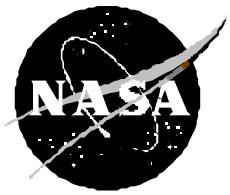
IG-01-043

AUDIT REPORT

INFORMATION TECHNOLOGY SECURITY REQUIREMENTS IN NASA CONTRACTS, GRANTS, AND COOPERATIVE AGREEMENTS

September 28, 2001



National Aeronautics and
Space Administration

OFFICE OF INSPECTOR GENERAL

Additional Copies

To obtain additional copies of this report, contact the Acting Assistant Inspector General for Audits at (202) 358-1232, or visit www.hq.nasa.gov/office/oig/hq/issuedaudits.html.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Acting Assistant Inspector General for Audits. Ideas and requests can also be mailed to:

Assistant Inspector General for Audits
Code W
NASA Headquarters
Washington, DC 20546-0001

NASA Hotline

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at (800) 424-9183, (800) 535-8134 (TDD), or at www.hq.nasa.gov/office/oig/hq/hotline.html#form or write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

Reader Survey

Please complete the reader survey at the end of this report or at http://www.hq.nasa.gov/office/oig/hq/audits.html

---

Acronyms

FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
GISRA	Government Information Security Reform Act
IT	Information Technology
OMB	Office of Management and Budget
PIC	Procurement Information Circular

W September 28, 2001

TO: A/Administrator

FROM: W/Inspector General

SUBJECT: INFORMATION: Information Technology Security Requirements in NASA Contracts, Grants, and Cooperative Agreements
Report Number IG-01-043

The NASA Office of Inspector General has completed an audit of NASA compliance with the Government Information Security Reform Act (GISRA) requirement to integrate information technology (IT) security into contracts (that include purchase orders), grants, and cooperative agreements. We found that the Agency has identified contracts subject to the requirements and was making progress in incorporating IT security requirements into contracts at two of the three Centers[1] reviewed. However, Marshall had made considerably less progress than the other two Centers. Further, NASA had not included the applicable security requirements in its purchase orders, grants, and cooperative agreements. As a result, the Agency lacks reasonable assurance of complying with GISRA requirements, and NASA's systems and information may be subject to additional security risks

Background

GISRA requires agencies to integrate IT security into contracts, grants, and cooperative agreements. In July 2000, the Agency directed Centers to identify contracts subject to IT security requirements and modify applicable contracts with an IT security clause prescribed by the NASA Federal Acquisition Regulation (FAR) Supplement. Centers were to complete the identification and modification of applicable contracts by December 31, 2000.

[1] The three Centers were Goddard Space Flight Center (Goddard), Lyndon B. Johnson Space Center (Johnson), and George C. Marshall Space Flight Center (Marshall).

Recommendations

We made three recommendations related to the incorporation of IT security requirements into applicable NASA contracts, grants, and cooperative agreements. Specifically, we recommended that NASA establish controls and timeframes to ensure that the Centers properly identify contracts subject to the IT security clause and modify the contracts to incorporate the clause, where appropriate. This will help NASA identify all applicable contracts in accordance with GISRA. We also recommended that NASA direct the Centers to include purchase orders, grants, and cooperative agreements in their IT security reviews. Finally, we recommended that NASA comply with GISRA by incorporating IT security requirements in purchase orders, grants, and cooperative agreements, where appropriate. These actions will help NASA comply with GISRA and incorporate IT security in its applicable contracts, grants, and cooperative agreements.

Management's Response and OIG Evaluation

Management concurred with all three recommendations. Management revised the NASA FAR Supplement, which clarified guidance related to identification, control, modification, and timeframes for implementation of the IT security clause. In addition, management stated it would monitor the Centers' progress in reviewing and implementing the clause. Further, management stated it would emphasize to the Centers that they must review cooperative agreements and purchase orders. Finally, management will issue guidance to review any grants valued at $100,000 or more and that do not expire before March 30, 2002.

Management's actions are responsive to the recommendations. Details on the status of the recommendations are in the findings section of the report.

[original signed by]
Roberta L. Gross

Enclosure
Final Report on Audit of Information Technology
Security Requirements in NASA Contracts, Grants, and Cooperative Agreements

INFORMATION TECHNOLOGY SECURITY REQUIREMENTS IN NASA CONTRACTS, GRANTS AND COOPERATIVE AGREEMENTS

W September 28, 2001

TO: H/Associate Administrator for Procurement

FROM: W/Assistant Inspector General for Audits

SUBJECT: Final Report on Audit of Information Technology Security Requirements in NASA Contracts, Grants, and Cooperative Agreements
Assignment Number A-01-036-00
Report Number IG-01-043

Enclosed please find the subject final report. Please refer to the Executive Summary for the overall audit results. Our evaluation of your response has been incorporated into the body of the report. Your comments on a draft of this report were responsive to the recommendations. The recommendations will remain open for reporting purposes until corrective action is completed. Please notify us when action has been completed on the recommendations.

