DoD Software Assurance Program

The MDA is piloting a DoD software assurance program focused on risks to the MDA BMDS organic software. According to MDA Acquisition Security personnel, organic software is software written by or for the MDA for the GMD System. The MDA personnel stated that they also refer to it as tactical software, which is the software that makes the GMD function and launches the interceptor to the target. The goal of the pilot program is to make software assurance a part of the MDA's normal acquisition process. The pilot program consists of three phases and is structured to develop, update, and execute MDA software assurance policy. The first phase began in August 2016, and as part of the pilot program the MDA plans to:

- conduct software assurance assessments,
- develop a risk assessment process,
- develop and collect metrics,

- conduct policy gap analysis,
- update MDA software assurance policy, and
- develop threat models and training.

At the completion of the pilot program, the MDA intends to issue a final policy memorandum for implementation. As part of the first phase of the pilot program, the GMD tactical software for ground systems was scanned for threats as part of the Joint Federated Assurance Center's[14] concept of operations exercise. The MDA's software assurance officials for the GMD System informed us in March 2017 that they were still awaiting the final report of the results of the software scans. The MDA software assurance pilot program is scheduled for completion in the third quarter of FY 2018.

MDA Established Limited Contractual Requirements for SCRM

The MDA used the PMAP to establish the technical baseline requirements for its systems. The original GMD contract, awarded in December 2011, referenced the PMAP (Revision A).[15] While the MDA issued a contract modification after the PMAP (Revision B) became effective in January 2016, the MDA applied only some of the SCRM requirements to the GMD contract.

Specifically, the MDA incorporated two specific SCRM sections from the PMAP (Revision B) into the GMD contract's Parts, Materials, and Processes Control Plan, which the MDA approved in January 2016.[16] The SCRM-related sections added to the control plan include the section from the PMAP (Revision B) on enhanced counterfeit parts avoidance and most of the section on supplier selection and surveillance.

MDA Performed Criticality Analysis on the GMD System

The MDA performed a criticality analysis that identified the GMD System's mission-critical functions and the key components whose failure would result in mission failure. The DoD SCRM guidance requires DoD organizations to prepare a PPP and to document the identification of mission-critical functions and critical components.

[14] A federation of DoD organizations established to ensure the security of DoD software and hardware. The federation was established in response to a congressional mandate in the National Defense Authorization Act for Fiscal Year 2014.

[15] MDA "Parts, Materials, and Processes Mission Assurance Plan," Revision A, March 26, 2008.

[16] A GMD contract deliverable that defines requirements for all new or modified GMD safety and mission-critical products.

The GMD Program Protection Plan

The DoD provided detailed guidance on preparing a PPP.[17] Program protection is the integrated process for managing risks to advanced technology and mission-critical functionality from foreign collection, design vulnerability, and supply insertion. The purpose of the PPP is to help programs ensure that they adequately protect their technology, components, and information. The process of preparing the PPP is intended to help program offices think through what needs to be protected and to develop a plan to provide that protection. The DoD guidance specified minimum information for inclusion in the PPP.

- Critical program information and critical function or component identification and updates
- Identification of threats, vulnerabilities, and countermeasures
- System security-related plans and documents
- Program protection risks
- Foreign involvement
- Processes for management and implementation of the plan
- Processes for monitoring and reporting compromises

To comply with the DoD guidance, the MDA documented the results of its criticality analysis for the GMD System in a PPP and included a critical components list as an appendix.

The GMD Critical Components List

The DoD PPP guidance identifies a specific methodology for DoD organizations to use to identify critical program information and mission-critical functions and components. The guidance describes the process for identifying critical components and specifies that the criticality analysis should be updated regularly and should be tied to system engineering technical reviews. The DoD PPP guidance requires identification of the missions, critical functions, supporting logic-bearing components, and system impact. Criticality is assessed in terms of relative impact on the system's ability to complete its mission if the critical component fails. Table 1 identifies the criticality levels used to identify the system impact resulting from failure of the critical component.

[17] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Program Protection Plan Outline and Guidance," July 18, 2011, and Defense Acquisition Guide, Chapter 13 "Program Protection," May 15, 2013.

Table 1. DoD Criticality Levels for Critical Components and System Impact

Criticality Level	System Impact
Level I	Total Mission Failure
Level II	Significant/Unacceptable Degradation
Level III	Partial/Acceptable
Level IV	Negligible

Source: Defense Acquisition Guidebook, Chapter 13 "Program Protection," May 15, 2013.

The next step in the criticality analysis involves prioritization of the level I and II critical components for resources and attention. Each critical component should be assigned an overall priority level of high, medium, or low based on a variety of factors, including the number of missions supported and whether the component is:

- a COTS or developmental item;
- a new or legacy item;
- an integrated circuit and, if so, the type (for example, an application-specific integrated circuit); or
- specifically designed for military use.

In March 2015, the MDA tasked the GMD prime contractor through a contract modification to perform a criticality analysis and to identify the GMD critical components.[18] The MDA's tasking required the prime contractor to perform a criticality analysis in accordance with the Defense Acquisition Guidebook, Chapter 13. The instruction specified that MDA provided the contractor with a template to use for conducting the criticality analysis and to document the mission-critical functions and capture existing critical component and supplier data. The instruction stated that the prime contractor:

> shall identify only the primary logic-bearing components (hardware, software, and firmware) that implement critical functions of the GMD System. Identification includes primary logic-bearing components installed in contractor "make" items, Non-Developmental Items (NDI), and Commercial Off-The-Shelf (COTS) items that are part of the GMD Technical Data Package (TDP). Logic-bearing components may include Application Specific Integrated Circuits (ASICs), Field-programmable gate arrays (FPGAs), Single Board Computers (SBCs), Complex programmable logic devices (CPLDs), microcontrollers, and other programmable devices.

[18] MDA Technical Intelligence personnel stated that several BMDS programs had to issue task instructions to their prime contractors to assist with the criticality analysis because the MDA did not have access to the assembly break down information to identify parts and vendors.

The MDA accepted the GMD critical components list from the prime contractor in May 2016 and incorporated the critical components list as an appendix to the GMD PPP.

GMD Critical Components List Not Accurate or Effectively Used to Vet Suppliers

(~~FOUO~~) The MDA did not maintain an accurate critical components list to manage risks to the GMD System. The DoD SCRM policy requires the MDA to reduce vulnerabilities to system design or sabotage or subversion and manage risk throughout a program's life cycle and to prioritize supplier threat assessment requests for the [redacted] to vet critical component suppliers. However, the MDA did not fully comply with the DoD SCRM policy.

