Report No. DODIG-2018-143

~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

AUGUST 14, 2018

Air Force Space Command Supply Chain Risk Management of Strategic Capabilities

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

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

~~FOR OFFICIAL USE ONLY~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Air Force Space Command Supply Chain Risk Management of Strategic Capabilities

August 14, 2018

Objective

We determined whether the Air Force Space Command implemented an adequate supply chain risk management program for four critical strategic systems. Specifically, we conducted a detailed review of the Space Based Infrared System and a limited review of the Air Force Satellite Control Network, the Family of Advanced Beyond Line-of-Sight Terminals, and the Global Positioning System.

We conducted this audit in response to a reporting requirement contained in House Report 114-537, to accompany House Report 4909, the National Defense Authorization Act for Fiscal Year 2017. This is the second in a series of audits on supply chain risk management for DoD strategic capabilities in response to the Congressional requirement.

Background

The Space Based Infrared System is a follow-on capability to the Defense Support Program satellites, which help protect the U.S. and its allies by detecting missile launches, space launches, and nuclear detonation.

The Air Force Satellite Control Network is a global system providing command, control, and communications for space vehicles.

The Family of Advanced Beyond Line-of-Sight Terminals develops nuclear event-survivable terminals capable of communicating with satellite constellations using jam-resistant, low probability of intercept and low probability of detection waveforms for airborne, ground-fixed, and transportable applications.

Visit us at www.dodig.mil

Background (cont'd)

The Global Positioning System is a constellation of orbiting satellites that provides navigation data to military and civilian users all over the world.

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 designing, manufacturing, producing, packaging, handling, storing, transporting, operating, maintaining, and disposing.

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 requires DoD organizations 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 Air Force Space Command established initiatives to manage supply chain risk for the Space Based Infrared System but did not fully implement DoD supply chain risk management policy. This occurred because the Air Force Space Command did not take the steps and establish the controls and oversight necessary to:

- conduct a thorough criticality analysis and identify all critical components and associated suppliers to manage risks to the system throughout its life cycle;
- ~~(FOUO)~~ submit complete and accurate requests for the [redacted] to conduct threat assessments of critical component suppliers;
- require the purchase of all application-specific integrated circuits from trusted suppliers using trusted processes that are accredited; or

Results in Brief

Air Force Space Command Supply Chain Risk Management of Strategic Capabilities

Finding (cont'd)

- ~~(FOUO)~~ ensure the use of rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing [redacted]

In addition, our limited review of three other Air Force Space Command critical systems revealed concerns similar to those found with the Space Based Infrared System supply chain risk management.

As a result, an adversary has opportunity to infiltrate the Air Force Space Command supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the critical hardware, software, and firmware.

Recommendations

We recommend that the Air Force Space Command Commander develop a plan of action, with milestones, for the Space Based Infrared System to comply with DoD supply chain risk management policy. The plan should establish controls and oversight and require Air Force Space Command personnel to develop internal procedures or establish contract requirements to:

- improve the accuracy of the critical components list to manage risks to the Space Based Infrared System throughout its life cycle and require the identification of all critical logic-bearing hardware, software, and firmware, and the associated suppliers;
- ~~(FOUO)~~ improve the accuracy of the requests for supplier threat assessments and require the prioritization of the critical components on the requests and the inclusion of all key information needed by the [redacted] to conduct the assessments;
- determine the risk posture and potential mitigations for all application-specific integrated circuits not procured from a trusted supplier using trusted processes that are accredited; and
- ~~(FOUO)~~ ensure the use of rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing [redacted] and require establishment of verification and validation procedures for critical logic-bearing hardware, software, and firmware.

We also recommend that the Air Force Space Command Commander conduct a detailed review of the supply chain risk management for the Air Force Satellite Control Network, Family of Advanced Beyond Line-of-Sight Terminals, and Global Positioning System programs, and all other programs deemed critical to the Air Force Space Command, to ensure compliance with DoD supply chain risk management policy. If deficiencies are identified, Air Force Space Command officials must develop a plan of action with milestones to correct the deficiencies.

Management Comments and Our Response

The Air Force Space Command Space and Missile Systems Center Vice Commander, responding for the Air Force Space Command Commander, agreed with the recommendations and stated that the Air Force Space Command will improve the supply chain risk management for the Space Based Infrared System and:

- conduct a criticality analysis to accurately identify and compile a parts list for all critical components;

Results in Brief

Air Force Space Command Supply Chain Risk Management of Strategic Capabilities

Comments (cont'd)

- ~~(FOUO)~~ produce a critical components list that includes the break down for all logic-bearing devices to the component level and provide the [redacted] with a request for information that includes all key information necessary to conduct threat assessments of critical item suppliers;
- ~~(FOUO)~~ use the [redacted] supplier threat assessment reports to determine the risk posture and identify potential mitigations for application specific integrated circuits not procured from a trusted supplier using trusted processes that are accredited; and
- incorporate modernized requirements and verification processes to ensure the security of the program and perform verification and validation of these requirements using program protection surveys, independent third party assessors, and developmental and operational tests.

In addition, the Vice Commander agreed to conduct a supply chain risk management review of the Air Force Satellite Control Network, Family of Advanced Beyond Line-of-Sight Terminals, and Global Positioning System programs, and other programs deemed critical to the Air Force Space Command, to ensure compliance with DoD supply chain risk management policy.

The comments from the Vice Commander addressed our recommendations; therefore, the recommendations are resolved and will remain open. We will close the recommendations once the Vice Commander provides the documentation showing that the actions have been completed. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Air Force Space Command Commander	None	1.a, 1.b, 1.c, 1.d, 2	None

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

August 14, 2018

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH, AND ENGINEERING
COMMANDER, AIR FORCE SPACE COMMAND
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Air Force Space Command Supply Chain Risk Management of Strategic Capabilities (Report No. DODIG-2018-143)

We are providing this report for your information and use. We performed this audit in response to a reporting requirement contained in House Report 114-537, to accompany House Report 4909, the National Defense Authorization Act for Fiscal Year 2017. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on the draft of this report when preparing the final report. Comments from the Air Force Space Command addressed all specifics of the recommendations and conformed to the requirements of DoD Instruction 7650.03; therefore, we do not require additional comments.

We appreciate the cooperation and assistance received during the audit. Please direct questions to me at Theresa.Hull@dodig.mil, (703) 604-9312 (DSN 664-9312).

Theresa S. Hull
Assistant Inspector General
Acquisition, Contracting, and Sustainment

Contents

Introduction

Objective 1

Background 1

Review of Internal Controls 6

Finding. Opportunities Exist for Improved AFSPC Supply Chain Risk Management 7

AFSPC Supply Chain Risk Management for the SBIRS 7

Criticality Analysis Not Thorough 8

Supplier Threat Assessment Requests Not Complete or Accurate 12

Purchase of ASICs from DMEA-Accredited Suppliers Not Always Required 15

Rigorous Test and Evaluation Capabilities Missing 16

Other AFSPC Critical Systems also Revealed Concerns 19

Adversaries Have Opportunity to Infiltrate the AFSPC Supply Chain 21

Recommendations, Management Comments, and Our Response 22

Appendixes

Appendix A. Scope and Methodology 25

Use of Computer-Processed Data 27

Prior Coverage 27

Appendix B. House Armed Services Committee Request and Our Response 29

Management Comments

Air Force Space Command 31

Acronyms and Abbreviations 34

Glossary 35

Introduction

Objective

We determined whether the Air Force Space Command (AFSPC) implemented an adequate supply chain risk management (SCRM) program for four critical strategic systems. Specifically, we conducted a detailed review of the Space Based Infrared System (SBIRS) and a limited review of the Air Force Satellite Control Network (AFSCN), the Family of Advanced Beyond Line-of-Sight Terminals (FAB-T), and the Global Positioning System (GPS).