We appreciate the courtesies extended to the audit staff. If you have questions concerning the report please contact Mr. David L. Gandrud, Program Director, Information Technology Program Audits, at (650) 604-2672, or Mr. Roger W. Flann, Program Manager, at (818) 354-9755. See Appendix C for the report distribution.

[original signed by]
Alan J. Lamoreaux

Enclosure

cc:
AB/Associate Deputy Administrator for Institutions
AO/Chief Information Officer
B/Acting Chief Financial Officer
B/Comptroller
BF/Director, Financial Management Division
G/General Counsel
JM/Director, Management Assessment Division

Contents

NASA Office of Inspector General

IG-01-043 **September 28, 2001**
A-01-036-00

Information Technology Security Requirements in NASA Contracts, Grants, and Cooperative Agreements

Executive Summary

Background. On October 30, 2000, the President signed into law the fiscal year 2001 Defense Authorization Act (Public Law 106-398), including Title X, subtitle G, "Government Information Security Reform" (the Security Reform Act, or GISRA). GISRA primarily addresses the program management and evaluation aspects of security. Specifically, GISRA requires agencies to perform annual program reviews. GISRA also requires Inspectors General to perform annual security evaluations and to annually report the results of reviews to OMB. [2]

Objectives. Our audit objectives were to determine whether NASA contracts reference applicable IT security requirements of GISRA, contain performance metrics requirements for IT security, and consider IT security in award fee plans. Specifically, we determined whether NASA had included IT security requirements, performance metrics, and award fee plans in its contracts, purchase orders, grants, and cooperative agreements. Details of our objectives, scope, and methodology are in Appendix A.

Results of Audit. Generally, NASA has identified contracts subject to the requirements and was making progress in incorporating IT security requirements into contracts at two of the three Centers reviewed. However, Marshall made considerably less progress than the other two Centers (Finding A). Further, NASA had not included the applicable IT security requirements in its purchase orders, grants, and cooperative agreements. Until NASA incorporates IT security requirements into all applicable acquisition instruments, the Agency lacks reasonable assurance of complying with GISRA requirements, and NASA's systems and information may be subject to additional security risks (Finding B).

NASA included IT security performance metrics in contracts and considered IT security in award fee plans, where appropriate, at the three Centers we reviewed. Regarding performance metrics, NASA used an IT security clause to impose GISRA requirements on applicable contractors. Contracts that included the IT security clause referenced IT security performance metrics. We did not review the adequacy of the IT security performance metrics. Regarding contracts with award fee plans, NASA contracts provide for consideration of IT security violations when determining award fees.

Recommendations. NASA should establish controls and timeframes to ensure that the Centers properly identify contracts subject to the IT security clause and modify the contracts

[2] GISRA became effective on November 29, 2000, and expires 2 years after that date.

to incorporate the clause, where appropriate. Also, NASA should direct the Centers to include purchase orders, grants, and cooperative agreements in their IT security reviews. Finally, NASA should comply with GISRA by incorporating IT security requirements in purchase orders, grants, and cooperative agreements, where appropriate.

Management's Response. Management concurred with the report's recommendations. Management revised the NASA FAR Supplement, which clarified guidance related to identification, control, modification, and timeframes for implementation of the IT security clause. In addition, management stated it would monitor the Centers' progress in reviewing and implementing the clause. Further, management stated it will emphasize that cooperative agreements and purchase orders must also be reviewed and will issue guidance to review any grants valued at more than $100,000 or more that will continue beyond the next 6 months.

Evaluation of Management's Response. We consider management's comments responsive to the recommendations.

Introduction

OMB's "Guidance on Implementing the Government Information Security Reform Act" (M-01-08, January 16, 2001) required all Federal agencies to include contractors in their IT security implementation plan. Specifically the guidance states, " . . . the Security Act includes contractor systems. The Clinger-Cohen Act[3] definition of information technology includes technology 'used by the agency directly or is used by a contractor under contract to the agency . . .'" The guidance further states that GISRA essentially codified existing requirements of OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," which required Government agencies and their contractors to provide adequate security for information collected, processed, transmitted, stored, or disseminated.

