III. INDEPENDENT AUDITORS' REPORT AND MANAGEMENT'S RESPONSE

February 26, 2002

To: Dr. Eamon M. Kelly
Chairman, National Science Board

Dr. Rita Colwell
Director, National Science Foundation

From: Christine C. Boesz, Dr. P.H.
Inspector General

Subject: Audit of the National Science Foundation's
Fiscal Years 2001 and 2000 Financial Statements

This memorandum transmits KPMG LLP's report on its Fiscal Years 2001 and 2000 financial statement audit of the National Science Foundation (NSF).

Results of Independent Audit

The Chief Financial Officer's (CFO) Act of 1990 (P.L. 101-576), as amended, requires NSF's Inspector General or an independent external auditor, as determined by the Inspector General, to audit the Foundation's financial statements. Under a contract monitored by the Office of Inspector General (OIG), KPMG, an independent public accounting firm, performed an audit of NSF's Fiscal Years 2001 and 2000 financial statements. The contract required that the audit be performed in accordance with the Government Auditing Standards issued by the Comptroller General of the United States, and Bulletin 01-02, *Audit Requirements for Federal Financial Statements*, issued by the United States Office of Management and Budget.

KPMG issued an unqualified opinion on NSF's financial statements. In its Report on Internal Controls Over Financial Reporting, KPMG identified two reportable conditions relating to (1) post-award procedures for monitoring awardees' administrative and financial management practices and tracking of NSF-owned property, plant and equipment in the custody of awardees, and (2) entity-wide information security. In its Report on Compliance with Laws and Regulations, KPMG identified one instance of noncompliance with the Federal Financial Management Improvement Act of 1996 (FFMIA) relating to Federal financial management system requirements. This noncompliance pertains to the finding reported in the Report on Internal Control concerning physical and logical access controls.

NSF management disagrees with the facts and circumstances regarding each of the reportable conditions, as well as the designation of these matters as reportable conditions.

NSF management also disagrees with the finding of non-compliance with FFMIA. Management's response is located in Attachment 1.

Evaluation of KPMG's Audit Performance

To fulfill our responsibilities under the CFO Act of 1990, as amended, and other related financial management legislation, the Office of Inspector General:

- Reviewed KPMG's approach and planning of the audit;
- Evaluated the qualifications and independence of the auditors;
- Monitored the progress of the audit at key points;
- Examined working papers related to assessing internal controls over NSF's financial reporting process;
- Coordinated periodic meetings with NSF management to discuss audit progress, findings and recommendations;
- Reviewed KPMG's audit report to ensure compliance with Government Auditing Standards and Office of Management and Budget Bulletin No. 01-02;
- Coordinated issuance of the audit report; and
- Performed other procedures that we deemed necessary.

Due to the timing for completing the NSF Fiscal Year 2001 Accountability Report, we have not yet completed our review of the working papers prepared by KPMG.

KPMG is responsible for the attached auditor's report, dated January 18, 2002, and the conclusions expressed therein. Our review, as differentiated from an audit in accordance with auditing standards generally accepted in the United States of America, was not intended to enable us to express, and accordingly we do not express, an opinion on NSF's financial statements and report on NSF's internal control over financial reporting and compliance with laws and regulations. Nevertheless, we believe that KPMG's work provides a reasonable basis for its report.

The Office of Inspector General appreciates the courtesies and cooperation extended to KPMG LLP and OIG staff by NSF during the audit. If you or your staff have any questions, please contact me or Deborah H. Cureton, Associate Inspector General for Audit.

cc: Dr. Stanley V. Jaskolski, Chair, Audit and Oversight Committee

2001 M Street, N.W.
Washington, D.C. 20036

INDEPENDENT AUDITORS' REPORT

Dr. Eamon M. Kelly
Chairman, National Science Board

Dr. Rita Colwell
Director, National Science Foundation

We have audited the accompanying balance sheets of the National Science Foundation (NSF) as of September 30, 2001 and 2000, and the related statements of net cost, changes in net position, budgetary resources, and financing (hereinafter collectively referred to as the "financial statements") for the years then ended. The objective of our audits was to express an opinion on the fair presentation of these financial statements. In connection with our audits, we also considered NSF's internal control over financial reporting and tested NSF's compliance with certain provisions of applicable laws and regulations that could have a direct and material effect on its financial statements.