This audit is in response to a reporting requirement contained in House Report 114-537, to accompany House Report 4909, the National Defense Authorization Act for Fiscal Year 2017. This is the second in a series of four audits on DoD strategic capabilities SCRM. See Appendixes A for scope, methodology, and prior audit coverage. See the Glossary for specialized terms used throughout the report.

Background

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 designing, manufacturing, producing, packaging, handling, storing, transporting, operating, maintaining, and disposing.

The House Armed Services Committee's Request

The House Committee on Armed Services, Subcommittee on Strategic Forces, expressed concerns that the DoD possesses limited 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 based these concerns on findings in a Government Accountability Office (GAO) audit report.[1]

The committee directed the DoD Office of Inspector General (OIG) to conduct an audit to evaluate and report on the supply chain security and assurance of the networks or systems deemed critical in the AFSPC, the Missile Defense Agency, the nuclear command and control system, and the delivery system or platform for

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

U.S. nuclear weapons.[2] The committee also identified specific matters that the DoD OIG should address. See Appendixes B for the complete request to include the specific matters the committee wanted addressed and our responses.

Air Force Space Command

The AFSPC provides military focused space and cyberspace capabilities with a global perspective to the joint war fighting team. The AFSPC provides space lift operations and has command and control of all DoD satellites. In addition, the AFSPC uses ground based radar and space surveillance radars, which monitor ballistic missile launches around the globe and provide vital information on the location of satellites and space debris for the nation and the world.

The Space and Missile Systems Center (SMC) is a subordinate unit of the AFSPC and is the center for developing, acquiring, fielding, and sustaining military space systems. The SMC mission is to deliver resilient and affordable space capabilities and is responsible for on-orbit check out, testing, sustainment, and maintenance of military satellite constellations and other DoD space systems.

Space Based Infrared System

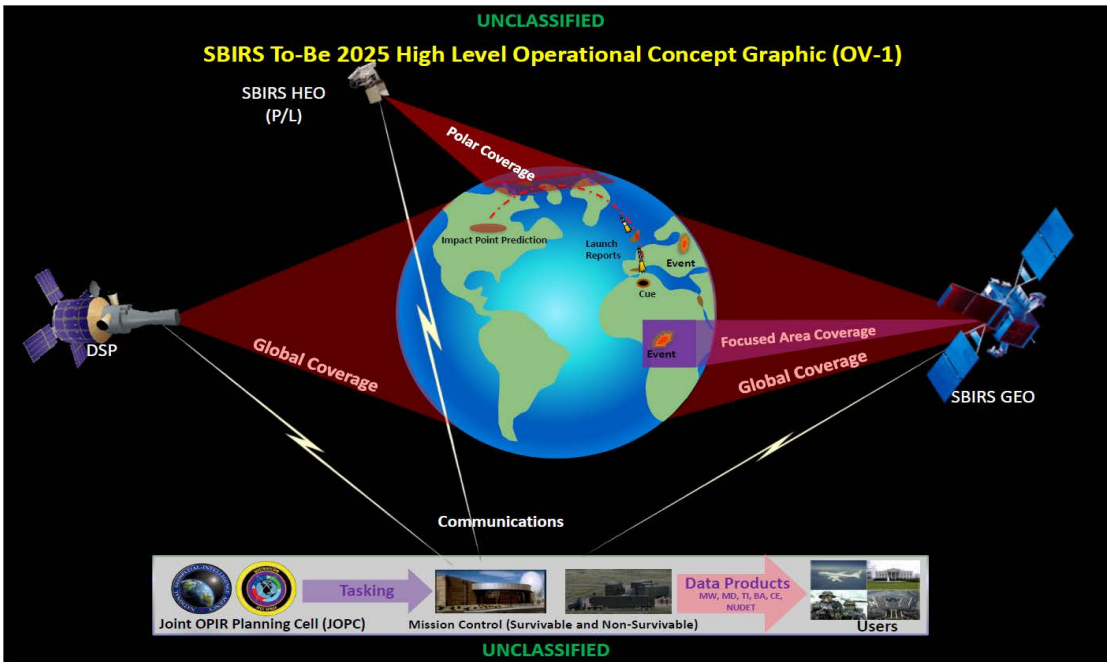
The SBIRS program is a follow-on capability to the Defense Support Program (DSP) satellites, which help protect the U.S. and its allies by detecting missile launches, space launches, and nuclear detonation. The AFSPC designed the SBIRS program to meet jointly defined requirements of the defense and intelligence communities in support of mission areas such as missile early warning, missile defense, battlespace awareness, and technical intelligence.

The SBIRS program consists of the space segment of geosynchronous earth orbit (GEO) satellites and highly elliptical orbit (HEO) sensors riding on host satellites, with the associated worldwide-deployed ground systems. The SBIRS sensors are designed to provide greater flexibility and sensitivity than the DSP infrared sensor. The SBIRS sensors also detect short-wave and mid-wave infrared signals, which allows SBIRS to perform a broader set of missions. These enhanced capabilities result in improved prediction accuracy for global strategic and tactical warfighters. The ongoing evolution of the ground system uses improved mission processing software, resulting in increased event message accuracy, and reduced manpower for support and operations.

[2] Based on an agreement made with the subcommittee staffers, the DoD OIG would conduct a series of audits and this audit is the second in the series. The first audit focused on the Missile Defense Agency.

Both the GEO and HEO infrared sensors gather raw, unprocessed data that are down linked, so that the same scene observed in space will be available on the ground for processing. The GEO sensors also perform onboard signal processing and transmit detected events to the ground. Figure 1 illustrates the SBIRS satellites communicating with the associated ground systems.

Figure 1. SBIRS Satellites Communicating with Associated Ground Systems



Acronyms: BA – Battlespace Awareness, CE – Civil and Environment, MD – Missile Defense, MW – Missile Warning, NUDET – Nuclear Detonation, P/L – Payload, TI – Technical Intelligence.

Source: AFSPC SMC.

The AFSPC SMC Remote Sensing Systems Directorate is responsible for managing the SBIRS program and contracted with a prime contractor for SBIRS program development, systems engineering, and spacecraft development. We reviewed AFSPC SCRM for the production of the GEO 5 and 6 satellites and an upgrade to the ground segment.[3]

Other Air Force Space Command Critical Systems Reviewed

In addition to our detailed review of the SBIRS system, we conducted a limited review of the AFSCN, FAB-T, and GPS.

[3] The GEO 5 and 6 satellites are to be launched as part of the SBIRS program and represent the newest infrared and missile warning satellites, which improve the system and add flexibility for future payloads.

Air Force Satellite Control Network

The AFSCN is a global system providing command, control, and communications for space vehicles. The AFSCN consists of dedicated and common-user equipment and facilities, which collectively provide operational telemetry, tracking, and commanding support for virtually all DoD space vehicles, plus selected space programs of the National Aeronautics and Space Administration and foreign allied nations. The AFSCN supports all major U.S. launches, on-orbit operations, disposal, and emergency recovery of all national security space satellites. We reviewed the AFSPC SCRM for the AFSCN remote tracking station block change.

Family of Advance Beyond Line-of-Sight Terminals

The FAB-T develops nuclear event-survivable terminals capable of communicating with satellite constellations using jam-resistant, low probability of intercept and low probability of detection waveforms for airborne, ground-fixed, and transportable applications. The FAB-T terminals are an essential component of the strategic nuclear execution system. We reviewed the AFSPC SCRM for the FAB-T production.

Global Positioning System

The GPS is a constellation of orbiting satellites that provides navigation data to military and civilian users all over the world. The GPS satellites orbit the Earth every 12 hours, emitting continuous navigation signals. With the proper equipment, users can receive these signals to calculate time, location, and velocity. We reviewed the AFSPC SCRM for the GPS Next Generation Operational Control System.