Critical Components List Not Accurate

The MDA tasked the GMD prime contractor to perform a criticality analysis and to identify the GMD critical components. The critical components list the prime contractor developed was not accurate because:

- it did not contain all critical components,
- it did not contain accurate part numbers, and
- the MDA did not establish a mechanism to update the list throughout the GMD System's life cycle.

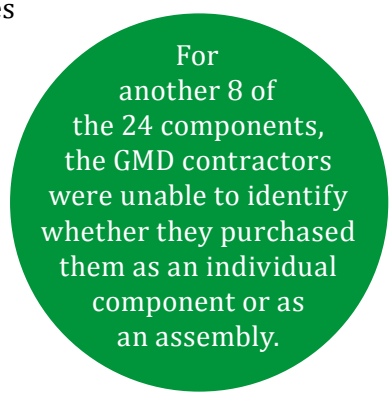
Critical Components List Did Not Contain All Critical Components

(~~FOUO~~) We used nonstatistical methods to select a sample of 24 [redacted] hardware components from the GMD critical components list for review and analysis. One analysis we performed was to determine whether the GMD critical components list included only primary logic-bearing components, including those installed in contractor-made assemblies. We requested the MDA to identify whether the GMD prime contractor or subcontractors (GMD contractors) purchased the sampled components as individual components or as assemblies. Of the 24 sampled critical hardware components, the GMD contractors identified 6 as assemblies, and there was no identification of the individual primary logic-bearing components that made up the 6 assemblies on the critical components list.

We traced the six assemblies to a subcontractor who informed us that two of the assemblies were built as a kit at one of its facilities and that these kits consisted of numerous subcomponents. The prime contractor indicated that the 2 assemblies contained 21 and 456 lower-level components, respectively. The subcontractor also informed us that the assemblies contained multiple programmable logic-bearing

components obtained from a variety of sources and that significant time and resources would be needed to identify the supply sources for the logic-bearing components that made up the two assemblies.

In addition, for another 8 of the 24 components, the GMD contractors were unable to identify whether they purchased them as an individual component or as an assembly. Therefore, it is possible that these eight critical hardware components also consisted of multiple logic-bearing components.



Furthermore, the GMD critical components list did not contain all critical software and firmware. We asked the MDA and the GMD prime contractor officials why the GMD critical components list did not contain any organic software or firmware. The MDA and prime contractor officials stated that they omitted organic software and firmware because they believed organic software presented a low supply chain security risk. Overall, the GMD critical components list did not provide an accurate reflection of all critical hardware, software, and firmware.

Critical Component List Did Not Contain Accurate Part Numbers

The GMD critical components list did not contain the most current part number configuration for 19 of the 24 sampled hardware components. In response to our data request for purchase orders and other information for the 24 components, the GMD contractors identified that the part numbers for 19 components were not current. Specifically, the items were identified as "heritage items" or identified as no longer listed on the current "As-Designed Parts, Materials, and Processes List."[19] For 2 of the 19 components, the GMD prime contractor provided us with the part number for the new configuration, and neither of the part numbers were on the GMD critical components list.

The GMD contractors stated that the part numbers used to develop the critical components list were part numbers from an older configuration that was prior to the award of the current GMD contract. The GMD contractors stated that the older configuration part numbers were most likely still installed in the field, but the contractors were no longer purchasing them because they were purchasing the new configuration part numbers.

[19] A program-specific list of all parts, materials, and processes used in safety and mission-critical applications, including parts and materials used in the life cycle of the product.

MDA Did Not Establish a Mechanism to Update the Critical Components List Throughout the GMD System's Life Cycle

The MDA tasked the prime contractor to develop the critical components list in March 2015 and accepted the list in May 2016. MDA officials informed us that they did not establish a mechanism to keep the list current to reflect changes throughout the GMD System's life cycle. The As-Designed Parts, Materials, and Processes List is a deliverable on the GMD contract and represents the primary parts list for all mission and safety critical components. The As-Designed Parts, Materials, and Processes List should be updated to reflect changes throughout the GMD System's life cycle, and MDA officials acknowledged that all critical components should be identified as a subset of the list. However, there was no mechanism to update the critical components list to reflect changes to the As-Designed Parts, Materials, and Processes List. Therefore, without additional MDA controls or a contract modification, there was no assurance that the GMD critical component list was accurate.

(~~FOUO~~) Critical Components List Not Prioritized for [redacted] Threat Assessments

(~~FOUO~~) The MDA did not prioritize the GMD critical components list for [redacted] threat assessments. DoDI 5200.44 required the MDA to coordinate and prioritize requests for threat analysis of critical component suppliers from the [redacted] and use the [redacted] analysis as a basis for risk management decisions. The DoD PPP guidance[20] requires agencies to prioritize their level I and level II critical components for [redacted] threat assessments to prevent undue burden on the [redacted] resources. The GMD critical components list contained [redacted] critical components. Table 2 identifies the breakout of the GMD critical hardware components by assigned criticality level.

(~~FOUO~~) Table 2. GMD Critical Hardware Components by Assigned Criticality Level

Criticality Level	System Impact	(FOUO [redacted]
Level I	Total Mission Failure	[redacted]
Level II	Significant/Unacceptable Degradation	[redacted]
Level III	Partial/Acceptable	[redacted]
Level IV	Negligible	[redacted]
Not Assigned	Unknown	[redacted]
Total		[redacted]

Source: DoD OIG.

[20] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Program Protection Plan Outline and Guidance," July 18, 2011 and Defense Acquisition Guide, Chapter 13 "Program Protection," May 15, 2013.

(~~FOUO~~) The MDA did not prioritize level I and level II critical components to guide the [redacted] threat assessments. Furthermore, the GMD critical components list that the MDA provided to its liaison in July 2016 at the [redacted] contained only [redacted] components, and the MDA categorized all of the components as criticality level I. The MDA officials could not explain why all components were categorized as criticality level I. Had the MDA included only the actual criticality level I and II items derived from its criticality analysis, it would have submitted only [redacted] components for [redacted] threat assessments. In addition, if the MDA prioritized the list of criticality level I and II components as high, medium, or low, it would have allowed for the [redacted] to focus on the most important critical components.

