

---

November 24, 2003

---



# Acquisition

Development Testing of Space  
Based Infrared System Mission-  
Critical Software  
(D-2004-022)

---

Department of Defense  
Office of the Inspector General

---

*Quality*

*Integrity*

*Accountability*

### **Additional Copies**

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at [www.dodig.osd.mil/audit/reports](http://www.dodig.osd.mil/audit/reports) or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

### **Suggestions for Future Audits**

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)  
Inspector General of the Department of Defense  
400 Army Navy Drive (Room 801)  
Arlington, VA 22202-4704

### **Defense Hotline**

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to [Hotline@dodig.osd.mil](mailto:Hotline@dodig.osd.mil); or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

### **Acronyms**

AFI	Air Force Instruction
CA	Certifying Authority
DAA	Designated Approval Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
IATO	Interim Authority to Operate
IHC	Interim Highly Elliptical Orbit Capability
IPT	Integrated Product Team
IRT	Independent Review Team
SSAA	System Security Authorization Agreement
SBIRS	Space Based Infrared System
SEIT	System Engineering Integration Team
SMM	System Maturity Matrix



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

November 24, 2003

MEMORANDUM FOR AIR FORCE PROGRAM EXECUTIVE OFFICER SPACE

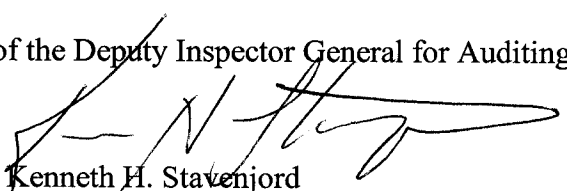
SUBJECT: Report on Development Testing of Space Based Infrared System  
Mission-Critical Software (Report No. D-2004-022)

We are providing this report for review and comment. We considered management comments on a draft of this report in preparing the final report.

The System Program Director, Space Based Infrared Systems, Space and Missile Systems Center comments were responsive to the intent of the recommendations. However, we request that the System Program Director provide additional information showing completion of Recommendations A. and B. by January 26, 2004.

We appreciate the courtesies extended to the staff. Questions on the evaluation should be directed to Mr. Kenneth H. Stavenjord at (703) 604-8952 (DSN 664-8952) or Mr. Peter C. Johnson at (703) 604-9601 (DSN 664-9601). See Appendix C for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

  
Kenneth H. Stavenjord  
Program Director, Audit Followup  
and Technical Support Directorate

## Office of the Inspector General of the Department of Defense

Report No. D-2004-022  
(Project No. D2002PT-0206)

November 24, 2003

### Development Testing of Space Based Infrared System Mission-Critical Software

#### Executive Summary

**Who Should Read This Report and Why?** Acquisition officials, program managers, and software managers who are responsible for the development and test of software should read this report. It explains steps for effective government oversight of development testing as well as information assurance requirements for developmental test information systems.

**Background.** This report is one of a series, which evaluate the adequacy of development testing of mission-critical software in selected weapon systems. The previous report “Development Testing of Prophet Mission-Critical Software,” (D-2003-051) January 22, 2003, reviewed software development testing in the Army Prophet system. This report reviews the testing of mission-critical software contained in the Air Force Space Based Infrared System High.

The Space Based Infrared System (SBIRS) High is a constellation of high altitude satellites with a ground system. It is the successor to the Defense Support Program with the mission to provide missile warning, missile defense, technical intelligence, and battle space characterization. Development of SBIRS High is in two increments. Increment 1 achieved initial operational capability in December 2001. Increment 2 is currently in development and is scheduled to be complete in FY 2010. Estimated cost for Increments 1 and 2 is \$4.86 billion.

During the fall of 2001, the SBIRS Program Director reported a likely Nunn-McCurdy Breach. On December 31, 2001, the Secretary of the Air Force notified Congress that the program had a cost breach. Because of the breach, the Under Secretary of Defense for Acquisition, Technology, and Logistics performed program reviews. In addition, during the time of the review the Under Secretary of the Air Force directed that the program office remove the total system performance responsibility clause from the contract. Based on those efforts the program was recertified on May 3, 2002.

**Results.** The program office has not implemented effective requirement flow control by tracking the technical progress of requirements, assumed responsibility for approving all critical test plans and reports and established a metric for annually reporting extended developmental testing. The Designated Approval Authority inappropriately issued an Interim Authority To Operate for the Interim Highly Elliptical Orbit Capability and annually plans to issue one until initial operational capability scheduled for FY 2010.

Without effective management and oversight of development testing, Space Based Infrared System High is at risk of repeating problems previously identified by the Independent Review Team during program recertification, which included inadequate

management of requirements, insufficient oversight of system development and lack of meaningful metrics. The System Program Director, Space Based Infrared System, Space and Missile Systems Center should implement a System Maturity Matrix or similar tool, assume sign off responsibility for all critical test plans and reports, and provide to key decisions makers an annual interim test report documenting extended developmental testing. For details of this recommendation, see finding A of this report.

Validation of system security features for the Interim Highly Elliptical Orbit Capability as required by the Defense Information Technology Security Certification and Accreditation Process were incomplete. By not validating the correct implementation and operation of system security features, the correctness of Interim Highly Elliptical Orbit Capability test data is in doubt, and its capability to test, assess, and support Space Based Infrared System is questionable. The Certifying Authority should ensure all validation tasks, which include security test and evaluation and penetration test are complete. The Designated Approval Authority should then accredit, withhold accreditation, or issue an Interim Authority To Operate. In addition, the Program Director should remove the reaccreditation requirement for an annual Interim Authority To Operate from the System Security Authorization Agreement and plan to have the Interim Highly Elliptical Orbit Capability achieve full accreditation within the next 12 months. For details of this recommendation, see finding B of this report.

**Management Comments and Evaluation Response.** The System Program Director, SBIRS, Space and Missile Systems Center agreed to develop a System Maturity Matrix, and stated that the program office approves all critical system test plans and reports. The System Program Director agreed to implement an annual interim test report during extended developmental testing. In addition, the System Program Director agreed to complete security testing for the Interim Highly Elliptical Orbit Capability – now known as the Interim Test Center, and have the Designated Approval Authority verify that all validation tasks are completed before issuing an accreditation decision. The System Program Director also agreed to discontinue the use of the Interim Authority to Operate as a “recurring, routine exercise,” but anticipated using an Interim Authority to Operate for an additional 2 years. A discussion of management comments is in the Findings section of the report and the complete text is in the Management Comments section.

The System Program Director comments were responsive. However, we require further detail in order to determine if the actions are sufficient. Specifically, the System Program Director agreed to develop a System Maturity Matrix, but did not explain how the System Maturity Matrix will track requirements to effectivities and test results. We request that the System Program Director provide a description of the System Maturity Matrix explaining how it will track requirements to effectivities and test results. In addition, the System Program Director stated that the program office approves all critical system test plans and reports but did not explain whether the critical test plans and reports we identified, that did not require government approval, were included. We request that the System Program Director provide detailed information on the government approval process for the critical test plans and reports that we identified as not requiring government approval. As a final point, the System Program Director stated that security testing for the Interim Test Center is planned for completion in December 2003, and the use of the Interim Authority to Operate as a re-accreditation requirement will be discontinued. We request that the System Program Director provide the updated Interim Test Center System Security Authorization Agreement containing the summary of the Interim Test Center security test results as well as the plan to achieve full accreditation. We request that the documents be provided by January 26, 2004.

# Table of Contents

---

<b>Executive Summary</b>	i
<b>Background</b>	1
<b>Objectives</b>	3
<b>Findings</b>	
A. Management and Oversight of Development Testing	4
B. Interim Highly Elliptical Orbit Capability Temporary Authority to Operate	13
<b>Appendixes</b>	
A. Scope and Methodology	21
Management Control Program Review	22
B. Prior Coverage	24
C. Definitions of Technical Terms	25
D. Report Distribution	27
<b>Management Comments</b>	
Department of the Air Force	29

---

## Background

This report is one of a series, which evaluate the adequacy of development testing of mission-critical software in selected weapon systems. The previous report “Development Testing of Prophet Mission-Critical Software,” (D-2003-051) January 22, 2003, reviewed software development testing in the Army Prophet system. This report reviews the testing of mission-critical software contained in the Air Force Space Based Infrared System High.