On July 14, 2000, NASA issued Procurement Information Circular (PIC) 00-12, "IT Security Requirements for Unclassified Information Technology Resources; Existing and New Contracts and Subcontracts." PIC 00-25, same title, superceded PIC 00-12 on November 29, 2000.[4] The PIC's require contracting officers to ". . . modify all existing solicitations and contracts involving unclassified information technology (IT) resources to incorporate NFS [NASA FAR Supplement] clause 1852.204-76 where appropriate." The clause requires NASA vendors to comply with the IT security requirements of NASA Policy Directive 2810.1, "Security of Information Technology," dated October 1, 1998, and NASA Procedures and Guidelines 2810.1, same title, dated August 26, 1999, which together represent NASA's guidance for implementing OMB Circular A-130, Appendix III. According to PIC 00-12 and PIC 00-25, the contracting officer was to ". . . consult with the requiring organization for assistance in identifying applicable contracts and solicitations, and the extent to which the clause is applicable to all or a segment of the statement of work requirements." The PIC's also require the contracting officers to incorporate these changes into the appropriate contracts by December 31, 2000.

[3] In 1996, Congress enacted the Clinger-Cohen Act to improve the way Federal agencies acquire and manage IT resources.

[4] PIC 00-25 clarified the applicability of the IT security clause contained in PIC 00-12.

Findings and Recommendations

Finding A. IT Security Clause in Contracts

As of May 2001, 5 months after NASA's deadline for incorporating the IT security clause into all applicable contracts, Goddard, Johnson, and Marshall were still negotiating IT security requirements with some vendors. Goddard had almost completed and Johnson had completed reviews to identify contracts subject to the clause and were making progress in incorporating the clause in their applicable contracts. However, Marshall had completed the review process for only 36 (18 percent) of its 202 contracts. Marshall's delay can be attributed to inadequate controls over the Center's actions to implement the PIC requirements and to other workload priorities. Until NASA includes the security clause in all applicable contracts, the Agency lacks assurance that it meets GISRA requirements, and NASA systems and information may be subject to additional security risks.

Agency Policies and Procedures

NASA PIC's 00-12 and 00-25 require contracting officers to incorporate NASA FAR Supplement 1852.204-76, also known as the IT security clause, into contracts where applicable. The IT security clause requires contractors to comply with NASA Policy Guidance 2810.1, which is NASA's implementing guidance for OMB Circular A-130, Appendix III. PIC 00-12 established deadlines of August 15, 2000, for conducting reviews to identify applicable contracts, and December 31, 2000, for incorporating the clause in the contracts. The PIC's require the Centers to report their progress to the Principal Center IT Security Manager each month.[5]

Center Implementation of PIC 00-25

The status of actions taken by the three Centers in implementing PIC 00-25 as of May 2001, is shown in Table 1:

Table 1. Implementation of PIC 00-25

	Goddard	Johnson	Marshall
Total Contracts	297	147	202
Contracts Reviewed	294	147	36
Percentage of Contracts Reviewed	99	100	18
Contacts Not Reviewed	3	0	166
Contracts Reviewed that Are Subject to the Security Clause	92	45	20
Contracts with Clause Incorporated	22	39	8
Contracts Pending Clause Incorporation	70	6	12

Need for Controls at Marshall to Implement PIC-00-25. As indicated in the table, Marshall had reviewed only about 18 percent of its contracts and was in the process of

[5] NASA designated Ames Research Center as its Principal Center for IT Security.

modifying 12 of the 20 contracts that it found to be subject to the clause. Marshall's delays in implementing PIC 00-12 and PIC 00-25 related to management's lack of controls to ensure that the Center complied with PIC requirements. For example, procurement officials had not coordinated with the Center IT Security Manager until March 2001 to identify contracts subject to the clause. In addition, Marshall officials told us that workload priorities contributed to the Center's delay in identifying all contracts subject to the IT security clause. As of May 2001, Marshall had taken no action to review 166 contracts.

Reliance on Centers' Implementation. NASA Office of the Chief Information Officer and the Headquarters Office of Procurement representatives indicated that they relied on the Centers to implement PIC 00-12 and PIC 00-25 guidance. Although NASA established controls to track implementation of the applicable contracts after the Centers identified the contracts, NASA had no formal controls to ensure that the Centers identified all contracts subject to the clause. As a result, the NASA Office of the Chief Information Officer and Office of Procurement were not aware that Marshall was far behind in identifying the applicable contracts.

Conclusion

Until NASA establishes appropriate management controls, the Agency cannot be assured that the Centers will identify all contracts subject to the IT security clause and that the Agency complies with GISRA requirements. Further, NASA systems or information may be subject to additional security risks.