SUMMARY

As stated in our opinion on the financial statements, we conclude that NSF's financial statements as of and for the years ended September 30, 2001 and 2000, are presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America.

As a result of our consideration of internal control over financial reporting, we identified the following conditions that we consider to be reportable conditions but not material weaknesses:

- ***Post-award Management*** - Adequate procedures for monitoring (i) awardees' administrative and financial management practices and compliance with laws and regulations, and (ii) NSF-owned property, plant and equipment in awardees' custody are not in place.

- ***Information Security*** - NSF has several weaknesses in its entity-wide information security that result in vulnerabilities in logical and physical access controls.

The results of our tests of compliance with certain provisions of laws and regulations, exclusive of those referred to in the Federal Financial Management Improvement Act (FFMIA) of 1996, disclosed one instance of potential noncompliance in Fiscal Year (FY) 2000 that was required to be reported under *Government Auditing Standards,* issued by the

Comptroller of the United States, and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements.* This matter related to potential noncompliance with Federal appropriations law arising from NSF expending funds from its Research and Related Activities appropriation to supplement potential shortfalls in its Major Research Equipment appropriation for a large international project. This potential noncompliance with law was identified in a report issued by the NSF Office of Inspector General in December 2000. This condition was resolved during FY 2001.

Our tests of compliance with FFMIA section 803(a) requirements disclosed an instance where NSF's financial management systems did not substantially comply with Federal financial management systems requirements.

NSF management disagrees with the facts and circumstances regarding each of the reportable conditions, as well as the designation of these matters as reportable conditions. NSF management also disagrees with the finding of non-compliance with FFMIA. Management's response is located in Attachment 1.

The following sections discuss our opinion on NSF's financial statements, our consideration of NSF's internal control over financial reporting, our tests of NSF's compliance with certain provisions of applicable laws and regulations, and management's and our responsibilities.

OPINION ON FINANCIAL STATEMENTS

We have audited the accompanying balance sheets of the National Science Foundation as of September 30, 2001 and 2000, and the related statements of net cost, changes in net position, budgetary resources, and financing for the years then ended.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the National Science Foundation as of September 30, 2001 and 2000, and its net cost, changes in net position, budgetary resources, and reconciliation of net cost to budgetary obligations for the years then ended, in conformity with accounting principles generally accepted in the United States of America.

NSF adopted the provisions of Statement of Federal Financial Accounting Standards (SFFAS) No. 10, *Accounting for Internal Use Software*, and SFFAS No. 21, *Reporting Corrections of Errors and Changes in Accounting Principles*, effective October 1, 2000.

The information in the *Management's Discussion and Analysis*, *Required Supplementary Information,* and *Required Supplementary Stewardship Information* sections is not a required part of the financial statements but is supplementary information required by the Federal Accounting Standards Advisory Board and OMB Bulletin No. 97-01, *Form and Content of Agency Financial Statements*, as amended. We have applied certain limited procedures, which consisted principally of inquiries of management, regarding the methods of measurement and presentation of this information. However, we did not audit this information, and accordingly, we express no opinion on it. Based upon our limited procedures, we determined that NSF did not complete the intragovernmental balance

reconciliations with its governmental trading partners, as specified by the January 2000 technical amendment to OMB Bulletin No. 97-01, because, although NSF issued confirmations to its major partners, such partners did not respond with adequate information to assist in reconciling balances.

INTERNAL CONTROL OVER FINANCIAL REPORTING

Our consideration of internal control over financial reporting would not necessarily disclose all matters in the internal control over financial reporting that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants and OMB Bulletin No. 01-02, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of the internal control over financial reporting that, in our judgment, could adversely affect NSF's ability to record, process, summarize, and report financial data consistent with the assertions by management in the financial statements.

Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements, in amounts that would be material in relation to the financial statements being audited, may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal control, misstatements due to error or fraud may nevertheless occur and not be detected.