**Space Based Infrared System.** The Space Based Infrared System (SBIRS) High is a constellation of high altitude satellites with a ground system and is the successor to the Defense Support Program with the mission to provide missile warning, missile defense, technical intelligence, and battle space characterization. SBIRS High consists of a space segment and a ground segment and is being developed in two increments. The space segment will employ overhead non-imaging infrared satellite systems in geosynchronous and highly elliptical orbits. The ground segment consolidates the Defense Support Program ground assets to support continuing space operations and provides the capabilities to support transitions, launch, and mission operations for the SBIRS High space segment. Increment 1, which consolidated the current ground assets and is currently supporting Defense Support Program operations, achieved initial operational capability in December 2001. Increment 2, which replaces the Defense Support Program satellites with the SBIRS High constellation, adds capability to the ground segment. Increment 2 is in development and is scheduled to be complete in FY 2010. Estimated cost for Increments 1 and 2 is \$4.86 billion. The program office has stated that the cost of SBIRS High software is \$892.3 million.

**Program Recertification.** During the fall of 2001, the SBIRS Program Office performed an estimate at completion analysis because of questionable cost and schedule parameters in the Acquisition Program Baseline. The analysis reported a potential research, development, test and evaluation cost growth in excess of \$2 billion and schedule delays of 18-24 months. As a result, the System Program Director reported a likely Nunn-McCurdy Breach. On December 31, 2001, the Secretary of the Air Force notified Congress that the SBIRS High program had a cost breach. Because of the breach, the Under Secretary of Defense for Acquisition, Technology, and Logistics conducted program reviews, which included an Independent Review Team (IRT). In addition, during the time of the review, the Under Secretary of the Air Force directed the program office to remove the total system performance responsibility clause from the contract. Based upon the need of the program for national security, a revised acquisition strategy, implementation of IRT recommendations, and the removal of the total system performance responsibility, the program was recertified on May 3, 2002.

**Development Testing Objectives.** Two objectives of development testing are to verify system compliance to specifications and to demonstrate system readiness to enter operational test and evaluation. Verification of SBIRS ground software requirements is done through a series of test activities called the software development lifecycle. During the development lifecycle, code and unit test, development integration test, and component integration test progressively verify

---

that the software meets the design, performs correctly, and integrates with other components. In the course of component integration testing, ground segment design document qualification and segment verification tests are performed to verify software requirement specifications and ground segment requirements. Once segment verification tests are complete, the System Engineering Integration Team accepts the ground segment software and performs a series of system level tests. For Increment 2, system level tests verify that the integrated ground and space segments meet SBIRS High component specifications. Successful completion of system level tests ensures system intersegment interface compatibility and system operational capability.

**Certification and Accreditation of Development Sites.** During the evaluation, we reviewed the status of information assurance for SBIRS development sites used for software development. There are three contractor development sites used for development, integration, and testing of SBIRS ground segment, space segment, and system software. The locations of the contractor development sites are Sunnyvale, California; Azusa, California; and Boulder, Colorado. DoD 5220.22-M National Industrial Security Program Operating Manual applies to all contractor information systems that process classified information and is used for contractor information system certification and accreditation. The Defense Security Service oversees the certification and accreditation of all three contractor development sites and ensures that they are in compliance with DoD policy. According to DoD 5220.22-M, in order for a contractor development facility to be certified and accredited it must have an Automated Information System Security Plan and an accreditation letter approved by a cognizant security agency. During our review, we were able to verify that an Automated Information Security Plan and a Defense Security Service accreditation letter exist for the Sunnyvale and Azusa contractor development sites. We requested the Automated Information System Security Plan and accreditation letter for the Boulder site during our visit to Boulder in October 2002. In February 2003, we received an Automated Information System Security Plan for Boulder dated February 3, 2003. In addition, in February 2003 the Defense Security Service provided us an Interim Authority to Operate (IATO) for Boulder. An IATO gives permission for an information system to operate before formal certification and accreditation and the signing of the accreditation letter. The date of the IATO was February 24, 2003. We contacted the Defense Security Service regional representative and discussed the discrepancy concerning the dates of our request and the issuance of the Boulder Automated Information System Security Plan and IATO. The Defense Security Service representative told us that the Boulder facility has been certified for 10 years and that the IATO was issued in February 2003 in order to meet new DoD 5220.22-M requirements. We also met with the Defense Security Service Assistant Deputy Director for Operations who told us that they plan to issue a new IATO because the current one is based on old requirements. In addition, DSS provided a synopsis of their oversight of the Boulder site and a summary of the different equipment configurations used since the facility became operational in 1982.



---

## **Objectives**

The overall objective of our evaluation was to review issues concerning development testing and evaluation of SBIRS High mission-critical software. Specifically, we evaluated the completeness and adequacy of the testing to include planning, executing, and reporting of two ground-segment software domains: Telemetry, Tracking, and Commanding; and Mission Processing. We also reviewed specific areas during SBIRS development testing concerning information assurance, interface and interoperability testing, and computer test resources.

---

## **A. Management and Oversight of Development Testing**

The program office has not implemented effective requirement flow control by tracking technical progress of user and system requirements to test results and effectivity milestones, assumed approval responsibility for all critical test plans and reports, and established a meaningful metric for key decision makers by annually reporting extended development testing. Those conditions occurred because the program office has not implemented management and oversight requirements specified in Air Force Instruction 99-101, "Developmental Test and Evaluation." Specifically, the program office does not have a System Maturity Matrix or an equivalent management tool used to track the program's technical progress and risks, the program office does not sign off on all critical test plans and reports, and the program office has not planned for the issuance of annual interim test reports during extended developmental testing. As a result, without effective management and oversight of development testing, the \$4.86 billion program is at risk of repeating problems previously identified during program recertification, which included inadequate management of requirements, insufficient oversight of system development, and lack of meaningful metrics.

### **Space Based Infrared System Program Recertification**

Space Based Infrared System (SBIRS) High is in the Engineering and Manufacturing Development Phase of the program. Since the contract award in 1996, the program has experienced technical difficulties, schedule delays, and cost increases. Because of questionable cost and schedule parameters in the Acquisition Program Baseline, the SBIRS Program Office performed an Estimate at Completion analysis. The analysis disclosed a potential research development test and evaluation cost growth in excess of \$2 billion and schedule delays of 18-24 months. As a result, the System Program Director reported a likely Nunn-McCurdy Breach. On December 31, 2001, the Secretary of the Air Force notified Congress that the SBIRS High program had a Nunn-McCurdy cost breach. Because the breach involved a program acquisition cost unit above the 25 percent threshold for SBIRS High, the Defense Acquisition Executive was required to certify to Congress that the program is essential to national security, there are no alternatives that provide the same capability at less cost, new costs are reasonable, and program management is adequate to control costs.

In order to provide necessary information for program recertification, the Under Secretary of Defense for Acquisition, Technology, and Logistics performed program reviews between the period of December 2001 and April 2002. Part of those reviews included an assessment of the program by an Independent Review Team (IRT). The IRT identified a number of deficiencies in the program, such as improper control mechanisms for the management of requirements; circumvention of responsibilities while the total system performance responsibility clause was in place, and the lack of meaningful metrics for determining technical progress.

---

The IRT proposed recommendations correcting the deficiencies. (IRT Summary), (IRT pg 33-40) At the same time, the Under Secretary of the Air Force also directed the program office to remove the total system performance responsibility clause from the contract. The program manager removed the clause.

The Defense Acquisition Executive completed the Nunn-McCurdy certification activities and an acquisition decision memorandum documenting certification also directed a revised acquisition strategy be approved by the end of August 2002. Approval of the revised acquisition strategy included the implementation of the IRT recommendations.

## **Requirements for Management Oversight of Development Testing**

**Air Force Instruction 99-101, “Developmental Test and Evaluation,” November 1, 1996.** Air Force Instruction (AFI) 99-101 provides mandatory procedures for the management of development test and evaluation programs on systems, subsystems, and components and it describes planning, conducting, and reporting cost-effective development test and evaluation to support acquisition and sustainment program decisions and actions throughout a system’s life cycle. AFI 99-101 requires that all acquisition programs, with the exception of programs in production that have met all of their user requirements, require a System Maturity Matrix (SMM). The SMM is an acquisition management tool used to aid in tracking a program’s technical progress and risk. SMM links user requirements, allocated requirements, and system specifications to expected test results to be achieved over time and provides critical technical and operational characteristics that will be assessed at major decisions or event milestones. The instruction states that the greater reliance on contractors for testing, the greater the need for knowledgeable government officials, and that the system manager along with the responsible test organization will approve all test plans and reports and will oversee contractor testing. In addition, the instruction states that when a program has an extended test phase, the instruction requires that the responsible test organization provide annual interim test reports.