Federal Government Information and Communication Technology Supply Chain Threats

The modern information and communication technology supply chain is subject to a variety of cyber security threats.[4] These threats may affect the confidentiality, integrity, or availability of government information and information systems and include counterfeiting, tampering, theft, reduced or unwanted functionality, or malicious content. As products pass through the supply chain, vulnerabilities exist for federal departments or agencies. These vulnerabilities enable threat agents to insert malicious content, transfer data, or take advantage of the vulnerabilities in many other ways and may result in substandard products or services, unanticipated failure rates, or compromise of federal missions and information.

[4] National Institute of Standards and Technology Interagency or Internal Report 7622, "Notional Supply Chain Risk Management Practices for Federal Information Systems," October 2012.

DoD Supply Chain Risk and Risk Management

DoD Instruction (DoDI) 5200.44 defines the DoD supply chain risk and risk management.[5] Supply chain risk is the vulnerability that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise compromise the design, integrity, manufacturing, 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.

SCRM is 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.

DoD Supply Chain Risk Management Policy

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 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.[6]
- 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] and use the intelligence analysis as a basis for risk management decisions.[7]
- Manage the supply chain risks to applicable systems throughout their entire life cycle from acquisition through sustainment. Risk management must include processes, tools, and techniques to:

[5] DoDI 5200.44 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 2, Effective July 27, 2017).

[6] 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.

[7] ~~(FOUO)~~ Coordinate requests from the [redacted] 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).

  - Control the quality, configuration, software patch management, and security of software, firmware, hardware, and systems throughout their life cycles, including components or subcomponents from secondary sources.[8]
  - 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.[9]
  - Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats.
  - Implement tailored acquisition strategies, contract tools, and procurement methods for critical components in applicable systems.

- Purchase integrated circuit-related products from a trustworthy supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) 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 [ASICs]).[10]

Air Force Supply Chain Risk Management Policy

Air Force Pamphlet (AFPAM) 63-113 provides procedures to implement the program protection planning requirements contained within DoDI 5200.44.[11] AFPAM 63-113 also requires all new or legacy systems to address mission critical functions and components requiring risk management to protect capabilities.

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.[12] We identified an internal control weakness where the AFSPC did not fully implement DoD SCRM policy for the SBIRS. We will provide a copy of the report to the senior official responsible for internal controls in the AFSPC.

[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 other computer hardware.

[9] A field-programmable gate array is an integrated circuit designed to be configured by a customer or a designer after manufacturing.

[10] 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.

[11] AFPAM 63-113, "Program Protection Planning For Life Cycle Management," October 17, 2013.

[12] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

Opportunities Exist for Improved AFSPC Supply Chain Risk Management

The AFSPC established initiatives to manage supply chain risk for the SBIRS but did not fully implement DoD SCRM policy. This occurred because the AFSPC did not take the steps and establish the controls and oversight necessary to:

- conduct a thorough criticality analysis and identify all critical components and associated suppliers to manage risks to the system throughout its life cycle;
- ~~(FOUO)~~ submit complete and accurate requests for the [redacted] to conduct threat assessments of critical component suppliers;
- require the purchase of all ASICs from trusted suppliers using trusted processes accredited by the DMEA; or
- ~~(FOUO)~~ ensure the use of rigorous test and evaluation capabilities, including developmental, acceptance, and operation testing [redacted].

In addition, our limited review of three other AFSPC critical systems revealed concerns similar to those found with the SBIRS SCRM.

As a result, an adversary has opportunity to infiltrate the AFSPC supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the critical hardware, software, and firmware.

AFSPC Supply Chain Risk Management for the SBIRS

The AFSPC established initiatives to manage supply chain risk for the SBIRS. The initiatives included the completion of a criticality analysis, submission of supplier threat assessment requests, and establishment of SCRM contractual requirements. Despite these initiatives, the AFSPC's SCRM program for the SBIRS did not fully comply with DoD SCRM policy because the AFSPC did not:

- complete a thorough criticality analysis;
- submit complete or accurate supplier threat assessment requests;
- require the purchase of all ASICs from DMEA-accredited suppliers; or
- ensure the use of rigorous testing and evaluation capabilities.

Criticality Analysis Not Thorough

The AFSPC did not conduct a thorough criticality analysis and identify all critical components and associated suppliers. The critical components list was prepared at an assembly level and did not identify all supporting logic-bearing critical hardware components contained within the assemblies or the associated suppliers. In addition, the critical components list did not include critical software or firmware.

Criticality Analysis Guidance

DoDI 5200.44 specifies that a criticality analysis is an end-to-end functional breakdown performed to identify mission-critical functions and components. Criticality Analysis includes:

- identification of a system's missions,
- breakdown of each mission set into the functions to perform those missions, and
- tracing to the hardware, software, and firmware components that either implement those functions, protect those functions, or have unprotected access to those functions.

DoDI 5200.44 defines a critical component as "a component which is or contains ICT (information and communications technology), including hardware, software, and firmware." The definition includes components—whether custom, commercial, or otherwise developed—that deliver or protect the mission critical functionality of a system and, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

AFPAM 63-113 states that organizations should breakdown the system to the lowest possible level to identify potential critical program information and critical components. Examining a system with sufficient granularity is important because identification at the lowest possible sub-system or component level enables organizations to better focus countermeasures to protect against attacks.

DoD program protection guidance provides a specific methodology for DoD organizations to conduct a criticality analysis.[13] The guidance specifies that organizations should update the criticality analysis on a regular basis and tie the updates to system engineering technical reviews. The guidance also recommends

[13] Deputy Assistant Secretary of Defense, Systems Engineering, "Program Protection Plan Outline and Guidance," July 2011; and Defense Acquisition Guide, Chapter 13 "Program Protection," May 15, 2013.

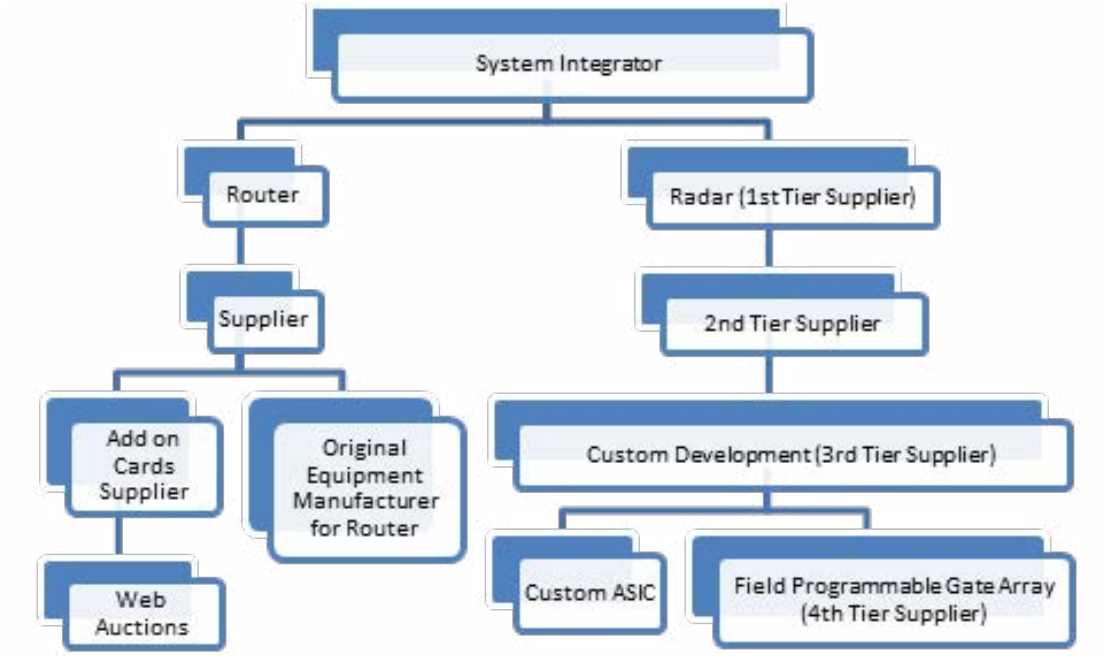
that organizations use a supplier-annotated work or system breakdown structure to assist with tracking and managing supply chain risks. The work or system breakdown structure is a detailed analysis that identifies all system assemblies, subassemblies, and components and their suppliers for all critical components.