We noted certain matters, described in Exhibit 1, involving the internal control over financial reporting and its operation that we consider to be reportable conditions. However, none of the reportable conditions are believed to be material weaknesses.

We also noted other matters involving internal control over financial reporting and its operation, which we do not consider to be reportable conditions, that we have reported to the management of NSF in a separate letter dated January 18, 2002.

COMPLIANCE WITH LAWS AND REGULATIONS

The results of our tests of compliance with certain provisions of laws and regulations, exclusive of those referred to in the FFMIA of 1996, disclosed one instance of potential noncompliance in FY 2000 that was required to be reported under *Government Auditing Standards* and OMB Bulletin No. 01-02. This matter related to potential noncompliance with Federal appropriations law arising from NSF expending funds from its Research and Related Activities appropriation to supplement potential shortfalls in its Major Research Equipment appropriation for a large international project. This potential noncompliance was identified in a report issued by the NSF Office of Inspector General in December 2000. This condition was resolved in FY 2001.

The results of our tests of compliance with certain provisions of other laws and regulations, exclusive of FFMIA, disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 01-02.

The results of our tests of compliance with FFMIA Section 803(a) requirements disclosed an instance, described in Exhibits 1 and 2, in which NSF's financial management systems did not substantially comply with Federal financial management systems requirements. As agreed with NSF management, the descriptions in Exhibits 1 and 2 do not address certain matters required by FFMIA Section 803 (b)(2) because of the sensitivity of such matters. These matters were provided in separate oral communications and a written communication to management dated December 7, 2001. The results of our tests disclosed no instances in which NSF's financial management systems did not substantially comply with applicable Federal accounting standards or the United States Government Standard General Ledger at the transaction level.

We noted other matters involving compliance with laws and regulations that we do not consider to be material non-compliance, which have been reported to the management of NSF in a separate letter dated January 18, 2002.

RESPONSIBILITIES

Management's Responsibilities. The Government Management Reform Act (GMRA) of 1994 requires Federal agencies to report annually to Congress on their financial status and any other information needed to fairly present the agencies' financial position and results of operations. To meet the GMRA reporting requirements, NSF prepares annual financial statements.

Management is responsible for:

- Preparing the financial statements in conformity with accounting principles generally accepted in the United States of America, and for preparing the other information contained in the FY 2001 Accountability Report.

- Establishing and maintaining internal controls over financial reporting, Required Supplementary Information, Required Supplementary Stewardship Information, and performance measures.

- Complying with laws and regulations, including FFMIA.

In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of internal control policies.

Auditors' Responsibilities. Our responsibility is to express an opinion on the financial statements of NSF as of and for the years ended September 30, 2001 and 2000, based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*; and OMB Bulletin No. 01-02. Those standards and OMB Bulletin No. 01-02 require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In planning and performing our FY 2001 audit, we considered NSF's internal control over financial reporting by obtaining an understanding of NSF's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 01-02 and *Government Auditing Standards*. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982. The objective of our audit was not to provide assurance on NSF's internal control over financial reporting. Consequently, we do not provide an opinion on internal control over financial reporting.

As required by OMB Bulletin No. 01-02, we considered NSF's internal control over *Required Supplementary Stewardship Information* by obtaining an understanding of NSF's internal control, determining whether these internal controls had been placed in operation, assessing control risk, and performing tests of controls. Our procedures were not designed to provide assurance on internal control over *Required Supplementary Stewardship Information*, and, accordingly, we do not provide an opinion on such controls.

As further required by OMB Bulletin No. 01-02, with respect to internal control related to performance measures determined by management to be key and reported in *Management's Discussion and Analysis*, we obtained an understanding of the design of significant internal controls relating to the existence and completeness assertions and determined whether they had been placed in operation. Our procedures were not designed to provide assurance on internal control over reported performance measures, and, accordingly, we do not provide an opinion on such controls.