**Air Force Manual 99-113, “Space Systems Test and Evaluation Process Direction And Methodology for Space System Testing,” May 1, 1996.** Air Force Manual 99-113 provides the Space Systems Test and Evaluation Process for use by program managers, test engineers, test organization personnel, major command headquarters staffs, and others regardless of command level, involved in Space Systems Test and Evaluation. Nonuse of the process is by exception only. The process includes the use of an SMM. The manual states that during test definition the SMM should be a primary reference for understanding what the expected capabilities and levels of performance of the system are to be at the time of the test, and that during tracking and reporting of cumulative test results the tester should relate test objectives to documented user requirements and SMM interim values. The manual requires that in order to measure system progress toward meeting user needs, test program results shall provide a clear picture of system maturity toward meeting the user’s documented requirements and that

---

decision makers need test results to determine whether to grant programs approval to proceed through each milestone. The manual also states that an annual test process summary is to be generated by the program office, which will record all Development Test and Evaluation and Operational Test and Evaluation accomplished, key test process decisions, test and evaluation deficiencies, and identified risk areas. This document can be included in the annual interim test report.

## **Tracking Technical Progress of User and System Requirements to Test Results and Effectivity Milestones**

The program office has not implemented effective requirement flow control by tracking development of the SBIRS High ground segment software as it relates to user requirements, and by tracking technical progress of user and system requirements to test results and effectivity milestones. In particular, the program office does not have a SMM or an equivalent tool. Such a tool would permit the program manager to link user requirements and system specifications to ground segment software requirements test results, and permit the program manager to track the technical progress of requirements by mapping ground segment software requirements to software increments, and high component specifications to effectivity milestones. In addition, the SMM would allow the program manager to trace back test results from software and system tests to user requirements.

**Requirements Process.** SBIRS High user requirements flow down to SBIRS High component specifications, then to ground segment requirements, and finally to software requirement specifications. The Systems Engineering Integration Team (SEIT) maintains traceability of high component specifications to ground segment requirements in the Modified Design Compliance Matrix. The Modified Design Compliance Matrix provides the basis for the Requirements Verification Ledger. The Requirements Verification Ledger identifies each high component specification requirement to be verified during testing as well as the approach, method, criteria, and status. The ground segment Integrated Product Team (IPT) maintains traceability of ground segment requirements to software requirement specifications in the ground segment design document. The ground segment software IPTs use the Requirements Traceability and Management tool for documenting requirements, traceability, and test verification. Part of the Requirements Traceability Management tool is the Requirement Verification Planning tool, which contains the verification method, approach, and a completeness check for each requirement. SEIT personnel are involved in final Ground Segment level tests to ensure that the Ground Segment is ready for site installation and system level test.

**Tracking Requirements to Test Results.** The ground segment test report documents test results for ground segment software testing. The test results are mapped to ground segment requirements. The SEIT uses those results in order to determine if the ground segment is ready for integration and system level testing. Before a software increment undergoes ground segment testing, it is developed

---

and tested by code and unit test, development integration test, component integration test and ground segment design document verification test. Each of those activities progressively verifies that the software meets the design, performs correctly, and integrates successfully with other hardware and software components. The program manager does not have a tool which would link software requirements tested back to high component specifications or user requirements and permit analysis of software maturity and development progress.

**Tracking Requirements to Effectivity Milestones.** SBIRS High is currently in Engineering and Manufacturing Development Phase. Delivery of ground software is in blocks, with each block increasing mission utility. During our evaluation, we reviewed two blocks: the Highly Elliptical Orbit Intersegment Test and Early On-Orbit Test. Deliveries of incremental system capability called effectivity, include ground and space segments. Effectivity indicates a level of system design maturity and represents a decision point to continued system development. There are 10 effectivities for SBIRS High. During our evaluation, we were unable to identify a tool that would allow the program manager to link user requirements to ground segment requirement test results, map high component specifications to effectivities, and map ground segment requirements to a specific software block. In the course of our evaluation, the program office informed us that the SEIT was in the process of developing a method of tracing high component specifications to effectivities.

During program recertification, the IRT recommended a block acquisition approach to ensure requirements satisfaction as well as implementing disciplined processes with meaningful metrics. Actions taken by the program office to implement those recommendations have not included an SMM or a similar tool. Without the SMM, there still exists inadequate management of requirements since the program manager is unable to track the technical progress of user and system requirements to test results, software blocks, and effectivity milestones. Specifically the program manager is unable to trace user requirements to ground segment verification test results, map ground segment requirements to software blocks, map high component specifications to effectivities and perform crucial analysis for determining software and system maturity.

## **Approval Responsibility for Critical Test Plans and Reports**

The program office has not assumed responsibility for approving all critical development test plans and reports. The program office is a participant in IPTs and SEIT. Both are responsible for reviewing plans, implementation, and results for many critical test activities. The program office relies on contractor representatives to sign off on numerous test results used to support program management decisions, thereby passing on oversight responsibility to the contractor. In particular, the government does not sign off on ground segment test plans and reports, and does not sign off on the subsequent SBIRS system tests for intersegment compatibility and initial telemetry tracking and commanding, and payload interface. Signing off on a test plan or test result indicates that the

---

software or system is ready to continue to the next major integration and test event.

**Approval Process.** SBIRS software IPTs define software builds, test plans, and schedules for ground segment software. The IPT represents all software disciplines: management, systems engineering, specialty engineering, software configuration management, software quality assurance, test, and software development. IPT membership also includes a government representative. During ground segment development, the government representative is a participant in the ground segment IPT, which designs, tests, and verifies ground segment software. In addition to normal IPT functions, the government representative also attends management meetings, engineering review and change control board meetings, and other relevant working groups and reviews. If the government representative has an unresolved issue with the IPT, he or she notifies the program office.

The SEIT, a contractor organization, is responsible for system development test and evaluation and maintains oversight of ground segment activities to assess its readiness to participate in system level tests. The SEIT test team consists of members of the High Orbit Space Vehicle IPT, ground segment IPT, test staff, and participating government organizations. The SEIT Test Director with the support of the SEIT test team is responsible for planning, conducting, and reporting the system level tests. The SEIT is also the sign off approval authority for ground segment requirement verification tests. Ground segment verification tests are critical because they ensure that ground segment software is ready for integration and test at the SBIRS system level.

**Critical Tests.** System test, which includes the space and ground segment, is the incremental process that ensures intersegment interface compatibility and system operational capability. System level tests use a building block approach. Completion of system level tests demonstrates segment interface compatibility, functionality, external element interoperability, and overall operational readiness. Critical system tests include intersegment compatibility, telemetry, tracking, and commanding, and payload interface functional test, pre-deployment readiness, launch base compatibility, post-deployment initial test, post-deployment integration and calibrations and combined development test/operational test. For pre-deployment readiness and launch base compatibility tests, the government is the final approval authority. For post-deployment initial test and post-deployment integration and calibration events, the government participates in test readiness reviews and test exit reviews. For intersegment compatibility, telemetry, tracking, and commanding, and payload interface functional tests the SEIT is the sign approval authority.

During our review of SBIRS system test reports for telemetry, tracking, and commanding, and payload interface, we found that test results addressed SBIRS High ground requirements, instead of high component specifications as required by the SBIRS Program Verification Plan, and that deficiencies generated did not have dispositions as required by SBIRS System Test Plan. We believe that with government approval authority, the test report would have more accurately documented what the test plans required.

---

**Contractor Reliance.** Even though the total system performance responsibility clause was removed from the contract, the program office is dependent upon contractor IPTs and SEIT for determining the adequacy of development test planning and test results. Furthermore, during program recertification one of the primary reasons for removing the clause was that the IRT identified circumvention of roles and responsibilities as a significant cause for past difficulties. With the reliance on contractor testing as well as the delegation of testing approval to the contractor, there is the risk that development testing will not provide an adequate assessment of software and system technical progress. In particular, AFI 99-101 states that there is a need for knowledgeable government officials to oversee testing and approve contractor test plans and reports. For SBIRS, oversight and approval of contractor test plans and reports should include all critical ground segment, space segment, and SBIRS system tests such as ground segment verification, intersegment compatibility, telemetry, tracking, and commanding, and payload interface.