The DoD program protection guidance specifies the expected output of an effective criticality analysis as:

- A complete list of mission-critical functions and components.
- Criticality level assignments for all items in the list.
- Supplier information for each critical component.
- ~~(FOUO)~~ Identification of critical elements for inclusion in a [redacted] request.

The Office of the Assistant Secretary of Defense, Research and Engineering, provided a notional example of the tiered supply chain problem illustrating how supplier threat can reside several layers down from the system integrator.[14] As shown in Figure 2, a logic bearing component, such as a field programmable gate array used in a radar, can originate several tiers down the supply chain at a fourth tier supplier.

Figure 2. Tiered Supply Chain Example



Source: Office of the Assistant Secretary of Defense, Research and Engineering.

[14] DoD Comprehensive Program Protection Planning, February 27, 2011.

SBIRS Criticality Analysis

SBIRS program office officials provided their methodology for conducting the SBIRS criticality analysis. SBIRS program office officials stated that subject matter experts performed a criticality analysis to identify potential critical components in accordance with DoDI 5200.44. The subject matter experts identified and evaluated each critical component to determine the system impact level if the critical component became compromised. They assigned each critical component a system impact rating of I through IV in accordance with DoD and other program protection guidance.[15] The results of the criticality analysis were submitted as a component of the SBIRS GEO 5 and 6 PPP and all noted discrepancies were satisfactorily resolved at various levels of the review process.

SBIRS Criticality Analysis Did Not Identify All Supporting Logic-Bearing Components

The AFSPC criticality analysis only resulted in a critical components list that was at an assembly level and did not identify supporting logic-bearing components and the associated suppliers. In addition, the criticality analysis did not include 58 ASICs identified in the SBIRS GEO 5 and 6 satellite production contract.

Critical Component Assemblies Not Broken Down

The SBIRS critical component list identified the components as containing multiple logic-bearing components, such as field programmable gate arrays, microprocessors, integrated circuits, and ASICs. SBIRS program office officials informed us that for some components on the SBIRS critical components list, the prime contractor purchased parts and assembled the component and for others the prime contractor purchased the assembled component.[16] However, the list contained no details or identifying information for the supporting logic-bearing components contained in the assemblies. Detailed information, such as the supplied item description and the associated supplier information, was missing for the supporting logic-bearing components. SBIRS program office officials could not explain why they kept the critical items list at an assembly level and did not identify the supporting logic-bearing components.

We selected an assembled component from the SBIRS critical components list and requested that the SBIRS program office provide a breakdown of all supporting logic-bearing components. The SBIRS program office did not have

[15] See Table 1 for definitions of system impact ratings I through IV. DoD and other program protection guidance included the DoD Comprehensive Program Protection Planning Briefing, February 27, 2011, and the Program Protection Plan Content Rich Template, Aerospace Report, TOR-2013-00825, September 30, 2015.

[16] In this situation, the prime contractor is the system integrator as illustrated in Figure 2.

information showing the breakdown. The SBIRS officials stated it was not a contract deliverable and they would have to request the information through their contracting office from the prime contractor. The SBIRS officials further stated that the information, if available, would not be received in a timely manner and could come at an additional cost. In summary, the SBIRS program office lacked the detailed information necessary to conduct a thorough criticality analysis and identify the critical supporting logic-bearing components and associated suppliers in accordance with DoD program protection guidance. This occurred because the SBIRS program office did not establish a specific contract deliverable or other means to identify and maintain the necessary information.

ASICs Missing from the Critical Components List

A list of 58 ASICs was included as Annex 3 to the SBIRS GEO 5 and 6 satellite production contract. The list identified the component, manufacturer's part number, part description, and supplier name for the 58 ASICs. However, the SBIRS program office did not include the 58 ASICs as part of the SBIRS critical components list and could not provide details on which ASICs they considered critical or non-critical.

SBIRS Criticality Analysis Did Not Include Critical Software and Firmware

The SBIRS criticality analysis did not include critical software or firmware. DoDI 5200.44 specifies that critical components include hardware, software, and firmware. In addition, DoD program protection guidance specifies that the critical components list resulting from the criticality analysis include supporting logic-bearing hardware, software, and firmware.

We requested that the SBIRS program office provide a complete list of software and firmware for the SBIRS GEO 5 and 6 satellites and the ground segment upgrade. We also requested that the SBIRS program office provide the name and nationality of the software and firmware developers.[17] However, the SBIRS program office was unable to deliver the requested information or give a reason why the SBIRS critical components list did not include critical software or firmware.

The AFSPC needs to conduct a thorough criticality analysis and improve the accuracy of the SBIRS critical component list by identifying all supporting logic-bearing hardware, software, and firmware components, and the associated suppliers. The criticality analysis should include the 58 ASICs from the GEO 5 and 6 production contract.

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

Supplier Threat Assessment Requests Not Complete or Accurate

(FOUO) The AFSPC did not submit complete and accurate requests for the [redacted] to conduct threat assessments of SBIRS critical component suppliers. Specifically, the requests lacked key information and the AFSPC did not prioritize components on the requests.

(FOUO) DoDI 5200.44 requires DoD organizations to coordinate and prioritize requests for threat analysis of critical component suppliers and use the intelligence analysis as a basis for risk management decisions. DoD program protection guidance specifies that the criticality analysis should produce a list of critical components and suppliers for use in generating threat assessment center requests and supplier risk mitigation. In addition, the guidance requires agencies to prioritize their critical components for [redacted] threat assessments to prevent undue burden on the intelligence community resources.

(FOUO) DoD program protection guidance specifies that the purpose of requesting threat assessments of critical item suppliers is to allow the [redacted] to conduct counterintelligence assessments to determine [redacted] with the suppliers. The counterintelligence analytical product that results from the analysis provides the program manager with an evaluation of [redacted]. If the assessments find a supplier to be high-risk of [redacted], then the requesting DoD organization can mitigate the risk by purchasing the critical components from a lower-risk supplier.

Supplier Threat Assessment Requests Lacked Key Information

(FOUO) The AFSPC submitted requests for supplier threat assessments to the [redacted] for the SBIRS critical components that did not contain the information necessary to allow the [redacted] to assess critical component suppliers. The Deputy Assistant Secretary of Defense for Systems Engineering provided guidance to the SBIRS program office on submitting requests for supplier threat assessments.[18] The guidance explained that logic-bearing components often implement critical functions and are susceptible to life cycle corruption. The guidance specified the

[18] DoD Comprehensive Program Protection Planning Briefing, February 27, 2011, and Deputy Assistant Secretary of Defense, Systems Engineering, "Program Protection Plan Outline and Guidance," July 2011.

~~(FOUO)~~ need to identify suppliers of logic-bearing components by including the company name, address, commercial and Government entity code, and a description of the supplied item.[19] However, the AFSPC SMC did not include all necessary information on their requests for supplier threat assessments.