(~~FOUO~~) In addition to not properly prioritizing the GMD critical component list for threat assessments, the list the MDA provided to its liaison at the [redacted] in July 2016 was stripped of manufacturer, model number, and part number information for the components. That information was necessary for the [redacted] to obtain threat analysis data on the critical components. However, the MDA's [redacted] liaison informed us in March 2017 that he had not submitted the list to the [redacted] because of a backlog of other requests but if he had submitted the request, the [redacted] would have rejected it.

(~~FOUO~~) By not prioritizing the GMD critical component list and not providing the necessary information to obtain threat assessments of critical item suppliers, the MDA is delaying its ability to obtain threat assessments from the [redacted] and increasing risk to the MDA supply chain security for GMD critical components. In response to our inquiries, MDA officials informed us that they retracted the list of critical components the MDA provided its liaison at the [redacted] to update the list with new GMD critical components and the information necessary to allow the [redacted] to perform threat assessments.

(~~FOUO~~) The MDA needs to improve the accuracy of the critical component list for the GMD System, maintain an accurate and updated list throughout the system's life cycle, and prioritize the list for supplier threat assessment requests to the [redacted] in accordance with DoD policy.

MDA Could Not Identify Critical Component Suppliers

(~~FOUO~~) The MDA could not identify suppliers of all GMD critical components. The identification of critical suppliers is necessary for the [redacted] to perform threat assessments on the suppliers, and for the MDA to use the results of those assessments to make risk management decisions. Our analysis of sampled critical hardware, software, and firmware components raised concerns about the MDA's ability to identify the suppliers of all GMD critical components.

MDA Could Not Identify Critical Hardware Suppliers

The MDA could not identify all critical hardware suppliers for the GMD System. For our nonstatistical sample of 24 critical GMD hardware components, we requested the MDA to provide purchase orders to identify the suppliers throughout the various tiers of the supply chain. The MDA sent our request to the GMD contractors to obtain the requested information.

Purchase Orders Not Always Available to Identify Suppliers

The GMD contractors could provide purchase orders for only half of the 24 sampled critical hardware components.

The GMD contractors could provide purchase orders for only half of the 24 sampled critical hardware components. The purchase orders showed that the GMD contractors purchased the 12 critical hardware components from either the original manufacturer or an authorized distributor. An authorized distributor is specifically authorized by a manufacturer to distribute the manufacturer's product. For the 12 sampled critical hardware components not supported by purchase orders, we were unable to identify the suppliers. In addition, the MDA QS supplier road map did not list the suppliers for 4 of the 12 critical hardware components.

Components Built or Purchased as Assemblies Lacked Audit Trail for Individual Subcomponents

The GMD contractors identified that 6 of the 24 components were built or purchased as assemblies. As previously mentioned, the GMD contractors informed us that the assemblies contained multiple programmable logic-bearing components obtained from a variety of sources and significant resources and time would be needed to identify the source that supplied their logic-bearing components.

MDA Could Not Identify Critical Software and Firmware Suppliers

(~~FOUO~~) The MDA could not identify critical software and firmware suppliers (developers) for the GMD System. The GMD critical software and firmware lists contained [redacted] software and firmware components (programs) deemed critical[21] Table 3 shows the quantity of software and firmware programs deemed critical to the GMD System by the MDA.

(~~FOUO~~) Table 3. Breakout of GMD Critical Software and Firmware by Criticality Level

Criticality Level	System Impact	(~~FOUO~~) [redacted]	(~~FOUO~~) [redacted]	(~~FOUO~~) [redacted]	(~~FOUO~~) [redacted]
Level I	Total Mission Failure	[redacted]	[redacted]	[redacted]	[redacted]
Level II	Significant/Unacceptable Degradation	[redacted]	[redacted]	[redacted]	[redacted]
Level III	Partial/Acceptable	[redacted]	[redacted]	[redacted]	[redacted]
Level IV	Negligible	[redacted]	[redacted]	[redacted]	[redacted]
Total		[redacted]	[redacted]	[redacted]	[redacted]

* The GMD prime contractor identified [redacted] programs as organic software, but an MDA official stated that the programs were not organic software.

Source: DoD OIG.

(~~FOUO~~) DoD policy specifies that access to the software development environment should be limited to cleared personnel.[22] The GMD PPP and the prime contractor's program protection implementation plan required controlled access to development environments, including maintaining lists of cleared personnel. We used nonstatistical methods to select 7 [redacted] programs from the GMD critical software and firmware lists and 2 additional GMD organic software programs identified on the QS supplier road map. As part of the audit, we requested the MDA provide the name and nationality of all developers involved for each of the nine sampled programs.[23] The MDA could not provide the names and nationalities of all developers for the nine sampled programs. MDA officials stated that the prime contractor did not request nationality information and that they did not know of a requirement to collect and report this

The MDA could not provide the names and nationalities of all developers for the nine sampled programs.

[21] There were two separate lists of critical software and firmware and each represented a different version of the GMD Ground Systems component.

[22] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Program Protection Plan Outline and Guidance," July 18, 2011.

[23] This was one of the specific matters the committee asked our audit to address. See Appendix B for details.

(~~FOUO~~) information. However, the identification of critical suppliers is necessary for the [redacted] to perform threat assessments on the suppliers, and for the MDA to use the results of those assessments to make risk management decisions. The inability to identify the developers increases the risk to the security of GMD critical software and firmware.

The MDA needs to identify the suppliers of all GMD critical components.

Rigorous Test and Evaluation Capabilities Missing

The MDA did not comply with DoDI 5200.44 to use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within GMD critical components. Specifically, the MDA did not:

- apply all SCRM requirements from the PMAP (Revision B) to the GMD contract,
- effectively execute requirements from the April 2014 MDA policy memorandum on SCRM, or
- establish or implement verification and validation procedures to fully comply with DoD SCRM requirements.

PMAP SCRM Requirements Not Applied to the GMD Contract

The MDA did not apply all SCRM requirements from the PMAP (Revision B) to the GMD contract. These requirements involved the acquisition of custom devices, supplier selection and surveillance, and the acquisition of COTS information assurance products.

Acquisition of Custom Devices Not Adequately Controlled

The MDA did not apply portions of the PMAP (Revision B), paragraph 3.2.7, to the GMD contract involving the acquisition of custom devices. The MDA omitted the requirement that GMD contractors procure integrated circuit products from a supplier accredited by the DMEA when the integrated circuit products are custom-designed, custom-manufactured, or tailored for a specific DoD military end use.