Recommendations, Management's Response, and Evaluation of Response

1. **The Associate Administrator, Office of Procurement, in coordination with the Chief Information Officer, should establish controls and timeframes to ensure that the Centers properly identify contracts subject to the IT security clause and modify the contracts to include the clause, where appropriate.**

Management's Response. Concur. Management stated that it had issued new guidance to implement IT security requirements (NASA issued new guidance after audit field work). Management revised various segments of the NASA FAR Supplement including 1804.470-1, 1804.470-2, 1804.470-3, 1804.470-4, and 1852.204-76. NASA also issued PIC-01-17 with guidance on implementing the NASA FAR Supplement clause and related requirements. The PIC addresses the OIG Recommendation. In addition, NASA's Office of Procurement will monitor the Centers' progress in reviewing existing contracts

and implementing the clause, where applicable, to assure that all Centers systematically progress in meeting the completion date of December 31, 2001. The complete text of NASA Headquarters response is in Appendix B.

Evaluation of Response. The actions taken by NASA are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed.

Finding B. IT Security Requirements in Purchase Orders, Grants, and Cooperative Agreements

The three Centers we reviewed had not included IT security requirements in applicable purchase orders, grants, and cooperative agreements. This condition occurred because NASA did not require the Centers to specifically review purchase orders to determine whether they were subject to the security clause or to include the IT security clause in grants. Also, NASA did not clarify the Agency's position regarding the applicability of the clause to cooperative agreements. Until NASA includes security requirements, as applicable, in all of its procurement instruments, it lacks assurance that its purchase orders, grants, and cooperative agreements comply with GISRA requirements, and NASA systems and information may be subject to additional security risks.

Policies and Procedures

GISRA Requirements. GISRA requires Government agencies to comply with the IT security provisions established in OMB Circular A-130, Appendix III. GISRA also applies to contractors who develop or maintain Government-owned information. Because OMB guidance did not address the applicability of GISRA to grants and cooperative agreements, we asked OMB for clarification regarding the applicability issue. In June 2001, OMB provided a written response stating that IT security provisions apply to contracts (which include purchase orders) and to grants and cooperative agreements when those instruments use Government resources (such as information, IT, or other equipment, personnel or other assets). OMB also stated that if a Government program official oversees the grantee, such as to assess whether the grant is returning any benefits, or to prevent fraud, waste, or abuse of public funds, then the Government has the authority and responsibility to demand adequate security.

NASA Policy. NASA policy for grants and cooperative agreements is established in NASA Procedures and Guidelines 5800.E, "Grant and Cooperative Agreement Handbook," dated October 19, 2000. Neither the Handbook nor any of its referenced provisions require recipients of grants or cooperative agreements to meet specific IT security requirements, except when the recipients handle classified data or must undergo background investigations. To assist the Centers in determining the applicability of the IT security clause to the cooperative agreements, NASA published guidance about IT security clause implementation in the form of Frequently Asked Questions (FAQ's).

Inclusion of the IT Security Clause

Purchase Orders. The three Centers we reviewed did not include the IT security clause in applicable purchase orders. Although FAR Subpart 2.101 considers purchase orders as contracts, PIC 00-12 and PIC 00-25 guidance did not specifically address purchase orders. Center officials said they did not include purchase orders in the review process because purchase orders were too numerous to review. Center officials also stated that

purchase orders would have expired before the clause could have been inserted in the purchase orders. As a result, none of the three Centers included purchase orders in their IT security reviews.

We identified some purchase orders that suggested the need for an IT security clause. Table 2 contains examples of purchase orders that may be subject to the IT security clause.

Table 2. Purchase Order Examples Potentially Subject to the IT Security Clause

Purchase Order Number	Center	Expiration Date	Purchase Order Value (in millions)	Description of Work
H32946D	Marshall	10/31/01	$6.7	IFMP* Core Financial Software
T2351W	Johnson	9/30/01	$1.0	IT Support Services
S43411G	Goddard	12/31/01	$1.3	Flight Dynamics Navigation Attitude and IT
S38657G	Goddard	12/21/01	$6.7	IT Services
S36205G	Goddard	8/26/02	$2.0	Multi-mission Flight Software Support

* Integrated Financial Management Program.

Until NASA includes purchase orders in the security review process, it cannot be assured that the Agency will meet GISRA requirements. Further, the Agency's systems and information may experience additional security risk.