~~(FOUO)~~ The AFSPC submitted requests for supplier threat assessments to the [redacted] for critical hardware components for the SBIRS GEO 5 and 6 satellites and the SBIRS ground segment. Our review of the lists found them to contain assemblies instead of the supporting logic-bearing components and associated suppliers. For example, the AFSPC requested information from the [redacted] on an assembly used on the SBIRS GEO 5 and 6 satellites. The SBIRS critical components list identified the assembly as containing ASICs, and SBIRS program office personnel informed us that the prime contractor purchases parts and cards from vendors and builds the assembly. On the request for supplier threat assessment, the AFSPC only provided a description of the assembly and the prime contractor's name, address, and commercial and Government entity code. The AFSPC did not provide a detailed description (such as make, model, or part number) of the ASICs or any other supporting logic-bearing components contained in the assembly or the associated suppliers. Therefore, the AFSPC did not provide the [redacted] the key information needed to assess the suppliers of the supporting logic-bearing components. The [redacted] did not respond to the AFSPC's requests for supplier threat assessments for critical hardware components for the SBIRS GEO 5 and 6 satellites and the SBIRS ground segment.

~~(FOUO)~~ Key details on the logic-bearing components and the associated suppliers are necessary for the [redacted] to conduct supplier threat assessments. For example, the requests for supplier threat assessments for the FAB-T critical components included [redacted]. The [redacted] was able to use this information to assess the FAB-T critical component suppliers and provide AFSPC with the results.

~~(FOUO)~~ As mentioned, a SBIRS GEO 5 and 6 ASICs list was included as Annex 3 to the SBIRS GEO 5 and 6 satellite production contract. The list identified the component, manufacturer's part number, part description, and supplier name for 58 ASICs. However, the SBIRS program office did not include the 58 ASICs as part of the SBIRS critical components list or include them in the requests for supplier threat assessments submitted to the [redacted].

[19] A commercial and Government entity code is a five-character identifier for companies doing business with the Federal Government that provides a standardized method of identifying a given facility at a specific location.

Supplier Threat Assessment Requests Not Prioritized

~~(FOUO)~~ The AFSPC did not prioritize criticality level I and II components in its requests to the [redacted] for supplier threat assessments. Prioritizing the list of criticality level I and II components as high, medium, or low allows the [redacted] to focus resources on the most important components.

DoD program protection guidance specifies that as part of the criticality analysis, DoD organizations should assess criticality 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.

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.

DoD program protection guidance specifies that the next step in the criticality analysis involves prioritization of the level I and II critical components for resources and attention. Specifically, DoD organizations should assign an overall priority level of high, medium, or low to each critical component based on a variety of factors, including the number of missions supported and whether the component is:

- a commercial off-the-shelf or developmental item;
- a new or legacy item;
- an integrated circuit and, if so, the type (for example, an ASIC); or
- specifically designed for military use.

~~(FOUO)~~ Our review of the SBIRS critical components lists found that the SBIRS program office did not prioritize the components as high, medium, or low. Instead, the SBIRS program office categorized all [redacted] critical components as high priority on supplier threat assessment requests submitted to the [redacted]. However, the critical components on the supplier threat requests ranged from complex assemblies containing ASICs and other logic-bearing components to commercial off-the-shelf switches and firewalls.

~~(FOUO)~~ The AFSPC needs to improve the accuracy of the requests for supplier threat assessments and require the prioritization of the critical components on the requests and the inclusion of all key information needed by the [redacted] to conduct the assessments.

Purchase of ASICs from DMEA-Accredited Suppliers Not Always Required

The AFSPC did not require the purchase of all ASICs from DMEA accredited suppliers. DoDI 5200.44 requires integrated circuit-related products and services to be procured from a trusted supplier using trusted processes accredited by the DMEA when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as ASICs). However, the AFSPC did not fully comply with this requirement.

As mentioned, a SBIRS GEO 5 and 6 ASICs list was included as ANNEX 3 to the SBIRS GEO 5 and 6 satellite production contract. The contract specified that for those ASICs listed in ANNEX 3, the "Trusted Product Flow" was not required.[20] The contract also requires the contractor to promptly notify the Government upon discovery of any heritage ASIC used in critical components or involving critical program information that were not listed in ANNEX 3. The contract defined heritage ASICs as those used on SBIRS engineering and manufacturing development and follow-on production programs, or other DoD military space applications that were also custom-designed, custom-manufactured, or tailored, for a specific DoD military end use. In response to our inquiries, SBIRS program office officials informed us that they were not aware of any waiver obtained to deviate from the DoDI 5200.44 DMEA requirements. SBIRS program office officials stated that their decision not to require the "Trusted Product Flow" was driven by a design and cost perspective; specifically, they wanted to use the same vendors and parts for the GEO 5 and 6 satellites that were used for the GEO 3 and 4 satellites.

The SBIRS GEO 5 and 6 satellite production contract specifies that the contractor shall implement the "Trusted Product Flow" requirements, as defined by the DMEA, for any new ASIC designs used in critical components or involving critical program information that were custom-designed, custom-manufactured, or tailored, for a specific DoD military end use. The contract also directed the prime contractor to submit any exceptions to "Trusted Product Flow" requirements for new ASIC designs for Government approval.

[20] The "Trusted Product Flow" are the requirements DMEA established for the trusted integrated circuit supplier program.

Although the "Trusted Product Flow" was not mandatory, the SBIRS GEO 5 and 6 production contract instructed the prime contractor to support the Government in determining the risk posture and potential mitigations for all 58 ASICs in accordance with a SBIRS GEO 5 and 6 ASIC supply chain management questionnaire. The SBIRS GEO 5 and 6 satellite production contract included the questionnaire as ANNEX 2. We requested the SBIRS program office to provide the completed questionnaires for all 58 ASICs and any resulting mitigations. The program office provided only three completed questionnaires; moreover, none of the part numbers identified on the questionnaires tied to the part numbers for the 58 ASICs in ANNEX 3. Consequently, the SBIRS program office did not comply with the DMEA accreditation requirement for the 58 ASICs and it could not provide evidence that it determined the risk posture and potential mitigations.

The AFSPC needs to determine the risk posture and potential mitigations for all ASICs not procured from a trusted supplier using trusted processes accredited by the DMEA.

Rigorous Test and Evaluation Capabilities Missing

~~(FOUO)~~ The AFSPC did not ensure the use of rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing [redacted]. The AFSPC included DoD SCRM-related requirements in the SBIRS GEO 5 and 6 satellite production contract but did not conduct independent reviews to verify contractor compliance. In addition, AFSPC program protection surveys did not address DoD SCRM requirements.

No Verification and Validation of Contract Requirements

The AFSPC included DoD SCRM-related requirements in the SBIRS GEO 5 and 6 satellite production contract but it did not conduct independent reviews to verify contractor compliance. DoDI 5200.44 requires DoD organizations to implement tailored acquisition strategies, contract tools, and procurement methods for critical components in applicable systems. AFPAM 63-113 requires Air Force organizations to ensure that contractual language requires contractors to participate in program protection. AFPAM 63-113 also requires Air Force organizations to provide suggested contractual language to meet DoD SCRM-related requirements.

The SBIRS GEO 5 and 6 satellite contract included DoD SCRM-related language requiring the prime contractor to:

- Identify all critical component vendors and manufacturers within the supply chain.