Supplier Selection and Surveillance Not Fully Addressed

The MDA did not apply portions of the PMAP (Revision B), paragraph 3.7.1, to the GMD contract involving supplier selection and surveillance. The MDA omitted the requirement that supplier selection and surveillance methodology at a minimum include processes to verify critical function components received from suppliers to ensure that components are free from malicious code in accordance with "National Security Agency Guidance for Addressing Malicious Code Risk," September 10, 2006.

Acquisition of COTS Information Assurance Products Not Controlled

The MDA did not apply portions of the PMAP (Revision B), paragraph 3.10, to the GMD contract involving the acquisition of COTS information assurance products. The MDA omitted wording from the contract that required COTS information assurance products[24] used in MDA hardware for entering, processing, storing, displaying, or transmitting national security information be limited only to those that have been evaluated and validated jointly by the MDA program office and the National Security Agency. In addition, the MDA also omitted wording that required the validation of COTS information assurance products be conducted by accredited commercial laboratories or the National Institute of Standards and Technology.

April 2014 MDA SCRM Policy Memorandum Not Effectively Executed

The MDA did not effectively execute the requirements from its April 2014 SCRM policy memorandum. The MSTIC was to meet at least twice yearly, and the MDA Director of Engineering was to report twice yearly to the Director, MDA, on the progress of the MDA SCRM initiatives and compliance. In addition, the MSTIC was responsible for overseeing MDA's SCRM implementation and reviewing and approving all critical components lists derived from program-level criticality analyses. The MSTIC did not effectively lead, coordinate, and monitor the MDA's SCRM efforts and had not met as required two times yearly because of resource constraints. The MSTIC met only twice, once in July 2013, before the MDA issued the SCRM policy memorandum, and once after, in May 2015. In addition, the MSTIC did not fulfill its requirement to review the GMD critical components list. The MDA informed us that it planned to reinstate the MSTIC activity in FY 2017.

The MSTIC did not effectively lead, coordinate, and monitor the MDA's SCRM efforts.

[24] These products include routers, switches, servers, and communication equipment.

In addition, the SCRM policy memorandum required the QS Director to coordinate with the MDA Director of Technical Intelligence to audit the compliance of vendors and sub-tier vendors for all logic-bearing parts identified through SCRM criticality analysis. However, the responsible directors did not coordinate and execute this requirement.

The MDA informed us that the Technical Intelligence Directorate performed the criticality analyses but had not shared the results with the QS Directorate. The MDA also informed us that the QS Directorate personnel had shared their audit plans with the Technical Intelligence Directorate and had invited them to participate in their audits since May 2013. However, at the time of our fieldwork, personnel from the Technical Intelligence Directorate had participated in only one QS supplier audit for the GMD program. The MDA also informed us that it was not aware of any formal plan to comply with MDA Policy Memorandum No. 70 and its SCRM-related requirement to audit the compliance of vendors and sub-tier vendors for all logic-bearing parts identified through SCRM criticality analysis for the GMD program.

SCRM Verification and Validation Procedures Not Established or Implemented

The MDA did not establish or implement verification and validation procedures to fully comply with DoD SCRM requirements for the GMD System critical components. This included verification and validation procedures for the GMD System critical hardware and for critical software and firmware.

MDA Lacked Verification and Validation Procedures for Critical Hardware

The MDA lacked verification and validation procedures for critical GMD System hardware. As previously mentioned, the MDA did not comply with its own requirement for the QS and Technical Intelligence directorates to audit the compliance of vendors and sub-tier vendors for all logic-bearing parts identified through SCRM criticality analysis.

(~~FOUO~~) The GMD PPP stated that the SCRM program would [redacted]

Specifically, the PPP stated that the MDA would:

- conduct SCRM audits and assessments, including hardware or software functional or verification testing, at contractor facilities;
- conduct engineering testing and acceptance testing on microelectronic components prior to use on the GMD System; and

- levy SCRM PPP requirements on the contractor, and that the finalized risk mitigation strategies would be addressed in the contractor program protection implementation plan, which is a contractually required document that details how the prime contractor would implement the GMD PPP requirements.

However, the MDA was unable to provide evidence to support the verification and validation efforts cited in the GMD PPP. In addition, the MDA did not levy SCRM PPP requirements on the contractor because the prime contractor's program protection implementation plan stated that DoDI 5200.44 compliance was not yet required by the contract.

MDA Lacked Verification and Validation Procedures for Critical Software and Firmware

The MDA lacked verification and validation procedures for critical GMD System software and firmware to comply with DoDI 5200.44. The GMD PPP did not address any MDA software assurance testing for malicious threats, and the MDA did not perform any associated independent verification and validation testing.

According to the GMD PPP, the MDA established software assurance countermeasures in the software development phase to ensure strong software assurance and planned to perform 100-percent testing of three categories[25] of developmental software in comparison to three industry standard databases[26] of known software security weaknesses and vulnerabilities. However, the GMD PPP did not identify any testing that the MDA would perform for malicious threats. The GMD PPP specified that the prime contractor or subcontractors performed all testing for malicious threats.

However, the prime contractor's GMD program protection implementation plan only addressed software assurance testing associated with testing for malicious threats using one of the three industry standard databases required by the MDA GMD PPP. The prime contractor's program protection implementation plan supported planned testing by the prime contractor and two of the three subcontractors. The plan indicated that two of the three subcontractors would test all three developmental software categories using only the Common Weakness Enumeration database, and the prime contractor would also test one of the three developmental software categories using the same database. However, the plan contained no information

[25] The three categories of developmental software were critical program information software, critical function software, and other software.

[26] The databases were the Common Vulnerabilities and Exposures database, the Common Attack Pattern Enumeration and Classification database, and the Common Weakness Enumeration database. These databases are used to identify and coordinate software vulnerabilities that enable various types of attacks, identify common destructive attack patterns, and examine software architecture and source code for weaknesses.

for planned testing by the third subcontractor, because the third subcontractor prepared its own program protection implementation plan and that information was not incorporated into the prime contractor's plan. In addition, the prime contractor's program protection implementation plan contained conflicting information, which made it unclear what testing was actually planned, and against which of the three industry standard databases.

The MDA GMD software assurance officials stated that they did not receive any deliverables from the prime contractor related to malicious risk analysis or mitigation.