Grants and Cooperative Agreements. The three Centers we reviewed did not include IT security requirements in applicable grants and cooperative agreements. Regarding grants, NASA had not published guidance on the inclusion of IT security requirements. Instead, NASA required the Centers to manage grants according to the Grant Handbook. The Handbook, however, imposed no specific IT security requirements relating to GISRA. Also, NASA officials said they believed that the inclusion of security requirements in grants could have the effect of reducing the number of prospective grantees because increased restrictions may discourage some applicants. Regarding cooperative agreements, NASA's guidance in the form of FAQ's on the applicability of the clause was unclear. Specifically, the guidance initially required the Centers to include cooperative agreements in their IT security reviews. NASA later revised the FAQ guidance to state, as follows: "Does the clause apply to cooperative agreements? Generally No. But Yes, but only if applicable . . . ." Lacking appropriate guidance, none of the three Centers included grants and cooperative agreements in their IT security reviews.

Until NASA includes IT security requirements in applicable grants and cooperative agreements, it cannot be assured that the Agency will meet GISRA requirements. Further, the Agency's systems and information may experience additional security risk.

Recommendations, Management's Response, and Evaluation of Response

The Associate Administrator, Office of Procurement, in coordination with the Chief Information Officer, should:

2. Provide guidance to the Centers to include purchase orders, grants, and cooperative agreements in their IT security reviews.

Management's Response. Concur. Management will implement a review of existing cooperative agreements with commercial firms for those agreements subject to anticipated revisions to Section D of the NASA Grant and Cooperative Agreement Handbook. Management expects to complete revisions to the Handbook in October 2001. NASA will also review existing grants with values of $100,000 or more and do not expire within the next 6 months (March 30, 2002). NASA plans to complete its review of grants by June 30, 2002, which includes time to create and approve the wording for grant-related IT security requirements. NASA also plans to emphasize that Centers should include purchase orders when reviewing existing contracts. This guidance will be included in a Web site that provides Centers with answers to FAQ's (see Appendix B).

Evaluation of Response. The actions taken by NASA are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed.

3. Incorporate IT security requirements as required by GISRA in purchase orders, grants, and cooperative agreements, where appropriate.

Management's Response. Concur. NASA will include the requirement to conduct IT security reviews in the revised Section D of the NASA Grant and Cooperative Agreement Handbook, which the Agency anticipates publishing in October 2001 as a Proposed Rule. NASA will also review existing grants, cooperative agreements and purchase orders to determine IT security clause applicability (see Appendix B).

Evaluation of Response. The actions taken by NASA are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed.

Appendix A. Objectives, Scope, and Methodology

Objectives

Our objectives were to determine whether NASA contracts:

- reference applicable IT security requirements of GISRA,
- contain performance metrics requirements for IT security, and
- consider IT security in award fee plans.

Scope and Methodology

We performed work at Goddard, Johnson, and Marshall. We reviewed their methodology and criteria for identifying contracts, grants, cooperative agreements, and purchase orders subject to the IT security clause. We examined the contract files to determine whether the Centers added the IT security clause to their applicable contracts.

To accomplish our objectives, we performed the following:

- To determine how NASA identified and implemented IT security requirements, we interviewed officials from the NASA Office of the Chief Information Officer, NASA Office of Procurement, NASA Principal IT Security Clause Coordinator, Center representatives/coordinators for the IT security clause, Center Offices of the Chief Information Officer and Center IT Security Managers, and contracting officers.

- To obtain an understanding of IT security laws and regulations and NASA policies and procedures relevant to IT security, we reviewed the Government Information Security Reform Act (GISRA); the Government Paperwork Elimination Act, 1998; the Clinger-Cohen Act, 1996; the Government Performance and Results Act, 1993; the Computer Security Act, 1987; the Federal Managers' Financial Integrity Act, 1982; OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources”; OMB Memorandum M-01-08, “Guidance on Implementing the Government Information GISRA”; NASA FAR Supplement Clause 1804.470, “Security Requirements for Unclassified Information Technology Resources”; NASA Policy Directive 2810.1, “Security of Information Technology”; NASA Procedures and Guidelines 2810.1, “Security of Information Technology”; NASA Procedures and Guidelines 5800.E, "Grant and Cooperative Agreement Handbook," dated October 19, 2000; NASA PIC 00-12 and PIC 00-25, dated July 2000 and November 2000, respectively; NASA IT Implementation Plan for fiscal years 2001-2005; and NASA Procurement Management Survey Report.

- To determine the population of active NASA contracts, purchase orders, grants, and cooperative agreements, we extracted relevant data from the NASA Financial and Contractual Status database for fiscal year 2001.

Management Controls Reviewed

We reviewed NASA management controls for identifying and implementing contracts subject to the IT security clause. We considered the management controls to be adequate except that NASA had not fully complied with all applicable IT security requirements. See Findings A and B.

Audit Field Work

We performed the audit field work from April through June 2001. We conducted the audit in accordance with generally accepted government auditing standards.