## **Extended Development Testing Annual Interim Test Report**

The program office has not established a meaningful metric for managing program's progress by establishing the requirement for annually reporting the extended developmental testing. The purpose of the annual interim test report is to document development and operational test accomplished, key test process decisions, test deficiencies, and identified risk areas. AFI 99-101 requires an annual interim test report when a program has an extended developmental test and evaluation period. SBIRS High Increment 2 has an extended developmental test and evaluation period with the intent of testing payload/satellite flight operations support activities after completion of space system tests for follow-on early orbit and payload calibration. Program documents such as the Single Acquisition Management Plan, Test and Evaluation Master Plan, and Integrated Test and Evaluation Plan do not call for an annual interim test report during extended developmental testing. Without the annual interim test report the program manager lacks a meaningful metric for assessing and reporting the progress of development testing.

**Extended Developmental Testing.** SBIRS High Increment 2 schedule identified extended developmental test and evaluation being performed from FY 2004 to FY 2008. The Combined Task Force along with supporting contractors will be conducting the tests. SBIRS High extended developmental tests include testing the interim mission control station backup and the mission control station, and ground segment checkout, launch, on-orbit test, and interim operations of Highly Elliptical Orbit and Geostationary Earth Orbit satellite payloads. Results of those tests support the assessment of SBIRS High capabilities, the decision to proceed with development of the next ground software increment, and the transitioning of developmental testing to operational testing.

**Annual Interim Test Report.** During program recertification, the IRT found that the program office lacked meaningful metrics to assess program progress and that the program office had overly optimistic assumptions in the area of software development, which led to unrealistic schedules. In order to address those issues,

---

the program office established metrics for measuring program executability and implemented an incremental delivery approach for ground software. Establishment of the Combined Task Force and extended developmental testing supports incremental ground software deliveries and block deliveries of SBIRS system capabilities. Nevertheless, the program office stated that there is no plan to annually report the results, deficiencies, and risks identified by the Combined Task Force during extended developmental testing. Such reporting to some extent would address the identified IRT deficiency. In particular, an annual interim test report would provide the program manager meaningful metrics for measuring progress of development tests as well as providing important information for key management decisions.

## Conclusion

Improved management and oversight of the SBIRS High is needed to reduce the risk of repeating problems previously identified during program recertification. During program recertification, the IRT identified deficiencies and corrective actions. Even though programmatic and contract changes have been implemented, the program office has not implemented effective requirement flow control by tracking the technical progress of requirements, assuming responsibility for approving all critical test plans and reports, and establishing a metric for annually reporting extended developmental testing. First, the program office should implement an SMM or similar tool for tracking the technical progress of user and system requirements to test results and effectivity milestones. Next, the program office should assume sign off responsibility for all critical test plans and reports so that development tests and results will provide adequate information for tracking technical progress and supporting program management decisions. Finally, the program office should provide to key decision makers an annual interim test report documenting extended developmental testing.

## Recommendations, Management Comments, and Evaluation Response

**A. We recommend that the System Program Director, Space Based Infrared System, Space and Missile Systems Center:**

**1. Implement a System Maturity Matrix, as required by Air Force Instruction 99-101, "Developmental Test And Evaluation," November 1, 1996, for tracking the system technical progress and maturity, by mapping user requirements and high component system specifications to ground segment software blocks, ground and space segment verification tests, system tests and effectivity milestones.**

**Management Comments.** The System Program Director, SBIRS, Space and Missile Systems Center concurred, and agreed to develop an SMM that will include mapping requirements to effectivities.



---

**Evaluation Response.** The System Program Director comment is responsive. We believe that having the SMM map requirements to effectivities, software blocks and test results will be an effective tool in implementing and managing the delivery of system blocks. We request that the System Program Director provide detailed information on how the SMM will track requirements to effectivities and test results.

**2. Approve all critical test plans and reports as required by Air Force Instruction 99-101, “Developmental Test And Evaluation,” November 1, 1996, by:**

**a. Assume sign off authority responsibility for all ground segment, space segment, and system critical test plans and reports. Critical test plans and reports include ground segment verification, intersegment compatibility, telemetry tracking and commanding, and payload interface tests.**

**Management Comments.** The System Program Director, SBIRS, Space and Missile Systems Center partially concurred. The System Program Director stated that they approve all critical system test plans and reports and that they have the authority to approve or disapprove test plans that merit their decision. The System Program Director also stated that along with their federally funded research and development center, they are involved in all critical system and segment level tests.

**Evaluation Response.** Although the System Program Director partially concurred, we consider the comments responsive. We based our analysis on the Integrated Master Plan and review of test plans and reports. We determined that not all critical ground segment, space segment, and SBIRS system tests such as ground segment verification, intersegment compatibility, telemetry, tracking, and commanding, and payload interface require government sign off authority. We also found that test reports for telemetry, tracking, and commanding, and payload interface, which do not require government sign off, did not meet requirements stated in the program verification plan. We request that the System Program Director provide detailed information on the government approval process for the critical test plans and reports we identified that did not require government approval. We also request that the System Program Director state if the deficiencies we identified in the test reports for telemetry, tracking and, commanding, and payload interface have been corrected.

**b. Update the Test and Evaluation Management Plan to specify that the program office is the sign off authority for all critical ground segment, space segment and system test plans and reports.**

**Management Comments.** The System Program Director, SBIRS, Space and Missile Systems Center concurred. The System Program Director stated that the Test and Evaluation Master Plan update is in progress and will reflect changes stated in management comments in response to recommendation A.2.a.

---

**3. Develop and implement procedures for the issuance to key program decision makers an annual interim test report during extended developmental testing as required by Air Force Instruction 99-101, "Developmental Test And Evaluation," November 1, 1996. The test report should include analysis of developmental and operational tests accomplished, key test process decisions, test deficiencies, and identified risk areas.**

**Management Comments.** The System Program Director, SBIRS, Space and Missile Systems Center concurred. The System Program Director stated use of the annual interim test report will help in the efforts to restore full government authority and accountability for SBIRS High.

---

## **B. Interim Highly Elliptical Orbit Capability Temporary Authority to Operate**

An Interim Authority To Operate (IATO) dated November 4, 2002, was inappropriately issued by the Designated Approval Authority for the Interim Highly Elliptical Orbit Capability (IHC). In addition, the Space Based Infrared System (SBIRS) Program Office plans to improperly issue a yearly IATO until initial operational capability scheduled in FY 2010. Issuance of the IATO was not in accordance with the Department of Defense Information Technology Security Certification and Accreditation Process. Specifically, during system validation the Certifying Authority (CA) did not ensure that the system security requirements were met by completing critical security tests and the Designated Approval Authority (DAA) did not make certain that validation tasks were complete before issuance of the IATO. Furthermore, the re-accreditation requirement in the System Security Authorization Agreement (SSAA) incorrectly makes use of the IATO to annually allow the IHC to operate. As a result, by not validating the correct implementation and operation of system security features, which affect system availability, integrity, authentication, confidentiality, the correctness of IHC test data is in doubt and the capability of IHC to test, assess, and support SBIRS is questionable.

### **Information Assurance for Interim Highly Elliptical Orbit Capability**

Information Assurance is information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. It includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. An information system can be any computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, reception of voice and or data, and includes software, firmware, and hardware.

**Interim Highly Elliptical Orbit Capability Systems.** The IHC is a stand-alone ground segment information system that supports the launch, early on-orbit tests, and analysis mode processing of the SBIRS Highly Elliptical Orbit Infrared Payload. The IHC consists of four subsystems and a connecting network. The four subsystems are the Interim Highly Elliptical Orbit Test Center, the Mission Control Station Technical Intelligence Center, the SBIRS Anomaly Resolution Center, and the Relay Ground Station. All of which have software, firmware, and hardware. The interim test center serves as the IHC control center and provides the mission control station capabilities. The technical intelligence center provides analysis support for missile warning. The anomaly resolution center enhances

---

telemetry, tracking, and command between the ground system and payload personnel by providing a more rapid response and integrated effort. The relay ground station provides the interface and archive capability between the ground station and the interim test center.