(~~FOUO~~) The MDA GMD software assurance officials stated that they did not receive any deliverables from the prime contractor related to malicious risk analysis or mitigation, [redacted] once it received the software from the contractor. The MDA GMD software assurance officials stated that they relied on their contractors for testing [redacted]; however, without receiving any deliverables, there is no evidence that the prime contractor actually tested [redacted]. The MDA officials responsible for GMD software assurance stated that they had personnel at the prime contractors' site to perform independent verification and validation that involved witnessing testing sessions, reviewing test results, and performing their own testing. However, those efforts focused strictly on software quality assurance and not security.

(~~FOUO~~) Neither the MDA nor its contractors conducted [redacted], and the MDA software assurance officials stated that they relied solely on their contractors for firmware quality. There were [redacted] in the GMD PPP or in the prime contractor's program protection implementation plan.

The MDA needs to use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within GMD critical components.

Increased Program Risks

DoD SCRM is an integral part of the DoD's trusted systems and networks strategy. The purpose of the DoD's trusted systems and networks strategy is to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage, or subversion of a system's mission critical functions or critical components, by foreign intelligence, terrorists, or other adversaries. By not fully complying with DoD SCRM requirements, the MDA faces

an increased risk that an adversary could infiltrate the supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the GMD System critical components.

Conclusion

The MDA did not fully comply with DoD SCRM policy to identify susceptibilities, vulnerabilities, and threats throughout the GMD supply chain and to develop mitigation strategies to combat those threats. This occurred because the MDA did not:

- (~~FOUO~~) establish controls and oversight to maintain an accurate critical components list to manage risks to the GMD System throughout its life cycle and prioritize the list for supplier threat assessment requests to the [redacted];
- identify the suppliers of all critical components for the GMD System; or
- use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within critical components for the GMD System.

However, if the MDA addresses our findings, it can decrease the risk that an adversary could infiltrate the supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the GMD System critical components.

Management Comments on the Finding and Our Response

The Director, MDA, provided the following comments on the Finding. For the full text of the Director's comments, see the Management Comments in the back of the report.

MDA Comments on QS Audits and Technical Assessments and Coordination with the Technical Intelligence Directorate

The Director, MDA, stated that for any supplier assessments the Technical Intelligence Directorate identified, the scope of QS audits and technical assessments can be, and has been, adjusted to accommodate SCRM, as it was for the one GMD assessment noted as having Technical Intelligence Directorate participation. The Director stated that the QS Directorate solicited input regarding which suppliers to assess and received no input from the Technical Intelligence Directorate. The Director also stated that the QS Directorate will assess any Technical Intelligence Directorate suppliers of interest with the Technical Intelligence Directorate's support.

Our Response

The Director did not provide any evidence to support how the scope of the QS audits and technical assessment had been increased to specifically address DoD SCRM requirements. At the time of our fieldwork, personnel from the Technical Intelligence Directorate had participated in only one QS supplier audit for the GMD program. We acknowledged that the Technical Intelligence Directorate performed the criticality analysis, but had not shared the results with the QS Directorate. We also acknowledged that the QS Directorate shared audit plans with the Technical Intelligence Directorate and invited the Technical Intelligence Directorate to participate in audits beginning in May 2013. However, their ineffective coordination is a contributing factor hindering the MDA's efforts to comply with MDA Policy Memorandum Number 70 and DoD SCRM requirements for the GMD System.

MDA Comments on the QS Supplier Road Map not Listing Suppliers

The Director, MDA, stated that the four critical hardware components that we determined were not listed on the MDA supplier road map appear on the GMD program "As Designed Product and Materials List," which the Director contends demonstrates that the program did account for those parts in at least one document.

Our Response

Whether or not the parts appeared on the "As Designed Product and Materials List" is irrelevant to the fact that the MDA did not identify the suppliers of the parts on its supplier road map for the GMD System. As noted in the report, the QS supplier road map did not list 4 suppliers identified in the 12 critical hardware components purchase orders that we reviewed. This raises concern with the effectiveness of the control.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Director, Missile Defense Agency, develop a plan of action with milestones, for the Ground-based Midcourse Defense System to comply with DoD Instruction 5200.44. The plan should establish controls and oversight and require Missile Defense Agency personnel to develop internal procedures or establish contract requirements to:

a. **Improve the accuracy of the critical components list to manage risks to the Ground-based Midcourse Defense System throughout its life cycle and require:**

   1. **Identification of all critical logic-bearing hardware components and critical software and firmware.**
   2. **Periodic updates to the critical components list to reflect changes in mission-critical parts lists such as the As-Designed Parts, Materials, and Processes List. The updates should be tied to system engineering technical reviews or similar events.**
   3. **(~~FOUO~~) Submitting only criticality level I and II components and prioritizing them when requesting supplier threat assessment from the [redacted] Include all information needed by the [redacted] to conduct the supplier threat assessments.**

b. **Improve the identification of suppliers of all critical components for the Ground-based Midcourse Defense System and establish a methodology to trace critical hardware, software, and firmware to their suppliers down to the lowest possible tier of the supply chain and retention of supporting purchase order data.**

c. **Use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within critical components of the Ground-based Midcourse Defense System and require:**

   1. **Implementation of all supply chain risk management-related requirements from the Missile Defense Agency Parts, Materials, and Processes Mission Assurance Plan (Revision B).**

2. **Implementation of the supply chain risk management requirements set forth by Missile Defense Agency Policy Memorandum Number 70.**
3. **Establishment of verification and validation procedures for critical hardware, software, and firmware for the Ground-based Midcourse Defense System.**

Director, Missile Defense Agency Comments

The Director, MDA, agreed, stating that the MDA will evaluate the type of work being considered for the extension of the GMD Development and Sustainment Contract and determine if additional changes are required for the Tailored Parts, Materials, and Processes (PMAP) Revision B. The Director stated that the MDA reviewed the Program Master Plan for the Redesigned Kill Vehicle and verified that no exceptions were taken to the four PMAP SCRM requirements. The Director also stated that the contract will include specific statement of work language restricting procurement of logic-bearing components from vendors approved by the DMEA. Furthermore, the Director stated that the GMD team is working with MDA Technical Intelligence Directorate, Security and Program Protection, and may consider adding additional SCRM language.