Appendix B. Management's Response

National Aeronautics and
Space Administration
Headquarters
Washington, DC 20546-0001

Reply to Attn of HC

SEP 1 2 2001

TO: W/Assistant Inspector General for Auditing

FROM: HC/Director, Analysis Division

SUBJECT: Code H Response to OIG Draft Audit Report on Information Technology Security Requirements in NASA Contracts, Grants, and Cooperative Agreements; Draft Audit Report Number A-01-036-00.

Enclosed is our response to the subject draft report dated August 3, 2001.

Please call Karl Beisel at 202-358-0416 or Jack Horvath at 202-358-0456 if you have any questions or need further coordination on this matter.

Anne Guenther

Anne Guenther

Enclosure

GENERAL COMMENTS:

The OIG conducted its review during the period in which the IT Security Requirements and Guidance were being reviewed, strengthened, clarified and ultimately revised. Appendix A of the Audit Report indicates that the OIG did not review what is now the most current NFS and PIC 01-17 language. Thus some recommendations have been overtaken by events. In addition, changes are in process for the Grant and Cooperative Agreement Handbook and the NFS to further address this area.

OIG RECOMMENDATION 1

The Associate Administrator, Office of Procurement, in coordination with the Chief Information Officer, should establish controls and timeframes to ensure that the Centers properly identify contracts subject to the IT security clause and modify the contracts to include the clause, where appropriate.

CODE H RESPONSE TO RECOMMENDATION 1: CONCUR

The NASA Office of Procurement has addressed each of the recommended changes in its recent revisions to the NASA FAR Supplement (NFS) and in associated guidance to implement IT security requirements. On July 12, 2001, the Federal Register published NASA's revised interim rule on IT Security. Various segments of the NASA FAR Supplement were revised including: 1804.470-1, 1804.470-2, 1804.470-3, 1804.470-4 and 1852.204-76. Published in conjunction with the changes made to the NFS, NASA issued an extensive Procurement Information Circular, PIC 01-17, (see this PIC on the NASA website at: http://www.hq.nasa.gov/office/procurement/regs/pic01-17.html) giving guidance on implementing the NFS clause and related requirements. The guidance covers the aspects enumerated in the OIG's Recommendation 1: Identification, control, modification and the timeframes in which these actions are to be achieved. In addition to the control and reporting aspects listed in PIC 01-17, NASA HQ, Code H, will also monitor the Centers' progress in reviewing existing contracts and implementing the clause, where applicable, to assure that all Centers systematically progress to meet the completion date of December 31, 2001.

NFS 1804.470-2(a) requires that all contracts in which the contractor must have physical or electronic access to NASA's sensitive information in unclassified systems contain security requirements. IT security requirements should be incorporated into the solicitation/contract requirements. The contractor's approach to ensuring IT security should be evaluated along with other technical requirements. The contractor's approach should demonstrate an understanding of the requirements of NPG 2810.1 as applicable to the solicitation/contract requirements (see 1804.470-3). When the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources, is included, the contractor's approach should also indicate how they will meet the requirements of the clause (i.e., the functions/positions that will require privileged or limited privileged access (see Section 4.5.3, NPG 2810.1), and who will conduct screening of individuals requiring this type of access, screening waivers, and training).

Appendix B

PIC 01-17 delineates a schedule, with a target completion date of December 31, 2001, for addressing existing contracts. All existing contracts will be reviewed and modified to include the requirement if the requirement applies by the cited date. This effort is being coordinated with the CIO's office. We believe that the actions taken above are fully responsive to this recommendation. The target resolution date remains the date for implementation of the clause into existing contracts: December 31, 2001.

CORRECTIVE ACTION OFFICIAL:	Code HC/K. Beisel
CORRECTIVE ACTION CLOSESURE OFFICIAL:	Code HC/A. Guenther
PROJECTED CORRECTIVE CLOSURE DATE:	December 31, 2001

OIG RECOMMENDATION 2:

The Associate Administrator, Office of Procurement, in coordination with the Chief Information Officer, should:

1. *Provide guidance to the Centers to include purchase orders, grants, and cooperative agreements in their IT security reviews.*
2. *Incorporate IT security requirements as required by GISRA in purchase orders, grants, and cooperative agreements, where applicable.*

CODE H RESPONSE TO RECOMMENDATION 2; PART 1: CONCUR

GRANTS AND COOPERATIVE AGREEMENTS:

There were over 7,000 research grants active agency-wide in FY 2000. The vast majority are low dollar, low risk research efforts that will expire within a short timeframe. They do not require the recipient to have electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. Most grants do not meet the necessary test for implementation of IT security procedures used in contracts (i.e.: computer control of spacecraft, satellites, or aircraft or their payloads; acquisition, transmission or analysis of data owned by NASA with significant replacement cost should the recipient's copy be corrupted; or access to NASA networks or computers at a level beyond that granted the general public, e.g. bypassing a firewall). We recognize the need to initiate measures addressing IT security, but reviewing all existing grants would not be considered productive.