As part of obtaining reasonable assurance about whether the NSF's financial statements are free of material misstatement, we performed tests of NSF's compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of the financial statement amounts, and certain provisions of other laws and regulations specified on OMB Bulletin No. 01-02, including certain requirements referred to in FFMIA. We limited our tests of compliance to these provisions described in the preceding sentence, and did not test compliance with all laws and regulations applicable to NSF. However, providing an opinion on compliance with laws and regulations was not an objective of our audit, and, accordingly, we do not express such an opinion.

Under OMB Bulletin No. 01-02 and FFMIA, we are required to report whether NSF's financial management systems substantially comply with (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States

Government Standard General Ledger at the transaction level. To meet this requirement, we performed tests of compliance with FFMIA Section 803(a) requirements.

DISTRIBUTION

This report is intended solely for the information and use of NSF's management, the NSF Office of Inspector General, OMB, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

January 18, 2002

Exhibit 1

Reportable Conditions

01-01 Post-award Management

The National Science Foundation (NSF) awards grants to various organizations, including colleges and universities, non-profit organizations, state and local governments, Federally Funded Research and Development Centers, and private foundations that are intended to promote and advance scientific progress in the United States. Through an award, NSF enters into relationships to fund a particular research activity conducted by grantees. NSF expends approximately 90% of its appropriated funds on grants in a given year. The following paragraphs discuss weaknesses noted in internal control over post-award management.

A. Financial Monitoring of Grant Awards

Our audit revealed that even though NSF has a robust system of award management over its pre-award and award phases, NSF does not have a comprehensive, risk-based internal grants management program to monitor its post-award phase, which should include more in-depth reviews of the administrative and financial management practices and compliance with laws and regulations at awardee institutions. At any point in time, NSF staff is engaged in administering as many as 20,000 active awards. This is a formidable task, in addition to their responsibility for soliciting and awarding approximately 10,000 new grants and cooperative agreements annually.

Over the years, NSF has utilized an award management system that strikes a careful balance of invested resources and oversight through an integrated process involving programmatic, financial and administrative staff. NSF's award management system includes a financial and administrative monitoring component, including the submission of financial status reports throughout the award continuum, but post-award monitoring is not systematic, risk-based, documented in writing, or consistently applied. In addition, NSF's awards are becoming larger, more cross-disciplinary and more complex in nature. Federal requirements are increasingly calling for improved accountability and Federal management of payments through improved internal controls.

NSF's post-award grantee monitoring procedures primarily consist of reviews of the grantee's Office of Management and Budget (OMB) Circular A-133, *Audits of States, Local Governments and Non Profit Organizations* audit reports, cost-incurred audits conducted on selected grantees by the NSF Office of Inspector General, and site visits to a few grantees that have been conducted by NSF staff as a result of concerns identified by NSF administrative and program office staff.

Our review of NSF's grant monitoring processes revealed that in general NSF should improve post-award monitoring by establishing written policies and procedures to ensure awardees' financial and administrative compliance with award terms and conditions. Specifically:

- There is no comprehensive risk-based program for financial monitoring of awards, which describes who will conduct the monitoring, the manner in which it will be performed, and when and what type of monitoring activities are planned;
- There are no systemic risk assessment processes in place to classify grantees into various risk categories, i.e., low, medium, and high; and
- Monitoring tools are not utilized to ensure that periodic and consistent review procedures are conducted to assess the financial management practices of grantees and to review financial information reported by grantees.

As a result, awardees' use of Federal funds may not be consistent with the objectives of the grant; programs and resources may not be protected from waste, fraud, and mismanagement; laws and regulations may not be followed; and reliable and timely information may not be obtained, maintained, reported, or used for decision-making. Additionally, since NSF grantee expenditures represent approximately 90% of total NSF expenditures for the year, the integrity and accuracy of grantee expenditures recorded by NSF may be compromised. NSF's Office of Inspector General's Semiannual reports continue to reveal material non-compliance with Federal regulations and awardee terms and conditions and material internal control weaknesses at awardee institutions. Instances noted at awardee institutions include missing or insufficient documentation for costs claimed on the awards; inadequate accounting systems, which do not properly record timekeeping, monitored workload systems, indirect costs, and cost-sharing allocations; and inadequate monitoring of subawards.