Our Response

While the Director, MDA, agreed with the recommendations, the response did not address all specifics of Recommendations 1.a.1, 1.a.2, 1.a.3, 1.b, 1.c.1, 1.c.2, and 1.c.3, and further comments are required. The Director's response did not describe how the MDA would improve the accuracy of the critical components list, improve the identification of suppliers of all critical components, and use rigorous test and evaluation capabilities to test for malicious threats and detect vulnerabilities within critical components. In addition, the Director needs to provide the results of the MDA's evaluation of the GMD Development and Sustainment Contract, including the specific rationale for excluding any DoD SCRM requirements. Finally, the Director needs to provide the specific contract terms for the Redesigned Kill Vehicle that require compliance with DoD SCRM requirements.

Appendix A

Scope and Methodology

We conducted this performance audit from September 2016 through April 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Based on the House Armed Service Committee request,[27] we reviewed the MDA's SCRM processes. Because the MDA did not fully incorporate the DoD's SCRM requirements into the GMD contract, we did not conduct a detailed review of the prime or subcontractors' SCRM-related processes.

(~~FOUO~~) We interviewed officials from the Office of the Deputy Assistant Secretary of Defense for Systems Engineering, the MDA, and the [redacted] In addition, we interviewed officials from the prime contractor and three major subcontractors for the MDA's GMD program.

We obtained and analyzed MDA documentation, specifically:

- GMD contract documentation and deliverables,
- QS supplier road map,
- GMD PPP and critical component list,
- prime contractor's GMD program protection implementation plan,
- MSTIC charter and meeting minutes,
- QS technical assessment reports, and
- prime contractor and subcontractor purchase orders for critical components.

We compared the MDA documentation to the DoD and the MDA policies, standards, and best practices, including:

- DoDI 4140.67, "DoD Counterfeit Prevention Policy," April 26, 2013;
- DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 1, Effective August 25, 2016);

[27] See Appendix B for the complete request, including the specific matters the committee asked to be addressed.

- Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, "Program Protection Plan Outline and Guidance," July 18, 2011;
- Defense Acquisition Guidebook, Chapter 13 "Program Protection," May 15, 2013;
- MDA Policy Memorandum No. 70, "Supply Chain Risk Management," April 10, 2014 (Certified Current October 20, 2015);
- MDA PMAP Revision B "Missile Defense Agency Parts, Materials, and Processes Mission Assurance Plan," March 2, 2012; and
- MDA "Parts, Materials, and Processes Mission Assurance Plan," Revision A, March 26, 2008.

(~~FOUO~~) We obtained the critical components list for the GMD System and reviewed the list for accuracy. Specifically, we obtained a population of [redacted] critical hardware, [redacted] critical COTS software programs, [redacted] critical COTS firmware programs, and [redacted] other software programs. We analyzed the population of MDA GMD critical components based on criticality levels and used nonstatistical methods to select 24 hardware items that the MDA deemed critical to the GMD System for review. In addition, we used nonstatistical methods to select nine software and firmware programs, seven of which the MDA deemed critical to the GMD System. In addition, we used nonstatistical methods to select two organic software programs from the QS supplier road map that the MDA identified as being part of the GMD System.

We reviewed each critical hardware component to determine whether:

- it was supported by a purchase order,
- it was purchased as an individual piece part or an assembly,
- it was purchased from a supplier accredited by the DMEA,
- it was purchased from the original manufacturer or an authorized distributor,
- its supplier was listed on the QS supplier road map, and
- MDA could provide evidence that any independent verification and validation was performed related to the purchase of the component.

We reviewed the sampled software and firmware programs to determine whether the MDA or its contractors could identify by name and nationality of all developers involved.[28]

[28] This was one of the specific matters the committee asked our audit to address. See Appendix B for details.

Use of Computer-Processed Data

We used computer-processed data in the form of spreadsheets the MDA provided that contained listings of critical components for the GMD System and suppliers of BMDS safety and mission-critical components. The GMD prime contractor developed the critical component list as part of a GMD contract modification. To test the reliability of the data, we made inquiries in the form of data requests, and interviewed MDA personnel, as well as the GMD prime contractor and subcontractor personnel. In addition, we analyzed and compared the critical component list to applicable DoD policy. We determined that the computer-processed data were sufficiently reliable for our purposes.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) issued one report discussing DoD SCRM. Unrestricted GAO reports can be accessed at http://www.gao.gov.

GAO

Report No. GAO-16-236, "DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," February 2016

> The DoD's agencies and contractors submitted 526 suspect counterfeit parts reports in the Government-Industry Data Exchange Program from fiscal years 2011 through 2015, submitted primarily by contractors. The Defense agencies and contractor officials explained that congressional attention to counterfeit parts in 2011 and 2012 led to increased reporting, and that the lower number of reports in more recent years is partly the result of better practices to prevent the purchase of counterfeit parts. Several aspects of the DoD's implementation of its mandatory Government-Industry Data Exchange Program reporting for suspect counterfeit parts have limited the program's effectiveness as an early warning system.
>
> All seven contractors the GAO spoke with have established systems to detect and avoid counterfeit electronic parts; however, the DoD has not finalized how these systems will be assessed. Contractors are seeking additional clarification on how to meet some of the DoD's requirements. Until the DoD clarifies criteria for contractors on how their systems will be evaluated, it cannot fully ensure these systems detect and avoid electronic counterfeit parts, as required.

Appendix B

House Armed Service Committee Request and Our Response

House Armed Service Committee Request

Supply Chain Security of Strategic Capabilities

The committee is aware of the report submitted by the Government Accountability Office (GAO), "DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," (GAO-16-236) in February 2016. The committee noted the finding that, "DoD contractors rely on thousands of subcontractors and suppliers, including the original component manufacturers that assemble microcircuits and the mid-level manufacturers subcontracted to develop the individual subsystems that make up a complete system or supply." The committee is concerned that, as a practical matter, it appears that the Department possesses very little real data about the supply chain associated with certain critical systems. It also appears that the Department largely relies on assurances it receives from prime contractors, but oftentimes those prime contractors rely on subcontractors and others for information regarding supply chains and there may be little or no actual data on which to base their assurances to the Department.

Furthermore, the committee is aware that the Department recently promulgated Defense Federal Acquisition Regulation Supplement Subpart 239.73, ("Requirements For Information Relating To Supply Chain Risk"), but the committee is concerned that there has been little practical progress in implementing these regulations. Moreover, even when implemented, an approach that relies primarily (or exclusively) on simply analyzing threat intelligence in Government databases will almost certainly not generate sufficient data about actual hardware and software components and subcomponents necessary to understand critical supply chains.