The Office of Procurement will review existing grants with values of $100,000 or more and do not expire within the next six months (3/30/02). We will also focus on pre-award reviews, where relevant, to identify and discuss IT security facets and issues in grant proposals. This is an appropriate solution considering the number, type and nature of grants and the cost-benefit-to-risk exposure. Such an approach is a prudent, efficient, and economical use of NASA resources. The existing grants review is projected to be completed by June 30, 2002 which considers time to create and approve grant related IT security requirements wording. For prospective grants, offerors will be asked to describe their approach to managing these facets pursuant to the NASA FAR Supplement Paragraph 1835.016-71, NASA Research Announcement, NFS 1852.235-72 (a proposed rule which was published August 31, 2001). Instructions for Responding to NASA

Research Announcements, will require the identification and discussion of IT security facets and issues throughout the proposal where they are relevant and the offeror's approach to managing those issues. In addition, NASA will be required to evaluate the offerors' proposed approach to managing IT Security issues (e.g., level of maturity of the technology being applied or developed, technical complexity, performance tolerances and specifications, etc.).

An analysis of existing commercial cooperative agreements subject to anticipated revisions to Section D of the NASA Grant and Cooperative Agreement Handbook (14 CFR Part 1274) will be implemented. Revisions to Section D to the NASA Grant and Cooperative Agreement Handbook (14 CFR Part 1274) are anticipated to be published in October 2001 as a Proposed Rule.

It has been noted in the contract arena that the IT security clause does not apply universally to all contracts nor does it universally apply to all IT related contracts. The same could be said for cooperative agreements. Revisions to Section D to the NASA Grant and Cooperative Agreement Handbook (14 CFR Part 1274) are anticipated to be published in October 2001 as a Proposed Rule. Final Rule expected at about January 2002. The revised Section D will include a new provision at Paragraph 1274.937, Security Requirements for Unclassified Information Technology Resources expanding on comments received on the proposed clause. Additional direction may be issued concerning post-award review of existing cooperative agreements.

PURCHASE ORDERS:

A Frequently Asked Questions (FAQ) website has been created for the IT security subject (see: http://ec.msfc.nasa.gov/hq/library/IT_Security_FAQ.html). The information includes an address of purchase orders which are technically contracts and therefore within the universe of required review of existing contracts and subject to evaluation in future issuance for IT security aspects and use of the IT security clause. That purchase orders should be included in the review of existing contracts (as appropriate) will be emphasized to each of the NASA Centers. The FAQ website will be modified to address the contract nature of purchase orders.

CORRECTIVE ACTION OFFICIAL:	Code HC/K. Beisel
CORRECTIVE ACTION CLOSESURE OFFICIAL:	Code HC/A. Guenther
PROJECTED CORRECTIVE CLOSURE DATE:	June 2002

CODE H RESPONSE TO RECOMMENDATION 2; PART 2: CONCUR

GRANTS AND COOPERATIVE AGREEMENTS:

The NASA Grant and Cooperative Agreement Handbook Paragraph 1260.35 Investigative Requirements includes wording that NASA reserves the right to perform security checks, and to deny or restrict access to a NASA Center, facility, computer system, or technical information as appropriate where risk has been identified. Further steps are being taking by way of changes to Section D where the concern for IT Security may be a real possibility.

Appendix B

The NASA Office of Procurement will include the requirement to conduct IT security reviews in the revised Section D to the NASA Grant and Cooperative Agreement Handbook (14 CFR Part

1274) which is anticipated to be published in October 2001 as a Proposed Rule. The Final Rule is expected in approximately January 2002. The new provision is Paragraph 1274.937 Security Requirements for Unclassified Information Technology Resources.

Paragraph 1274.937 requires that all cooperative agreements in which the recipient must have physical or electronic access to NASA's sensitive information in unclassified systems contain security requirements. The recipient shall provide, implement, and maintain an IT Security Plan as approved by NASA. The plan shall be incorporated into the cooperative agreement as a compliance document. Personnel screening of individuals requiring access at an appropriate level will be conducted in accordance with NPG 2810.1, Section 4.5; NPG 1620.1, Chapter 3. The Recipient shall ensure that its employees, in performance of the cooperative agreement, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices. The substance of these requirements will be included in all subcontracts and sub agreements that meet the conditions contained therein.