- Obtain all components from the original equipment manufacturer, original component manufacturer, or an authorized distributor.
- Notify the program office when not obtaining components from the original equipment manufacturer, original component manufacturer, or an authorized distributor and establish testing and verification requirements to assess and mitigate the component's counterfeit risk.
- Identify all integrated circuits containing higher-level logic that are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (ASICs, for example).
- Implement the "Trusted Product Flow" requirements, as defined by the DMEA, for the trusted integrated circuit supplier program for any new ASIC designs.
- Verify and update existing countermeasures and support identification of additional countermeasure recommendations as part of the SBIRS Program Security Working Group, including:[21]
  - The application of supply chain risk management best practices.
  - The processes to control access by foreign nationals to program information, including, but not limited to, system design information, DoD-unique technology, and software or hardware used to integrate commercial technology.
  - The processes and practices to ensure genuine information and communications technology will be employed and are levied upon subcontractors.
  - The process used to protect unclassified DoD information during developmental activities.
- Take the following preventative steps, at all levels of the respective supply chain, to commit suppliers to providing authentic material:
  - Establish measures to mitigate counterfeiting risks.
  - Manage residual risk throughout the life cycle.
  - Maintain traceability of parts origination and distribution.

~~(FOUO)~~ However, the AFSPC [redacted]. SBIRS program office officials

[21] AFSPC formed a Program Protection Working Group to focus on analysis and identification of SBIRS critical program information and critical components. The working group was a subset of a Systems Security Working Group, which assessed how threats affected SBIRS development and acquisition capabilities, and consisted of various program office, systems engineering, and cybersecurity subject matter experts.

(FOUO) informed us that they [redacted] but instead relied on the Defense Contract Management Agency (DCMA) because they were responsible for the administration of the SBIRS GEO 5 and 6 production contract.

(FOUO) DCMA officials responsible for the SBIRS contracts informed us that they [redacted]. DCMA officials stated that the AFSPC did not provide any specific quality-related instructions for them to conduct that type of work. In addition, DCMA officials informed us that their SBIRS product support team reviewed DCMA policy and was unable to identify a reference supporting the DoDI 5200.44 requirement to develop a strategy for managing the risk in the supply chain for integrated circuit-related products.

Program Protection Surveys Did Not Address DoD SCRM Requirements

SBIRS program office officials stated that they conducted program protection surveys on the prime contractor. However, the program protection surveys did not address DoD SCRM requirements. AFPAM 63-113 requires the program office to conduct a program protection survey on contractors and subcontractors to monitor countermeasure effectiveness and report compromises to critical program information and critical components. The policy specifies that the program office should design the survey to help limit the ability of adversaries to exploit vulnerabilities in critical program information and critical components.

Prior to this audit, the most recent SBIRS program protection survey was conducted in March 2016—it did not address DoD SCRM requirements; instead, it only addressed operations, information, and personnel security. Specifically, the survey included yes or no questions on topics such as completion of security training, disclosure of security awareness information, controls over safe combinations, end of day security checks, and personnel security clearances.

In February 2018, SBIRS program office officials informed us that they recognized the lack of SCRM requirements associated with the March 2016 program protection survey and that they completed another survey with the prime contractor. Specifically, SBIRS program office officials stated that they completed a program protection survey in November 2017 with the primary emphasis on program protection and SCRM.

(FOUO) The SBIRS program office provided us with the results of the November 2017 program protection survey in February 2018. However, we did not verify the information on the program protection survey because it was not brought to our attention until after we completed our audit fieldwork and had

~~(FOUO)~~ issued a discussion draft of this report. Our review of the survey results found that it primarily focused on security (personnel, information, computer, and physical) and security management and training. We also found that the survey results contained questions on the protection of critical program information and critical components and on managing the associated supply chain risks. However, the comments associated with each of the questions were limited and lacked supporting documentation, and there was no evidence of any [redacted] by the SBIRS program office.

For example, one survey question asked if critical program information and critical components are being protected as required. The associated comment only stated that training is included in the operation security training and buildings have access restrictions and there were no additional details or supporting evidence of any verification or validation.

~~(FOUO)~~ The AFSPC needs to ensure the use of rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing [redacted] and require establishment of verification and validation procedures for critical logic-bearing hardware, software, and firmware either independently or through delegation to the DCMA.

Other AFSPC Critical Systems also Revealed Concerns

In addition to our review of the SBIRS, we performed a limited review of three other AFSPC critical systems that revealed concerns similar to those found with SBIRS SCRM. These critical systems were the AFSCN, FAB-T, and GPS.

AFSCN Supply Chain Risk Management Concerns

We identified concerns pertaining to the AFSCN's change to the remote tracking station. AFSCN program office officials informed us that they were in the process of updating their PPP at the time of our review and they provided us a December 2016 update, which they included as Attachment 4 of the AFSCN PPP. The update consisted of the results of a criticality analysis and the associated critical components list for the change to the remote tracking station. Our review identified the following concerns.

~~(FOUO)~~ In the PPP update, the AFSCN program office noted that [redacted] critical hardware components and [redacted] critical software components should have been listed. However, the critical components list only contained [redacted] critical hardware and [redacted] critical software components. In addition, the AFSCN program office included level I and II critical components in its critical components list but did

(FOUO) not include level III or IV critical components. In response to our inquiries, AFSCN program office officials acknowledged errors with the critical component list but did not explain why the errors occurred.

(FOUO) The PPP update specified that the PPP working group developed the critical hardware and software lists in 2015 and identified candidates for submission to the [redacted] in 2016. However, at the time of our site visit in August 2017, AFSCN program office officials had not sent to the [redacted] the requests for supplier threat assessments. In addition, the AFSCN program office selected only a portion of its critical components as potential threat assessment candidates and did not provide information to explain their selection methodology.

The contract for the AFSCN's change to the remote tracking station, with a period of performance through December 31, 2020, did not include any language requiring the contractor to comply with DoD SCRM requirements. In addition, the AFSCN PPP update did not contain any verification or validation procedures to ensure compliance with DoD SCRM requirements.

FAB-T Supply Chain Risk Management Concerns

(FOUO) We identified concerns pertaining to the FAB-T production. FAB-T program office officials informed us that they were in the process of updating their PPP at the time of our review and did not provide an estimated completion date. FAB-T program office officials also informed us that they [redacted]. The FAB-T program office explained that they [redacted].[22] In addition, the FAB-T program office [redacted].

GPS Supply Chain Risk Management Concerns

(FOUO) We identified concerns pertaining to the GPS next generation operational system. The GPS program office officials informed us that they [redacted].[23]

[22] (FOUO) Our limited review of the FAB-T SCRM did not [redacted].
[23] (FOUO) Our limited review of the GPS SCRM did not [redacted].

~~(FOUO)~~ In addition, we were unable to reconcile the GPS components on the requests for supplier threat assessments submitted to the [redacted] with the GPS critical components list. We also identified concerns with the completeness and accuracy of the GPS critical components list. The GPS program office informed us that they were researching the issues we identified and that research was ongoing at the conclusion of our audit.

The GPS PPP contained a detailed section on supply chain risk management and described how GPS has or plans to comply with the DoD SCRM requirements. The GPS next generation operational system contract contained minimal DoD SCRM requirements; however, it included a requirement that the contractor shall develop and maintain a program protection implementation plan to ensure program compliance with the Government PPP. Our review of the contractor's program protection implementation plan for the GPS next generation operational system found that it did not address the DoD SCRM requirements outlined in the GPS PPP. For example, our review of the contractor's program protection implementation plan found that it did not mention SCRM, DMEA, critical components, or DoDI 5200.44, which were all included in the GPS PPP.

The AFSPC needs to conduct a detailed review of the SCRM for the AFSCN, FAB-T, and GPS programs, and all other programs deemed critical to the AFSPC, to ensure compliance with DoD SCRM policy.