Therefore, the committee directs the Inspector General of the Department of Defense to conduct an audit to evaluate the supply chain security and assurance of one network or system deemed critical in each of the Missile Defense Agency, Air Force Space Command, the nuclear command and control system, and a delivery system or platform for U.S. nuclear weapons. Furthermore, the committee directs the Inspector General to submit a final report to the Committees on Armed Services of the Senate and the House of Representatives not later than May 1, 2017, on the supply chain security and assurance evaluation of such

networks or systems. The committee further directs the Inspector General to provide an interim briefing to the House Committee on Armed Services not later than July 1, 2016, on the manner in which it intends to conduct this evaluation. As part of the Inspector General's assessment, the following matters should be addressed:

1. Does the defense agency or military service responsible for the particular system or network conduct actual forensic evaluations of the supply chain associated with the system or network? Does the agency or service rely on the representations of U.S. suppliers or does it perform independent verification and validation of the source of supply for each critical component and subcomponent of U.S.-branded products or systems?
2. For software, firmware, and chip design that is deemed by the command or agency to be critical to the reliability and performance of the designated network or system, can the service or agency (or its suppliers) identify by name and nationality the developers involved?
3. How much diligence has been performed by the service or agency on second- and third-tier suppliers?

Our Response

1. The MDA did not conduct actual forensic evaluations of the supply chain for the GMD System with regard to DoD SCRM requirements. The MDA relied on the representation of the prime contractor and subcontractors, and we found no evidence of any independent verification and validation of the source of supply for each critical component and subcomponent we sampled.
2. The MDA was unable to provide by name and nationality the developers involved with critical software, firmware, or chip design.
3. The MDA performed limited diligence on second- and third-tier suppliers in regards to DoD SCRM requirements. The MDA maintained a supplier road map that identified suppliers down to the fifth tier of the supply chain. However, there was no assurance that the supplier road map was complete. The MDA conducted audits and assessments of suppliers for the GMD System and the scope of those reviews included counterfeit parts avoidance. However, the scope of the audits and assessments did not include procedures to evaluate compliance with all DoD SCRM requirements.

Management Comments

Director, Missile Defense Agency

DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY
5700 18TH STREET
FORT BELVOIR, VIRGINIA 22060-5573

Mr. Patrick Nix
Department of Defense Inspector General
Program Director Acquisition
and Sustainment Management
Alexandria, VA 22350-1500

Dear Mr. Nix:

The Missile Defense Agency (MDA) appreciates the opportunity to review and comment on the Department of Defense Inspector General Draft Report, "The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System," dated April 4, 2017 (Project No. D2016-D000AG-0215.000). MDA comments are enclosed.

MDA concurs with the recommendation in the Draft Report and is already working to comply by doing the following:

1. For the Development and Sustainment Contract extension, the Ground-Based Midcourse (GM) team is evaluating the type of work being considered for the extension to determine if additional changes are required for the Tailored Parts, Materials, and Processes (PMAP) rev B or the Program Protection Plan/security Statement of Work (SOW) language, which is currently on contract.

2. For the Redesigned Kill Vehicle (RKV), the GM team has reviewed the Program Master Plan control plan for [redacted] and [redacted] and verified that no exceptions were taken to the four PMAP Supply Chain Risk Management (SCRM) requirements. The RKV contract will also include specific SOW language for SCRM, a major feature of which restricts procurement of logic bearing components from vendors approved by the Defense Microelectronic Activity. The GM team is working with MDA Security and may consider adding additional SCRM language.

For future acquisitions, any new contract will address the deficiencies identified in this report. My point of contact for this effort is [redacted].

Sincerely,

J. D. Syring
Vice Admiral, USN
Director

Enclosures:
As stated

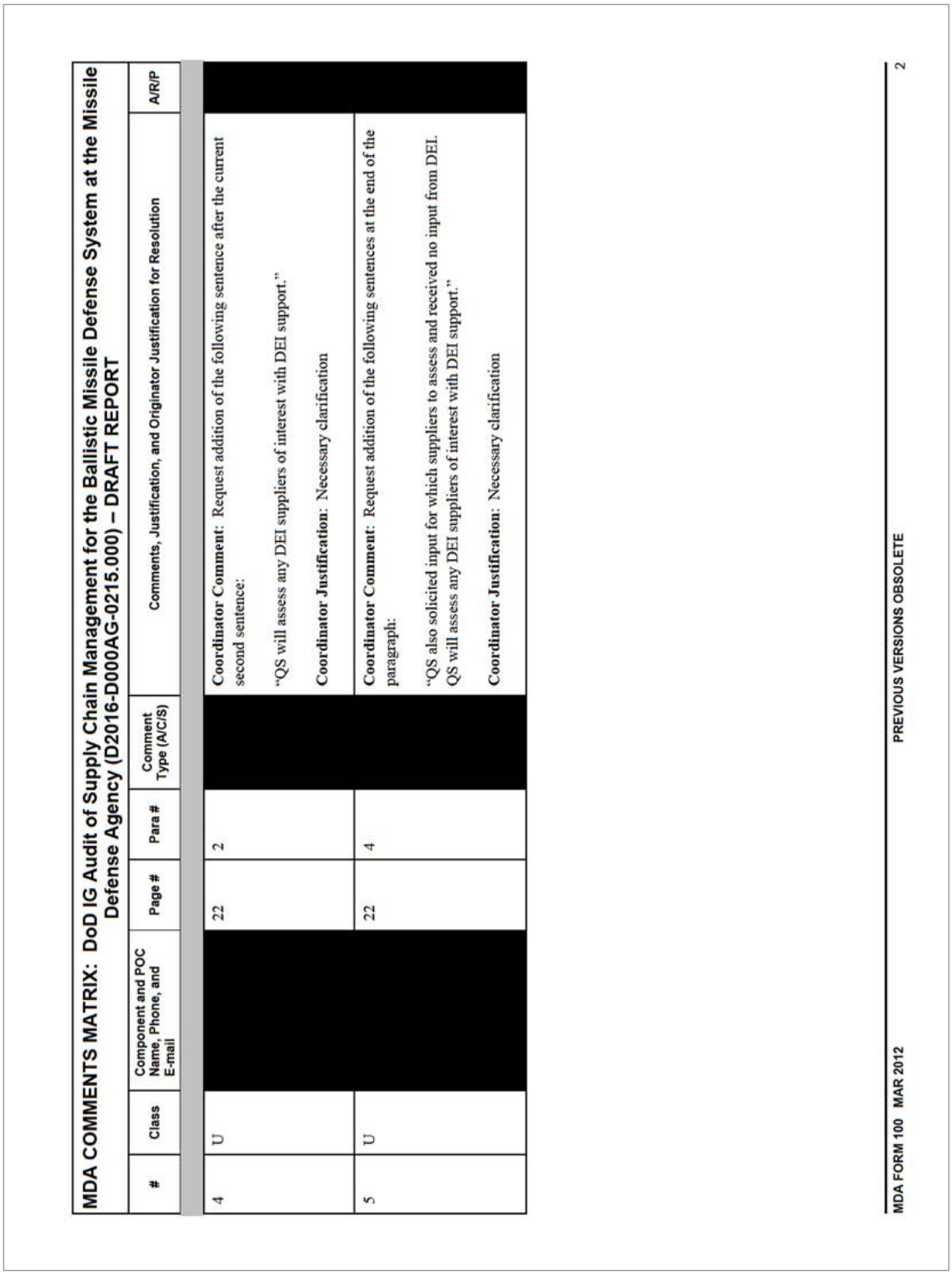
Director, Missile Defense Agency (cont'd)