**Availability, Integrity, Authentication, and Confidentiality.** For the IHC, protection of system availability, integrity, authentication, and confidentiality are essential. More over, if controls were not in place to ensure availability, integrity, authentication, and confidentiality of the IHC, its resources, and data, there would be uncertainty that tests performed by the IHC as well as test results were correct.

Availability is the timely and reliable access to data and information services for authorized users. The IHC needs to be timely and reliable in order to perform mission planning, mission management, mission processing, and control of space and ground segment hardware and software.

Integrity is the condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. IHC data includes sensor, telemetry, mission planning, mission scheduling, ground and space segment control, archive and system administration. All IHC data needs to be accurate and unchanged. If data is incorrect, the IHC will not be able to perform any of its tasks such as providing reliable control of satellites, accurately processing mission data, and correctly managing and controlling IHC hardware and software.

Authentication is a security measure designed to establish the validity of a transmission, message, user or system or a means of verifying an individual's authorization to receive specific categories of information. IHC authentication separates users into four categories: system level, configuration management, database management, and application operation. If IHC authentication did not provide adequate separation of user access to system resources, a user could unintentionally or maliciously affect IHC availability, integrity, authentication, and confidentiality.

Confidentiality is an assurance that information is not disclosed to unauthorized persons, processes, or devices. The IHC processes data up to the DoD Secret level and is required to operate in the high mode, which is defined as all users of the system having the appropriate clearance to system information but not all users having the need to know for all information. Confidentiality is required to restrict who or what can access need to know information and system resources as well as determining what type of access is permitted.

## **System Security Certification and Accreditation Requirements for Interim Highly Elliptical Orbit Capability**

**DoD Instruction 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process Instruction (DITSCAP),"**

---

**December 30, 1997.** DITSCAP defines a process that standardizes the activities leading to system security accreditation, and applies to the acquisition, operation, and sustainment of any DoD system that collects stores, transmits, or processes unclassified or classified information. The SBIRS Program Office is required to use DITSCAP for the IHC. The DITSCAP process consists of four phases: Phase 1, Definition; Phase 2, Verification; Phase 3, Validation; and Phase 4, Post Accreditation. Information collected during Phase 1 is used to determine the certification level of the system, which in turn determines the level of effort required. Phase 2 is to verify system compliance with security requirements and evaluate vulnerabilities. Phase 3 is used to validate that the fully integrated system operates in a specified computing environment with an acceptable level of risk. Completion of Phase 3 culminates in the accreditation of the system. Phase 4 is used to manage and operate the system while preserving an acceptable level of residual risk. During Phase 3 if a system does not meet requirements, but mission criticality mandates that the system become operational, a temporary approval may be issued. If a temporary approval is used, the system is required to return to Phase 1 activities to negotiate accepted solutions, schedule, necessary security actions, and milestones.

**DoD 8510.1-M, “Department of Defense Information Technology and Security Certification and Accreditation Process (DITSCAP) Application Manual,” July 31, 2000.** This manual supports DITSCAP by presenting a detailed approach to the activities comprising the certification and accreditation process as well as the content of SSAA. Chapter 3, Phase 1 definition provides a task description on how to determine the appropriate certification level of a system. The certification level of a system determines the level of analysis required for the certification and accreditation process for all four phases. Chapter 5, Phase 3 validation provides a task description on ensuring that requirements and agreements apply, certifying that the fully integrated and operational system comply with stated requirements and during certification performing tests and evaluations to validate all security features are in place. At the completion of Phase 3, if the CA concludes that the system satisfies security requirements, the CA recommends that the DAA accredit the system. If the CA uncovers deficiencies but believes that short-term operation of the system is within acceptable bounds, the CA may recommend to the DAA an IATO. The DAA then reviews the CA’s recommendation and determines whether to accredit the system or not. If the DAA determines that the system does not meet requirements but mission criticality mandates that the system become operational, the DAA may issue an IATO.

## **Basis Used for the Interim Authority to Operate**

On November 4, 2002, the DAA issued an IATO for the IHC. In addition, the SBIRS Program Office plans to issue a yearly IHC IATO until initial operational capability scheduled in FY 2010. Before issuance of IATO, the IHC SSAA dated May 2002 documented that the security test and evaluation certification test was incomplete, and that penetration testing certification test was not done. Furthermore, the IHC SSAA re-accreditation requirement states “IHC elements

---

will be receiving IATO accreditations on a yearly basis and full accreditation after operational initial operational capability,” thereby possibly avoiding further IHC security test and evaluation and penetration testing.

**System Security Requirements.** The IHC SSAA is the IHC certification and accreditation package and generally follows the SSAA format required by DITSCAP. The SSAA is a formal agreement among the DAA, CA, user representative, and program manager. The SSAA is required to document the DITSCAP process used for certifying and accrediting the system. DoD 8510.1-M provides an outline on what is required in SSAA. It requires SSAA to contain sections, which identify system security and re-accreditation requirements, and calculate a system certification level.

IHC SSAA states that there are system security requirements for data, files, operating systems, applications, databases, and networks and that system certification Level is 3. The SSAA security requirement section states that IHC operating systems meet Class 2 criteria. Class 2 criteria include unique user logon Ids and passwords, auditing and accountability of users and processes, and access controls for the protection of object reuse. IHC operating systems achieve Class 2 requirements by implementing the following system security requirements: identification and authentication for all system users, assurance measures such as encryption, security countermeasures, and auditing, and access controls for files, operating systems, applications, and databases. Also included in the SSAA security requirement section are tools for managing network security, which are the Simple Network Management Protocol, Enterprise Security Management, and the Unix Privilege Manager. The SSAA security requirement section states that IHC elements will be receiving IATO accreditations on a yearly basis and full accreditation after operational initial operational capability.

**Level of Effort.** Along with the security requirements, the DITSCAP Application Manual also requires attachments to the SSAA. A few of the required appendixes are the Security Test and Evaluation Plan and Procedures, the Test and Evaluation Reports, the Residual Risk Assessment Results, and the Certification and Accreditation Statement. The Security Test Plans and Test Evaluation Reports verify and validate that the system security requirements have been met; the Residual Risk Assessment analyzes threats and the vulnerability of the information system to those threats; and the Certification and Accreditation Statement is the DAA approval to operate the system. Along with those required appendixes, the IHC SSAA also includes Minimal Security Activity Checklists and the Network Vulnerability Assessment. The Minimal Security Activity Checklist documents analysis and work performed on the system and the Network Vulnerability Assessment assesses the adequacy of security measures for the network.

The IHC SSAA appendixes do document the level of effort performed by the contractor during the certification and accreditation process. The Security Test and Evaluation appendix states “due to IHC network maturity level on 1 April 2002, this report is postponed as such time, as the IHC network is ready for full security test and evaluation;” and the Residual Risk Assessment appendix states “Air Force Operational Test and Evaluation Center has been contacted about

---

doing an Air Force penetration assessment.” The Minimal Security Activity Checklist, Task 3-1 and 3-2 state “security test and evaluation have not been performed and there has not been a penetration test assessment.” The Network Vulnerability Assessment appendix states, “vulnerability assessment of the IHC network is under review by government for applicability.” Lastly, the Certification and Accreditation Statement appendix includes an IATO for the IHC dated November 4, 2002, which permits the IHC to operate for a 12-month period while security verification testing is being performed.

All of the appendixes in the IHC SSAA indicate that during the 12-month period while the IHC is being used for SBIRS High early on-orbit development testing, system security requirements, such as Class 2 criterion, and network management tools will not be validated. Without validation, there will be doubt on the protection of IHC availability, integrity, authentication, and confidentiality.

## **Remaining Requirements for Interim Authority to Operate Issuance**

The IHC CA did not ensure that system security requirements were met by completing system security test and evaluation, penetration testing and the DAA did not make certain validation tasks were complete before issuance of the IATO. Furthermore, the IATO re-accreditation requirement in the IHC SSAA incorrectly makes use of the IATO to annually allow the IHC to operate. For IHC a Level 3 system, security functions must be tested to verify the integration and operation of all security features. Security test and evaluation must validate the correct implementation of identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, discretionary access controls and network connection rule compliance. Penetration testing must include insider and outsider penetration attempts based on known vulnerabilities and the implemented system must be tested for flaws, with the results described to an appropriate level for the exploitation.