Adversaries Have Opportunity to Infiltrate the AFSPC Supply Chain

The 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 the DoD's warfighting mission capability will be impaired due to vulnerabilities in system design, or sabotage 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 AFSPC provides adversaries the opportunity to infiltrate its supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of critical components.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Air Force Space Command Commander develop a plan of action with milestones for the Space Based Infrared System to comply with DoD supply chain risk management policy. The plan should establish controls and oversight and require Air Force Space Command personnel to develop internal procedures or establish contract requirements to:

a. Improve the accuracy of the critical components list to manage risks to the Space Based Infrared System throughout its life cycle and require the identification of all critical logic-bearing hardware, software, and firmware, and the associated suppliers. The criticality analysis should include the 58 application specific integrated circuits from the geosynchronous earth orbit satellite 5 and 6 production contract.

AFSPC Comments

The AFSPC SMC Vice Commander, responding for the AFSPC Commander, agreed and stated that the AFSPC SMC Remote Sensing Systems Directorate would conduct a criticality analysis for the GEO 5 and 6 to accurately identify and compile a parts list for all critical components by December 31, 2018.

Our Response

Comments from the Vice Commander addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved but will remain open. We will close this recommendation once we verify that an accurate parts list for all critical components has been created.

b. ~~(FOUO)~~ Improve the accuracy of the requests for supplier threat assessments and require the prioritization of the critical components on the requests and the inclusion of all key information needed by the [redacted] to conduct the assessments.

AFSPC Comments

~~(FOUO)~~ The AFSPC SMC Vice Commander, responding for the AFSPC Commander, agreed and stated that the AFSPC SMC Remote Sensing Systems Directorate will produce an updated critical components list that includes the break down for all logic bearing devices to the component level and provide the [redacted] with a Request for Information that includes all key information needed for the [redacted] to conduct the assessment by January 31, 2019.

Our Response

Comments from the Vice Commander addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved but will remain open. We will close this recommendation once we verify that the accuracy of the requests for supplier threat assessments have been improved and include prioritization.

c. Determine the risk posture and potential mitigations for all application specific integrated circuits not procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity.

AFSPC Comments

~~(FOUO)~~ The AFSPC SMC Vice Commander, responding for the AFSPC Commander, agreed and stated that the risk posture and potential mitigations will be identified upon completion of the [redacted] threat assessment and receipt of [redacted] reports by March 31, 2020.

Our Response

Comments from the Vice Commander addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved but will remain open. We will close this recommendation once we verify that the risk posture and potential mitigations have been determined for all application specific integrated circuits not procured from a trusted supplier.

d. ~~(FOUO)~~ Ensure the use of rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing [redacted] and require establishment of verification and validation procedures for critical logic-bearing hardware, software, and firmware either independently or through delegation to the Defense Contract Management Agency.

AFSPC Comments

The AFSPC SMC Vice Commander, responding for the AFSPC Commander, agreed and stated that the AFSPC SMC Remote Sensing Systems Directorate, in coordination with AFSPC/A2/3/6M, is incorporating modernized requirements and verification processes to ensure the security of the program by December 31, 2019.[24] The Vice Commander stated that verification and validation

[24] AFSPC/A2/3/6M represents the AFSPC Security and Mission Assurance Division under the Integrated Air, Space, Cyberspace, and Intelligence, Surveillance, and Reconnaissance Operations Directorate.

of these requirements will be accomplished through program protection surveys, independent third-party assessors, and developmental and operational tests of the existing SBIRS system and GEO 5 and 6.

Our Response

Comments from the Vice Commander addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved but will remain open. We will close this recommendation once we verify that the modernized requirements and verification processes have been incorporated to ensure the security of the program.

Recommendation 2

We recommend that the Air Force Space Command Commander conduct a detailed review of the supply chain risk management for the Air Force Satellite Control Network, Family of Advanced Beyond Line-of-Sight Terminals, and Global Positioning System programs, and all other programs deemed critical to the Air Force Space Command, to ensure compliance with DoD supply chain risk management policy. If deficiencies are identified, Air Force Space Command officials must develop a plan of action with milestones to correct the deficiencies.

AFSPC Comments

The AFSPC SMC Vice Commander, responding for the AFSPC Commander, agreed and stated that his staff will provide resources and hard schedules to conduct a SCRM review of AFSCN, FAB-T, GPS, and other programs deemed critical to AFSPC in accordance with DoDI 5200.44 by December 31, 2018. In addition, the Vice Commander stated that additional measures to include program protection awareness and training would also be executed to ensure that program offices effectively implement their SCRM program in compliance with DoD program protection policies.

Our Response

Comments from the Vice Commander addressed all specifics of the recommendation. Therefore, the recommendation is resolved but will remain open. We will close this recommendation once we verify that the programs have been reviewed to comply with DoD policy and a plan of action exists to correct deficiencies that are identified.

Appendix A

Scope and Methodology

We conducted this performance audit from June 2017 through May 2018 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 specific matters the House Armed Services Committee requested this audit focus on, we only reviewed the AFSPC's SCRM processes. We did not review the prime contractors and subcontractors SCRM processes for the AFSPC critical systems.

We interviewed officials from the AFSPC Headquarters and the AFSPC SMC. We conducted interviews with SBIRS program office officials.

We obtained and analyzed AFSPC documentation on the SBIRS to include:

- contract documentation on the GEO 5 and 6 satellite production and ground segment upgrade;
- PPPs and critical component lists;
- ~~(FOUO)~~ requests for supplier threat assessments submitted to the [redacted] for critical components;
- the prime contractor's system security plan;
- lists of software and firmware for the GEO 5 and 6 satellite production and the ground segment upgrade; and
- AFSPC SMC program protection survey dated March 3, 2016.

We interviewed DCMA officials responsible for oversight of the SBIRS contracts to determine if they performed verification and validation of DoD SCRM-related contract requirements.

~~(FOUO)~~ We conducted a detailed review of the SBIRS criticality analysis. We reviewed a listing of [redacted] critical hardware items for the SBIRS GEO 5 and 6 satellites and the SBIRS ground segment upgrade contained in the SBIRS Enterprise PPP, version 5.0, June 12, 2017. In addition, we obtained lists of software and firmware for the SBIRS GEO 5 and 6 satellites and the SBIRS ground segment upgrade.

We reviewed the critical hardware components to determine if they represented an assembly or a supporting logic-bearing component. We also determined whether AFSPC could provide evidence that it performed independent verification and validation of critical component suppliers to ensure compliance with DoD SCRM requirements.

We reviewed all software and firmware programs for the SBIRS GEO 5 and 6 satellites and ground segment upgrade to determine whether the AFSPC SMC could identify by name and nationality all developers involved.

We performed a limited review of the AFSCN, FAB-T, and GPS SCRM. We also conducted interviews with program office officials and obtained and analyzed AFSPC documentation on these programs to include:

- contract documentation on the AFSCN remote tracking station block change, FAB-T production, and the GPS next generation operational system;
- PPPs and critical component lists;
- ~~(FOUO)~~ requests for supplier threat assessments submitted to the [redacted] for critical components; and
- FAB-T and GPS contractor program protection implementation plans.

We compared AFSPC documentation to the DoD and Air Force policies, standards, and best practices, including:

- DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 2, Effective July 27, 2017);
- Deputy Assistant Secretary of Defense, Systems Engineering, "Program Protection Plan Outline and Guidance," July 2011;
- Deputy Assistant Secretary of Defense for Systems Engineering Briefing, "DoD Comprehensive Program Protection Planning," February 27, 2011;
- Defense Acquisition Guide, Chapter 13 "Program Protection," May 15, 2013; and
- AFPAM 63-113, "Program Protection Planning For Life Cycle Management," October 17, 2013.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, the GAO and the DoD OIG issued two reports discussing DoD SCRM.

Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

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 to the Government-Industry Data Exchange Program from fiscal years 2011 through 2015; these reports were 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 have limited the program's effectiveness as an early warning system for identifying counterfeit parts.
>
> 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.