MDA COMMENTS MATRIX: DoD IG Audit of Supply Chain Management for the Ballistic Missile Defense System at the Missile Defense Agency (D2016-D000AG-0215.000) – DRAFT REPORT

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
1	U	[redacted]	8	3	[redacted]	**Coordinator Comment**: For the paragraph with the header "Audits and Technical Assessments…", request the following two sentences be substituted for the final sentence: "For any DEI-identified supplier assessments, the standard scope that QS uses is increased to assess compliance with DoD SCRM requirements. DEI supports these assessments and focuses on SCRM." **Coordinator Justification**: Necessary clarification that the scope of QS audits and technical assessments can be, and has been, adjusted to accommodate SCRM, as it was for the one GM assessment noted as having had DEI participation.	[redacted]
2	U	[redacted]	18	3	[redacted]	**Coordinator Comment**: For the paragraph with the header "Purchase Orders Not Always…", request the following clause be added to the end of the final sentence: ", however, these parts do appear on the GM program "As Designed Product and Materials List". **Coordinator Justification**: Necessary clarification that the program did account for these parts in at least one document.	[redacted]
3	U	[redacted]	22	1	[redacted]	**Coordinator Comment**: Request addition of the following sentence at the end of the paragraph: "QS also solicited input for which suppliers to assess and received no input from DEI." **Coordinator Justification**: Necessary clarification	[redacted]

MDA FORM 100 MAR 2012 PREVIOUS VERSIONS OBSOLETE 1

Director, Missile Defense Agency (cont'd)



MDA COMMENTS MATRIX: DoD IG Audit of Supply Chain Management for the Ballistic Missile Defense System at the Missile Defense Agency (D2016-D000AG-0215.000) – DRAFT REPORT

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
4	U	[redacted]	22	2	[redacted]	**Coordinator Comment**: Request addition of the following sentence after the current second sentence: "QS will assess any DEI suppliers of interest with DEI support." **Coordinator Justification**: Necessary clarification	[redacted]
5	U	[redacted]	22	4	[redacted]	**Coordinator Comment**: Request addition of the following sentences at the end of the paragraph: "QS also solicited input for which suppliers to assess and received no input from DEI. QS will assess any DEI suppliers of interest with DEI support." **Coordinator Justification**: Necessary clarification	[redacted]

MDA FORM 100 MAR 2012 PREVIOUS VERSIONS OBSOLETE 2

Glossary

Authorized Supplier. A supplier, distributor, or aftermarket manufacturer that is authorized by the original component manufacturer to buy parts or materials directly from the manufacturer. Parts provided from authorized suppliers typically have never left the manufacturer's authorized supply chain, and are accompanied by full manufacturer support and warranty.

Commercial Off-The-Shelf Equipment. Commercial items that typically require no unique Government modifications or maintenance to meet the needs of the procuring agency, during the life cycle of the product. Examples include hard drives and computers. If a source control drawing has been developed with specific requirements for an item, it is not considered commercial off-the-shelf.

Critical Component. A component which is or contains information and communications technology, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission-critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission-critical functions of an applicable system.

Criticality Analysis. An end-to-end functional decomposition performed by systems engineers to identify mission-critical functions and components. This includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions.

Information and Communications Technology. Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (for example, microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

Joint Federated Assurance Center. A federation of all DoD entities having software and hardware assurance capabilities needed by programs. The Joint Federated Assurance Center develops, maintains, and offers software and hardware vulnerability detection, analysis, and remediation capabilities through a federation of internal, coordinated organizations and facilities from across the DoD.

Mission-Critical Functions. Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed.

Original Component Manufacturer. An organization that designs or engineers a part and has obtained the intellectual property rights to that part. The part and its packaging are typically identified with the original component manufacturer's trademark. The original component manufacturer may contract out the manufacturing, test, or distribution of their product.

Program Protection Plan. A risk-based, comprehensive, living plan that captures the program's critical program information, mission-critical functions, and component associated threats, vulnerabilities, and countermeasures. A program protection plan is meant to help programs ensure that they adequately protect their technology, components, and information.

Software Assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle.

Supply Chain. The linked activities associated with providing materiel from a raw material stage to an end user as a finished product or system, including design, manufacturing, production, packaging, handling, storage, transportation, mission operation, maintenance, and disposal.

Supply Chain Risk. The risk that an adversary may sabotage, maliciously introduce unwanted function, 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.

Supply Chain Risk Management. A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the DoD's supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (for example, initial production, packaging, handling, storage, transport, mission operation, and disposal).

Acronyms and Abbreviations

BMDS	Ballistic Missile Defense System
COTS	Commercial Off-The-Shelf
(~~FOUO~~)	[redacted]
DMEA	Defense Microelectronics Activity
GAO	Government Accountability Office
GMD	Ground-based Midcourse Defense
MDA	Missile Defense Agency
MSTIC	MDA SCRM/Trusted System and Networks Integration Council
OIG	Office of Inspector General
PMAP	Parts, Materials, and Processes Mission Assurance Plan
PPP	Program Protection Plan
QS	Quality, Safety, and Mission Assurance
SCRM	Supply Chain Risk Management


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
http://www.dodig.mil/pubs/email_update.cfm

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098