DoD Instruction 5200.40 and DoD 8510.1-M define the process required for certification and accreditation as well as the issuance of an IATO. During the DITSCAP definition phase, the CA determines the appropriate certification level of the system and during the validation phase the CA ensures that all security requirements are met by making sure all required security testing is complete. At the completion of the validation phase, the CA provides an accreditation recommendation to the DAA. If the DAA determines that the system does not meet requirements but mission criticality mandates that the system become operational, the DAA may then issue an IATO.

The CA has determined that the IHC certification Level is 3. However, the appendixes, which contain the security test and evaluation report, penetration testing, minimal security activity checklist and network vulnerability assessment, do not document completion of required Level 3 security testing. The CA should have ensured that security testing was complete before submitting a

---

recommendation to the DAA and the DAA should have reviewed the SSAA and verified that all required testing was complete before issuance of the IATO. By verifying completion of required testing the DAA would have been certain that IHC system security requirements, such as Class 2 criterion, network security were correct. Furthermore, the SSAA re-accreditation requirement states that the SBIRS Program Office plans to issue an annual IATO for IHC until initial operational capability, scheduled for FY 2010. Such a requirement may circumvent security tests required to validate security requirements until initial operational capability.

## Conclusion

By not validating the correct implementation and operation of system and network security features, which affect system availability, integrity, authentication, confidentiality, the correctness of IHC test data is in doubt and the capability of IHC to accurately test, assess and support SBIRS High system is questionable. DITSCAP requires validation of system security and network security features and for a Level 3 or higher system a security test and evaluation and penetration test before system accreditation or issuance of an IATO. The DAA has granted IHC an IATO for a 12-month period while it is supporting development testing of SBIRS High early on-orbit tests. However, the DAA's decision to issue an IATO did not follow DITSCAP because IHC SSAA shows that the system is at Level 3, and security test and evaluation and penetration test are incomplete. In addition, IHC SSAA states that the program office plans to issue an annual IATO until initial operational capability scheduled for FY 2010. The CA should ensure all IHC validation tasks, which include security test and evaluation and penetration test are complete. The DAA should then accredit IHC, withhold accreditation, or issue an IATO. Also, the Program Director should remove the reaccreditation requirement for an annual IHC IATO from the SSAA and plan to have IHC achieve full accreditation within the next 12 months.

## Recommendations, Management Comments, and Evaluation Response

### **B.1. We recommend that the Interim Highly Elliptical Orbit Capability Certifying Authority:**

- a. Complete all validation tasks, which include security test and evaluation and penetration test for the Interim Highly Elliptical Orbit Capability.**
- b. Document test results in the Interim Highly Elliptical Orbit Capability System Security Authorization Agreement.**



---

**c. Provide recommendation to the Interim Highly Elliptical Orbit Capability Designated Approval Authority whether to accredit, withhold accreditation or issue an Interim Authority to Operate.**

**Management Comments.** The System Program Director, SBIRS, Space and Missile Systems Center concurred. The System Program Director stated that detailed DITSCAP Phase III security testing is scheduled to be complete in December 2003.

**Evaluation Response.** The System Program Director comments were responsive. We request that the System Program Director provide us the updated IHC – now known as the Interim Test Center, SSAA that contains a summary of the security test results once the tests are complete.

**B.2. We recommend that the Interim Highly Elliptical Orbit Capability Designated Approval Authority:**

**a. Verify all certification tasks, which include security testing are complete.**

**b. Accredite, withhold accreditation, or issue an Interim Authority to Operate for the Interim Highly Elliptical Orbit Capability based on Certifying Authority recommendation, certification task findings, and System Security Authorization Agreement documents.**

**Management Comments.** The System Program Director, SBIRS, Space and Missile Systems Center concurred.

**B.3. We recommend that the System Program Director, Space Based Infrared System, Space and Missile Systems Center:**

**a. Remove the annual Interim Authority to Operate re-accreditation requirement from the Interim Highly Elliptical Orbit Capability System Security Authorization Agreement.**

**b. Plan to have the Interim Highly Elliptical Orbit Capability achieve full accreditation within the next 12 months.**

**c. Document the plan in the Interim Highly Elliptical Orbit Capability System Security Authorization Agreement.**

**Management Comments.** The System Program Director, SBIRS, Space and Missile Systems Center partially concurred. The System Program Director stated that they agree to remove the IHC – now known as the Interim Test Center, annual IATO re-accreditation requirement but they chose to use the IATO as a viable alternative during system maturation.

**Evaluation Response.** Although the System Program Director partially concurred, we consider the comments responsive. We chose a 12-month time period for the IHC– now known as the Interim Test Center, to achieve full

---

accreditation based on the IATO provided by the program office. We acknowledge that achieving full accreditation during system maturation is difficult. We also believe that proper use of an IATO does provide a level of assurance that the Interim Test Center is performing correctly. We request that the System Program Director provide the updated Interim Test Center SSAA that documents the plan to achieve final accreditation.

---

## Appendix A. Scope and Methodology

To accomplish our evaluation objective, we examined development testing of SBIRS mission-critical software, which included planning, execution, and reporting. We reviewed system level testing. We reviewed information assurance testing, interface and interoperability testing, certification and accreditation and computer test resources.

We reviewed the organizational structure, software development process, and software development testing of SBIRS High Increment 2 ground segment. We reviewed portions of the current SBIRS High Component – Engineering Manufacturing Development Program Contract and a section of the original contract, which described Total System Performance Responsibility. We obtained and reviewed the SBIRS Single Acquisition Management Plan, Test and Evaluation Master Plan, Integrated Master Plan, Integrated Test and Evaluation Plan, Program Verification Plan, System Test Plan, and the Ground Segment Test Plans. We reviewed the System Protection Guide, Computer Security Plan, the System Security Authorization Agreement, and other certification and accreditation documents for development test information systems. We reviewed the Command, Control, Communications, Computers, and Intelligence Support Plan and Interface Control Plans. We reviewed requirement documents, including the Operational Requirements Document, the SBIRS High Component Specification and trace documents pertaining to the Ground Segment Design Documents. We reviewed deficiency reports, as well as the corrective action process. We obtained and reviewed test reports for the two software domains we examined.

We selected two software domains in SBIRS that contain mission-critical software for our evaluation. The first domain we selected was the Telemetry, Tracking, and Commanding domain within Highly Elliptical Orbit Intersegment Test, which had already completed the software development lifecycle. The second domain we selected was the Highly Elliptical Orbit Early-On-Orbit Test Mission Processing domain, which was going through the software development lifecycle during our evaluation. We visited the SBIRS Program Office in Los Angeles, California, and the contractor development and test facilities in Boulder, Colorado, and Azusa, California, to verify and validate test process and test results.

At the test facilities, we observed demonstrations of simulated SBIRS satellite operations and processing simulated satellite sensor exceedance data. We also received a walkthrough of the Mission Processing domain's system development folders capability, which is used for storage of programs and test results during development test and evaluation.

Our evaluation reviewed issues concerning development testing and evaluation of the SBIRS mission-critical software. Specifically, we evaluated the completeness and adequacy of the testing to include planning, executing and reporting of two ground-segment software domains: Highly Elliptical Orbit Intersegment

---

Telemetry, Tracking, and Commanding; and Highly Elliptical Orbit Early-On-Orbit Test Mission Processing. We also reviewed specific areas of SBIRS development testing concerning information assurance, interface, and interoperability testing and computer test resources.

We performed this evaluation from September 2002 to June 2003 according to standards implemented by the Inspector General of the Department of Defense. We visited or contacted individuals and organizations within DoD, Aerospace Corporation, Lockheed Martin Corporation, and Northrop Grumman Corporation to review software testing.

**Use of Computer-Processed data.** We reviewed data contained in management databases such as the Modified Design Compliance Matrix, the Requirements Traceability Matrix, and the Requirements Verification Ledger. We used this data to analyze requirement traceability and satisfaction. The Configuration Control Board manages the Modified Design Compliance Matrix the Requirement Traceability Matrix, and the Requirements Verification Ledger. Our findings are not dependent on the data contained in those databases. Nothing came to our attention because of the procedures that caused us to doubt the reliability of the computer-processed data.

We did not review the accuracy of the algorithms that process satellite data, as that was beyond the scope of this evaluation.

**General Accounting Office High Risk Area.** The General Accounting Office has identified several high-risk areas in the DoD. This evaluation report provides coverage of the Defense Systems Modernization high-risk area.

## Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

**Scope of the Review of the Management Control Program.** Management control was not an announced objective of this evaluation. However, we reviewed the management control program as it related to the overall evaluation objectives, which included requirements flow control for the tracking of user requirements, system specifications and technical progress to software and system testing; responsible sign off authority for test plans and reports, and a metric used to annually report extended developmental testing (see Finding A). In addition, we reviewed management's system security certification and accreditation process for the Interim Highly Elliptical Orbit Capability (see Finding B). We reviewed management's self-evaluation applicable to those controls.

**Adequacy of Management Controls.** We identified material management control weaknesses at the SBIRS Program Office as defined by DoD Instruction

---

5010.40. The SBIRS Program Manager has not implemented a System Maturity Matrix or similar management tool; has not assumed approval responsibility for all critical test plans and reports; and has not established the process for issuance of annual interim test report metric. The SBIRS Program Manager should implement a System Maturity Matrix or similar management tool for tracking the technical progress of user and system requirements to test results and effectivity milestones, should be the responsible authority for signing off all critical development test plans and reports, and should establish the metric of issuing annual interim test reports during extended developmental testing to key program decision makers.

If management implements the recommendations, the management control weaknesses identified will be corrected. A copy of the report will be provided to the senior official responsible for management controls within the office of the Air Force Program Executive Officer for Space.

**Adequacy of Management's Self-Evaluation.** On December 31, 2001, the Secretary of the Air Force notified Congress that the SBIRS High program had a Nunn-McCurdy cost breach. The cost breach was a material weakness. In order to fulfill Nunn-McCurdy requirements for program recertification, the Under Secretary of Defense for Acquisition, Logistics, and Technology conducted program reviews. These reviews included an evaluation of SBIRS by an IRT. The IRT reported on the root causes of the Nunn-McCurdy cost breach along with corrective actions. IRT corrective actions included establishment of requirements flow control, delivering system capabilities in blocks, and the establishment of new meaningful metrics.

Although the IRT evaluation identified and reported on the root causes of the Nunn-McCurdy Breach, the SBIRS Program Office did not completely implement corrections for the material weakness. In particular, SBIRS Program Office did not follow the policies in AFI 99-101 for use of a System Maturity Matrix, the program office had not assumed responsibility for sign off on all critical test plans and reports, and the program office had not established the process for issuance of annual interim test reports during extended developmental testing. Without effective management and oversight of development testing, SBIRS High is at significant risk of repeating problems previously identified during program recertification.

---

## **Appendix B. Prior Coverage**

During the last 5 years, the General Accounting Office (GAO) has issued three reports related to SBIRS High, and three reports were issued by internal Air Force reviews. Unrestricted GAO reports can be accessed over the Internet at <http://www.gao.gov/>.

### **GAO**

GAO Report No. GAO-04-48, “Despite Restructuring, SBIRS High Program Remains at Risk of Cost and Schedule Overruns,” October 31, 2003

GAO Report No. GAO-02-738, “Military Space Operations - Planning, Funding, and Acquisition Challenges Facing Efforts to Strengthen Space Control,” September 23, 2002

GAO Report No. GAO-01-7C, “Defense Acquisition: Risks Associated With Space-Based Missile Warning Need to be Addressed,” September 18, 2001

### **Air Force**

Independent Review Team, Report to Assistant Secretary of the Air Force (Acquisition) and Executive Vice President, Lockheed Martin Space Systems Company, February 2002

Management Assessment Team, Report to Assistant Secretary of the Air Force (Acquisition), March 31, 2000

Joint Estimate Team Report – May 1999

---

## Appendix C. Definitions of Technical Terms

**Class 2 Security** – Operating system security that includes unique user logon Ids and passwords, auditing and accountability of users and processes, and access controls for the protection of object reuse.

**Code and Unit Test** – The lowest level developer test of software. The purpose of unit testing is to validate requirements expressed in the detailed design descriptions and software requirements specifications. Unit testing is performed to ensure that all source statements in a unit have been executed, each conditional branch has been taken, and that all boundary values (for example, minimum-maximum values) and edit criteria are tested.

**Component Integration and Test** – Ground segment design document qualification and segment verification tests are performed to verify software requirement specifications and ground segment requirements.

**Development Integration Test** – The step in the software development lifecycle that follows code and unit test; it consists of the integration of code modules to form executables and/or libraries.

**Effectivity** – The point at which a major system requirement capability becomes available to the SBIRS Program. SBIRS Increment 2 development is divided into 10 effectivities.

**Interim Highly Elliptical Orbit Capability (IHC)** – Four SBIRS subsystems, plus the connecting network. The subsystems consist of the Interim Highly Elliptical Orbit Test Center, the Mission Control Station Technical Intelligence Center, the SBIRS Anomaly Resolution Center, and the Relay Ground Station.

**Mission-Critical Software** – Any software that operates the system.

**Mission Processing** – One of the five software domains in SBIRS. Accepts satellite telemetry; performs mission processing for Theater, Strategic, Battlespace Characterization, and Technical Intelligence missions; performs Human-to-Computer interface tasks; prepares messages for user communication interface, and other tasks.

**Penetration Test** – Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation, to identify methods of gaining access to a system by using common tools and techniques developed by hackers.

**Space Based Infrared System (SBIRS) Increment 1** – Consolidation of Defense Support Program assets under the SBIRS High program.

**Space Based Infrared System (SBIRS) Increment 2** – Delivery of SBIRS High satellites and additional capability for the ground segment.

---

**Security Certification Level 3** – A certification level for IT systems, determined by weighting system characteristics in accordance with the DoD Information Technology Security Certification and Accreditation Process. The level of effort required to perform the certification is dependent on choosing the correct certification level.

**Security Test and Evaluation** – Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.

**System Test** – These tests verify that the integrated ground and space segments meet SBIRS High component specifications.

**Telemetry, Tracking, and Commanding** – One of the five software domains in SBIRS. This domain is responsible for providing the space to ground interface via telemetry and command processing; it process satellite commanding requests from Mission Management and operator; processes satellite and sensor state of health data for display to the operator; and interfaces with Ground Control subsystem to provide status and to accept and execute system reconfiguration actions.



---

## **Appendix D. Report Distribution**

### **Office of the Secretary of Defense**

Under Secretary of Defense for Acquisitions, Technology, and Logistics  
Under Secretary of Defense (Comptroller)/Chief Financial Officer  
    Deputy Chief Financial Officer  
    Deputy Comptroller (Program/Budget)  
Assistant Secretary of Defense (Networks and Information Integration/Administration  
and Management)  
Director, Defense Procurement and Acquisition Policy

### **Department of the Army**

Auditor General, Department of the Army

### **Department of the Navy**

Naval Inspector General  
Auditor General, Department of the Navy

### **Department of the Air Force**

Assistant Secretary of the Air Force (Financial Management and Comptroller)  
Auditor General, Department of the Air Force  
Commander, Space and Missile Systems Center  
    System Program Director, Space Based Infrared System, Space and Missile Systems  
    Center

### **Other Defense Organization**

Deputy Inspector General (Industrial Security), Defense Security Service

### **Non-Defense Federal Organization**

Office of Management and Budget

---

## **Congressional Committees and Subcommittees, Chairman and Ranking Minority Member**

Senate Committee on Appropriations  
Senate Subcommittee on Defense, Committee on Appropriations  
Senate Committee on Armed Services  
Senate Committee on Governmental Affairs  
House Committee on Appropriations  
House Subcommittee on Defense, Committee on Appropriations  
House Committee on Armed Services  
House Committee on Government Reform  
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform  
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform  
House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform

# Department of the Air Force Comments



DEPARTMENT OF THE AIR FORCE  
WASHINGTON DC

OFFICE OF THE UNDERSECRETARY

17 OCT 2003

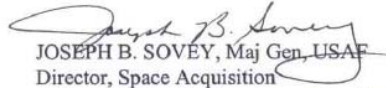
MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING  
OFFICE OF THE INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE

SUBJECT: "Development Testing of Space Based Infrared System Mission Critical Software"  
IG Report Project No. D2002PT-0206, dated 30 July 2003

This is in reply to your memorandum requesting the Assistant Secretary of the Air Force (Financial Management and Comptroller) provide Air Force comments on subject report.

The coordinated Air Force response is to partially concur with the stated findings and recommendations. The SBIRS System Program Director's detailed comments to the draft report, as requested, are attached to this letter.