A review to identify and discuss risk factors and issues throughout grant proposals where they are relevant, and describe their approach to managing these risks will be included in the NASA FAR Supplement Paragraph 1835.016-71. The NFS will require the issuing office to obtain input from the cognizant offices responsible for matters of safety and mission assurance, occupational health, environmental protection, information technology, export control, and security. In addition, the appropriate organization will be contacted for NASA Research Announcements that may involve mission critical ground systems.

NFS 1852.235-72 (Instructions for Responding to NASA Research Announcements) will require the identification and discussion of risk factors and issues throughout the proposal where they are relevant, and the offeror's approach to managing those risks.

PURCHASE ORDERS:

A Frequently Asked Questions (FAQ) website has been created for the IT security subject (see: http://ec.msfc.nasa.gov/hq/library/IT_Security_FAQ.html). The information includes an address of purchase orders which are technically contracts and therefore within the universe of required review of existing contracts and subject to evaluation in future issuance for IT security aspects and use of the IT security clause. That purchase orders should be included in the review of existing contracts (as appropriate) will be reemphasized to each of the NASA Centers. The FAQ website modified to address the contract nature of Purchase.

CORRECTIVE ACTION OFFICIAL:	Code HC/K. Beisel
CORRECTIVE ACTION CLOSESURE OFFICIAL:	Code HC/A. Guenther
PROJECTED CORRECTIVE CLOSURE DATE:	June 2002

Appendix C. Report Distribution

National Aeronautics and Space Administration (NASA) Headquarters

A/Administrator
AI/Associate Deputy Administrator
AA/Chief of Staff
AB/Associate Deputy Administrator for Institutions
B/Acting Chief Financial Officer
B/Comptroller
BF/Director, Financial Management Division
C/Associate Administrator for Headquarters Operations
G/General Counsel
H/Associate Administrator for Procurement
HK/Director, Contract Management Division
HS/Director, Program Operations Division
J/Associate Administrator for Management Systems
JM/Director, Management Assessment Division
L/Acting Associate Administrator for Legislative Affairs
M/Associate Administrator for Space Flight
P/Associate Administrator for Public Affairs
Q/Associate Administrator for Safety and Mission Assurance
R/Associate Administrator for Aerospace Technology
R/Chief Information Officer Representative
S/Associate Administrator for Space Science
U/Acting Associate Administrator for Biological and Physical Science
X/Acting Director, Office of Security Management and Safeguards
Y/Associate Administrator for Earth Science
Z/Acting Associate Administrator for Policy and Plans

NASA Centers

Director, Ames Research Center
Director, Dryden Flight Research Center
Director, John H. Glenn Research Center at Lewis Field
Director, Goddard Space Flight Center
Director, NASA Management Office, Jet Propulsion Laboratory
Acting Director, Lyndon B. Johnson Space Center
Director, John F. Kennedy Space Center
  Chief Counsel, John F. Kennedy Space Center
Director, Langley Research Center
Director, George C. Marshall Space Flight Center
Acting Director, John C. Stennis Space Center

Appendix C

Non-NASA Federal Organizations and Individuals

Assistant to the President for Science and Technology Policy
Director, Office of Management and Budget
Deputy Director of Management, Office of Management and Budget
Deputy Associate Director, Energy and Science Division, Office of Management and Budget
Branch Chief, Science and Space Programs Branch, Energy and Science Division, Office of Management and Budget
Managing Director, Acquisition and Sourcing Management Team, General Accounting Office
Associate Director, National Security and International Affairs Division, Defense Acquisition Issues, General Accounting Office
Senior Professional Staff Member, Senate Subcommittee on Science, Technology, and Space

Chairman and Ranking Minority Member - Congressional Committees and Subcommittees

Senate Committee on Appropriations
Senate Subcommittee on VA, HUD, and Independent Agencies
Senate Committee on Commerce, Science, and Transportation
Senate Subcommittee on Science, Technology, and Space
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on VA, HUD, and Independent Agencies
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations
House Subcommittee on National Security, Veterans Affairs, and International Relations
House Subcommittee on Technology and Procurement Policy
House Committee on Science
House Subcommittee on Space and Aeronautics

Congressional Member

The Honorable Pete Sessions, U.S. House of Representatives

Appendix Major Contributors to the Report

David L. Gandrud, Program Director, Information Technology Program Audits

Roger W. Flann, Program Manager

Carl L. Aley, Auditor-in-Charge

Rhodora Posey, Auditor

Kenneth C. Wood, Auditor

Nancy C. Cipolla, Report Process Manager

Betty G. Weber, Operations Research Manager

Barbara J. Smith, Program Assistant