DoD OIG

Report No. DODIG-2017-076, "The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System," April 2017

> 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 the DoD's supply chain risk

management policy for the Ground-based Midcourse Defense System. This occurred because the Missile Defense Agency did not take the necessary steps to establish the controls and oversight necessary to maintain an accurate critical components list to manage risks to the system throughout its life cycle and prioritize the list for supplier threat assessment requests to vet critical component suppliers. Moreover, the Missile Defense Agency did not identify the suppliers of all critical components or use rigorous test and evaluation capabilities to detect vulnerabilities within critical components.

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.

Appendix B

House Armed Services Committee Request and Our Response

House Armed Services Committee Request

Supply Chain Security of Strategic Capabilities

The committee is aware of the report submitted by the 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 DoD OIG 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, AFSPC, the nuclear command and control system, and a delivery system or platform for U.S. nuclear weapons. Furthermore, the committee directs the DoD OIG 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 DoD OIG 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 DoD OIG'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 AFSPC did not conduct actual forensic evaluations of the supply chain for the SBIRS System with regard to DoD SCRM requirements. The AFSPC relied on the representation of the SBIRS prime contractor and we found no evidence of any independent verification and validation of the source of supply for each critical component and subcomponent.
2. The AFSPC was unable to provide by name and nationality the developers involved with SBIRS critical software, firmware, or chip design.
3. The AFSPC did not perform due diligence on SBIRS second- and third- tier suppliers in regards to DoD SCRM requirements.

Management Comments

Air Force Space Command

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS SPACE AND MISSILE SYSTEMS CENTER (AFSPC)
LOS ANGELES AIR FORCE BASE, CALIFORNIA

MEMORANDUM FOR HQ AFSPC/CC JUN 29 2018

FROM: SMC/CV
483 North Aviation Boulevard
El Segundo CA 90245-2808

SUBJECT: Management Comments to DoD-IG Draft Report, Air Force Space Command Supply Chain Risk Management of Strategic Capabilities (Project No. D2017-D000AG-0155.000)

1. In accordance with AFI 65-402, para 3.3, Air Force comments, I am providing the following management comments to DOD-IG draft report recommendations:

Recommendation 1. The Commander, Air Force Space Command, develop a plan of action with milestones for the Space Based Infrared System (SBIRS) to comply with DoD supply chain risk management (SCRM) policy. The plan should establish controls and oversight and require Air Force Space Command personnel to develop internal procedures or establish contract requirements to:

a. Improve the accuracy of the critical components (CC) list to manage risks to the SBIRS throughout its life cycle and require the identification of all critical logic-bearing hardware, software, and firmware, and the associated suppliers. The criticality analysis (CA) should include the 58 Application Specific Integrated Circuits (ASIC) from the geosynchronous earth orbit satellite (GEO) 5 and 6 production contract.

Management Comments: SMC concurs with the recommendation. Until recently, there was no higher-level guidance that specified identification of CC. Now that guidance is in place, additional clarification is needed to cover programs that already completed the CA process. The Remote Sensing Systems Directorate (SMC/RS) has been working with the Engineering Directorate (SMC/EN) to improve the process and guidance of the SBIRS Enterprise Program Protection Plan, which includes GEO 5/6. SMC/RS will conduct a CA for GEO 5/6 to accurately identify and compile a parts list for all CC. Estimated completion date: 31 Dec 18

b. ~~(FOUO)~~ Improve the accuracy of the requests for supplier threat assessments and require the prioritization of the CCs on the requests and the inclusion of all key information needed by the [redacted] to conduct the assessments.

Management Comments: SMC concurs with the recommendation. An area to consider is the creation, review, analysis and approval process for a program protection plan (PPP) which incorporates SCRM and the resources required. Current assessments lack information needed to support timely SCRM activities. No matter what language is adopted into the contracts or

INTEGRITY, SERVICE, EXCELLENCE

Air Force Space Command (cont'd)

updates done to the PPP, without specific knowledge of where focus needs to be placed, it is difficult to effectively update legacy contracts in a fiscally constrained environment.

SMC/RS will produce an updated CC list that includes the break down for all logic bearing devices to the component level. We will provide the [redacted] with a Request for Information that includes all key information needed for the [redacted] to conduct the assessment. Estimated completion date: 31 Jan 19

c. Determine the risk posture and potential mitigations for all ASICs not procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity.

Management Comments: SMC concurs with the recommendation. SMC/RS continues working with members from SMC/EN to integrate SCRM into the organization-wide risk management process, in accordance with NIST SP 800-161. The risk posture and potential mitigations will be identified upon completion of the [redacted] threat assessment and receipt of [redacted] reports. Estimated completion date: 31 Mar 20

d. Ensure the use of rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing [redacted] and require establishment of verification and validation procedures for critical logic-bearing hardware, software, and firmware either independently or through delegation to the Defense Contract Management Agency.

Management Comments: SMC concurs with the recommendation. SMC/RS, in coordination with AFSPC/A2/3/6M, is incorporating modernized requirements and verification processes to ensure the security of the program. Verification and validation of these requirements will be accomplished via program protection surveys, independent third party assessors, and developmental and operational tests of the existing SBIRS system and GEO 5/6. Estimated completion date: 31 Dec 19

Recommendation 2. The Commander, Air Force Space Command, conduct a detailed review of the SCRM for the Air Force Satellite Control Network, Family of Advanced Beyond Line-of-Sight Terminals, and Global Positioning System programs, and all other programs deemed critical to AFSPC, to ensure compliance with DoD SCRM policy. If deficiencies are identified, AFSPC officials must develop a plan of action with milestones to correct the deficiencies.

Management Comments: SMC concurs with the recommendation. SMC/EN has been proactively involved in the review and validation of CCs. Prior to the IG report, my functional staff developed and proposed an event schedule to assist programs with criticality analyses of program systems. My staff will provide resources and hard schedules to conduct a SCRM review of AFSCN, FAB-T, GPS, and other programs deemed critical to AFSPC IAW with DODI 5200.44. Additional measures to include program protection awareness and training will also be executed to ensure that program offices effectively implement their SCRM program in compliance with DOD Program Protection policies. Estimated completion date: 31 Dec 18

Air Force Space Command (cont'd)

2. For questions, please contact [redacted], Enterprise Protection, SMC/ENX at [redacted] or [redacted], SMC Audit Liaison, SMC/FMW at [redacted].

PHILIP A. GARRANT
Brigadier General, USAF
Vice Commander

Acronyms and Abbreviations

AFSCN	Air Force Satellite Control Network
AFSPC	Air Force Space Command
ASIC	Application Specific Integrated Circuit
DCMA	Defense Contract Management Agency
~~(FOUO)~~	[redacted]
DMEA	Defense Microelectronics Activity
DoDI	DoD Instruction
DSP	Defense Support Program
FAB-T	Family of Advanced Beyond Line-of-Sight Terminals
GAO	Government Accountability Office
GEO	Geosynchronous Earth Orbit
GPS	Global Positioning System
HEO	Highly Elliptical Orbit
OIG	Office of Inspector General
PPP	Program Protection Plan
SBIRS	Space Based Infrared System
SCRM	Supply Chain Risk Management
SMC	Space and Missile Systems Center

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.

Commercial Off-The-Shelf. Technology products and systems that are ready made and available for sale, lease, or license, including proprietary and open source software products. A commercial off-the-shelf item is offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.

Critical Component. A component that is or contains information and communications technology, including hardware, software, and firmware; whether custom, commercial, or otherwise developed, and that delivers or protects mission-critical functionality of a system or that, 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; breakdown 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).

Mission-Critical Functions. Any function that 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.

Program Protection Implementation Plan. A plan the contractor uses to document the contractor's measures to protect critical program information and critical components at their facilities and supplier locations consistent with the Government's program protection plan.

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).

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/.

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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