The Air Force would like to thank the IG staff for their efforts. Please contact my action officer, Maj Brady Hauboldt at (703)-588-7789, for any further actions on this matter.

  
JOSEPH B. SOVEY, Maj Gen, USAF  
Director, Space Acquisition  
Office of the Under Secretary of the Air Force



**DEPARTMENT OF THE AIR FORCE**  
HEADQUARTERS SPACE AND MISSILE SYSTEMS CENTER (AFSPC)

OCT 10 2003

MEMORANDUM FOR AFPEO/SP  
SAF/USA

FROM: SMC/IS

SUBJECT: Air Force Comments to IG Report Project No. D2002PT-0206 "Development Testing of Space Based Infrared System Mission Critical Software" dated 30 Jul 03

1. This is in reply to subject DoD IG memorandum requesting the System Program Director, Space Based Infrared Systems (SBIRS), Space and Missile Systems Center to provide comments to the draft subject report. In general, the report accurately captures some of the management challenges facing the SBIRS High program. Originally, the SBIRS High contract assigned Total Systems Performance Responsibility (TSPR) to the contractor. The government program office's role was to maintain insight—which meant delegation of authority and responsibility to the contractor for basic program controls, processes, and disciplines. As a result of a significant program restructure, the government program office reclaimed TSPR and reasserted its historic authorities, responsibilities, and accountabilities. This reclamation, in turn, requires the program office to re-create and re-establish many of the traditional, structured program management processes that had been deferred to the contractor. Complete restoration of government authorities and controls will take time. The DoD IG has properly noted the fact that processes related to software development are not yet fully restored. Many of the DoD IG recommendations are extremely constructive and helpful "next steps" towards full restoration.

2. As part of the program restructure, we embarked on a plan to deliver capabilities in increments called "effectivities." These effectivities provide opportunities to take early advantage of some subset of ultimate system capabilities. However, the effectivities themselves are NOT tied to specific system requirements—they are "capability-based." The IG characterization of effectivities as "level[s] of system design maturity and...decision point[s] to continued system development" is not strictly accurate. There are no "requirements" for effectivities—instead, effectivities represent goals and expectations that, taken as a whole by the final effectivity, will meet the overall SBIRS High program requirements. Nonetheless, it is accurate to say that we have not yet properly documented the goals and expectations for each effectivity, nor have we mapped effectivities to a well-defined system maturity matrix. Of the 10 effectivities we have defined, effectivities one and two are now complete. We plan to have goals and expectations for effectivities three and four defined by a review called Baseline Update (BLU) 2003 in November 2003. BLU 2003 will also establish schedules to define the goals and expectations for effectivities five and up.

GUARDIANS OF THE HIGH FRONTIER

3. Finding A: Management and Oversight of Development Testing. The report's first finding is that the SPO has 1) not implemented effective requirements flowdown; 2) not assumed sufficient responsibility for test plans and reports, and 3) not established a metric for annual reporting of developmental testing. Response: Partially concur. Requirements flowdown to ground software and hardware previously lacked rigor; the current process is improving with the addition of careful analysis and rigorous review. We recently conducted a major review called "High Level Design Checkpoint Zero (HDC0)" which, among other things, evaluated requirements flowdown to the ground segment for the geosynchronous earth orbit (GEO) satellites. The review was largely successful although we do have liens remaining which we expect will be cleared by January 2004.

a. Recommendation A1: Implement a System Maturity Matrix (SMM). Response: Concur. As noted above, restoration of government management authority and accountability is a work in progress. We agree that development of a SMM would be a constructive and tangible step forward towards the restoration. Although effectivities are not requirements based, they will demonstrate steps to system maturation and we can map them to a SMM.

b. Recommendation A2a: Approve all critical test plans and reports. Response: Partially concur. Currently, we approve all critical *system* test plans and reports. Due to resource constraints, we do not have the capability to review and approve all test plans below the system level. However, we do assert our authority to approve or disapprove any test plans we believe merit our explicit decision. Currently the government and its federally funded research and development center (FFRDC—the Aerospace Corporation) are involved in all critical system and segment-level tests used for system requirement verification, and selected segment-level test activities. This involvement includes test plan reviews, test procedure reviews, test readiness reviews, test exit reviews, test problem reviews, and test report development, as well as the Requirements Verification activities. Involvement in segment-level test activities is focused on precursor activities to system-level tests (e.g. "Day in the Life" tests in the Ground Segment).

c. Recommendation A2b: Update the Test and Evaluation Master Plan (TEMP) to reflect recommendation A2a changes. Response: Concur. An update of the TEMP is in progress and is currently projected to be complete by the end of CY 04. Changes as stated in A2a are already included. The overall philosophy of the TEMP has changed to reflect recent changes in the acquisition process. A "core" TEMP has been developed that focuses primarily on the overall system test philosophy and processes. Additionally, TEMP "annexes," based on the program's effectivity structure, will be written to reflect the specific test needs for each effectivity. Together, both documents will encompass the same information as the previous TEMP, however the annexes provide us a great deal of flexibility that the previous method did not provide.

d. Recommendation A3: Create an annual interim test report during extended developmental testing. Response: Concur. This is an excellent recommendation which, like recommendation A1, will help us move ahead in our incremental efforts to restore full government authority and accountability for SBIRS High. Although we cannot concur fully with recommendation A2a, above, the discipline demanded by an annual interim test report will help ensure we maintain adequate cognizance over the complete developmental test program.

4. Finding B: Interim Highly Elliptical Orbit Capability Temporary Authority to Operate. The report's second finding is that the Interim HEO Test Center - now known as the Interim Test Center (ITC) - security certification and interim authority to operate (IATO) was granted inappropriately and not in accordance with Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and recommends obtaining full accreditation within 12 months. Response: Concur. Given what I now know, I agree that I erred in approving IATO for the ITC absent additional testing.

a. Recommendation B1: Certifying Authority complete all validation tasks, document test results, and provide accreditation recommendation to the Designated Approval Authority (DAA). Response: Concur. DITSCAP Phase III detailed testing is currently planned to complete in Dec 03. Continued testing will occur in the future as development of the ITC matures. NOTE: we are continuing to review the specific requirement for penetration testing as applicable to our specific configuration and mission.

b. Recommendation B2: DAA to verify all validation tasks are completed and issue accreditation decision. Response: Concur.

c. Recommendation B3: System Program Director to remove annual IATO re-accreditation requirement, plan to achieve full accreditation within 12 months, and document the plan. Response: Partially concur. We agree that IATO should not be a recurring, routine exercise. However, ITC system maturity and full accreditation is not anticipated before 2006, so full accreditation within 12 months is not achievable. Consequently, I must retain IATO as a viable decision alternative in the interim. Per DITSCAP procedure, the DAA, Certifier, program manager, and user representative will agree to the length of time for the IATO validity. The System Security Authorization Agreement (SSAA) will be updated to reflect results of the Phase III testing within 60 days of test completion, along with the plan to achieve full accreditation. The ITC currently has an Interim Security Accreditation Package dated 23 May 2003. The TEMP is our strategy for accomplishing ALL required security validation and analysis of our Developmental System prior to "Hand-Over" to the Operator. All required testing will be accomplished prior to delivery to operation users, which has been coordinated with HQ AFSPC/SC personnel.

5. Material Management Control Weakness (IG report Appendix A). The Program Office will fully implement the above responses, which will resolve the noted management control weaknesses. Subsequent to the Nunn-McCurdy breach, the SBIRS Program Office reorganized to provide greater visibility and responsiveness to these issues, including a Systems Integration Directorate chartered to integrate and deliver space and ground capabilities through quality processes that meets the users' needs (to include the Systems Engineering functions). Additionally, all test and operations activities in Colorado have been brought under a single directorate, enhancing the visibility given test activities. These management changes reflect the Program Office's commitment to continued improvement in both the government processes and the products to be delivered to the warfighters.

---

6. The Air Force would like to thank the IG staff for their efforts. Please contact my action officer Maj Bryn Turner, 310-363-0933, for any further actions on this matter.

*Alt Reese*  
for MARK S. BORKOWSKI, Colonel, USAF  
System Program Director  
Space Based Infrared Systems

## **Team Members**

The Audit Followup and Technical Support Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

David A. Brinkman  
Kenneth H. Stavenjord  
Peter C. Johnson  
Major Shurman L. Vines, USA  
Ernest G. Fine  
Ann A. Ferrante  
Anne V. Bonds