OMB Circular A-123, *Management Accountability and Control*, states that as Federal employees develop and execute strategies for implementing or re-engineering agency programs and operations, they should design management structures that help ensure accountability for results. As part of this process, agencies and individual Federal managers must take systematic and proactive measures to develop and implement appropriate, cost-effective management controls.

Management controls are the organization, policies, and procedures used to reasonably ensure that (i) programs achieve their intended results; (ii) resources used are consistent with agency mission; (iii) programs and resources are protected from waste, fraud, and mismanagement; (iv) laws and regulations are followed; and (v) reliable and timely information is obtained, maintained, reported, and used for decision making.

NSF is responsible for ensuring that grantees comply with applicable laws and regulations related to the administration of the respective grant awards, including those related to Federal cash management requirements. Because OMB Circular A-133 audits leave the identification of major programs, which are the only programs subject to compliance testing, to the judgment of the grantees' independent auditors, there is no assurance that NSF's programs will be selected for review during OMB Circular A-133 audits. Further, some of NSF's grantees fall below the $300,000 threshold of Federal expenditures that trigger an audit under OMB Circular A-133 requirements. Therefore, a combination of an internal program of grantee oversight, including risk-based site visits to review grantee financial management

compliance, and review of OMB Circular A-133 audit reports, is required to ensure effective grantee oversight is maintained.

Recommendations

We have the following recommendations:

1. Review current monitoring practices and develop a risk based monitoring program, which should also include an assessment of the financial and programmatic risks of every NSF grantee. The monitoring program should include a combination of site visits or other monitoring procedures such as desk reviews performed at regular intervals on grantees in the various risk categories;

2. Update the current written grant monitoring procedures to include specific monitoring and documentation requirements:

   (i) Monitoring procedures should include a description of who will conduct the monitoring, the manner in which it will be done, and what type of monitoring activities should be conducted on the grantees depending on the type and level of risk; and

   (ii) Documentation procedures should require grant managers to maintain documentation in grant files on their monitoring activities, using such techniques as written reports of on-site reviews and follow up, and telephone interview write ups.

3. Develop site visit monitoring tools to aid in the grantee monitoring process. Site monitoring tools should guide the reviewer and ensure that specific financial objectives are achieved, and include steps such as:

   (i) Review of the accuracy of the amounts reported on grantee Financial Status Reports/Progress reports submitted to NSF by comparing the information in the reports to the grantee's general ledger or some other equivalent data;

   (ii) Assessment of the adequacy of financial management procedures in place at the grantee to ensure grantees have complied with the terms of their grant agreements; and

   (iii) Assessment of grantees' monitoring practices over the accuracy of amounts reported by subgrantees through review of supporting documentation or other equivalent means of review.

4. Establish a program for follow-up procedures to address concerns raised by program personnel in a timely manner.

B. Monitoring of Assets Owned by NSF in the Custody of Other Entities

Funds provided by NSF to its grantees are used in certain cases to purchase or construct Property, Plant, and Equipment (PP&E) to be used by the grantee for operations or research on the projects or programs sponsored by NSF. In most cases the title of the asset transfers to the grantee, however, in some cases, NSF retains ownership to the PP&E. In those cases, in accordance with grant terms and conditions, NSF grantees are required to submit an annual inventory listing of NSF-owned property in their custody. Although certain procedures are in place to monitor these assets, significant improvement of current policies and procedures is necessary to ensure that such assets are protected from loss, misuse, or theft, and reliable and timely information is obtained on the value of these assets.

Current accounting standards do not adequately address accounting for such assets, so NSF received interim guidance in December 1997 from the Federal Accounting Standards Advisory Board (FASAB), which requires NSF to disclose the dollar value of these assets based on information contained in audited financial statements of organizations holding the assets, if available. Additionally, OMB Circular A-110, *Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations,* requires grantees to comply with the property management standards prescribed. However, NSF has not reported all such assets in the notes to the financial statements, and also has not reviewed grantee's compliance with property management standards. The following specific deficiencies were noted concerning the management of PP&E owned by NSF in the custody of grantees:

- Current procedures are inadequate to ensure that all of NSF's grantees, i.e., colleges and universities, non-profit organizations, state and local governments, Federally Funded Research and Development Centers (FFRDC), and private foundations that have custody of NSF-owned assets, report the relevant information to NSF, as required by grant agreements and OMB Circular A-110. NSF's PP&E in the custody of FFRDCs was reported in the notes to the FY 2001 financial statements as approximately $202 million and $207 million as of September 2001 and 2000, respectively. However, NSF was unable to disclose the value of NSF-owned property in the custody of colleges and universities, non- profit organizations, state and local governments, or private foundations due to the lack of such information; and

- There are no procedures within NSF to assess the accuracy of the inventory listings of NSF-owned property that are submitted by grantees or to assess the existence and condition of these assets.

Inadequate monitoring of such PP&E could result in potential loss, misuse, or theft of NSF-owned PP&E in the custody of others as well as misstatement of the PP&E held by others that is reported in the notes to the financial statements. NSF is responsible for ensuring that its grantees comply with applicable laws and regulations related to the administration of the respective grant awards. In order to ensure proper accountability and to meet reporting requirements, grantee oversight that includes site visits to review grantee financial

management compliance is needed to ensure that recipients comply with FASAB guidance and property management standards as prescribed in OMB Circular A-110.

Recommendations

We have the following recommendations:

1. Develop procedures to ensure that all grantees report information on the PP&E that they hold but is owned by NSF. Such procedures should include the use of a checklist of grantees to identify those that have not submitted the information required. This checklist should be periodically updated so that it reflects a complete listing of grantees that have custody of NSF-owned PP&E;
2. Establish standard footnote disclosure for grantees' use to ensure that the required information is disclosed separately in each grantees' audited financial statements;
3. Establish internal procedures for an annual review of the asset inventory listings submitted by grantees for accuracy and reasonableness. These procedures should include a reconciliation to amounts disclosed as NSF's PP&E in the grantee's audited financial statements;
4. Develop procedures to periodically confirm the existence and condition of these assets. These procedures should be carried out in conjunction with other grant monitoring activities conducted during grantee site visits. Grantee's property management systems must also be reviewed during site visits to ensure compliance with OMB Circular A-110 property management standards; and
5. Request guidance from FASAB with respect to accounting and reporting of assets in the custody of others to replace the interim guidance issued in 1997.

01-02 Information Security

NSF faces the challenging task of facilitating an open research culture while protecting its critical information assets against unauthorized intrusion. Although NSF has enhanced its security program by contracting for a managed Intrusion Detection Service and appointing a Security Officer, further improvements are needed to strengthen its security environment. As agreed with NSF management, the description herein of the issue does not address certain matters required by FFMIA Section 803 (b)(2) because of the sensitivity of such matters. These matters were provided in separate oral communications and a written communication to management dated December 7, 2001. Our review of the logical and physical access controls over NSF facilities, information system resources, applications, and data identified certain vulnerabilities in the design, administration, and monitoring of these controls. Specifically, we have noted weaknesses in:

- Application security design;
- Database security;

- Intrusion detection;
- Network infrastructure security;
- File sharing and remote access;
- Read and write access to certain application source code;
- Physical access; and
- Administration of access privileges.

The Computer Security Act requires Federal agencies to identify and provide security protection commensurate with the risk resulting from the loss of, misuse of, or unauthorized access to, or modification of, information collected or maintained by or on behalf of the agency. The Government Information Security Reform Act (GISRA) re-emphasizes that, as part of an agency-wide security program, agencies need to ensure that proper security controls are in place to manage information systems security throughout the life cycle of a system.

To accomplish NSF's mission of promoting science and engineering, research, and education, an open and distributed computing environment is a means for collaboration and knowledge sharing. Implementing and maintaining a secure computing environment is a significant challenge and requires senior management sponsorship and dedicated resources.

Although certain improvements to security were made subsequent to year-end, and NSF has been extremely responsive in initiating corrective actions for vulnerabilities identified during the audit, the mainframe to client-server migration of NSF's financial applications, limited resources, and competing management priorities are some of the reasons for the noted vulnerabilities. As a result, information security weaknesses could adversely affect NSF's ability to produce accurate data for decision-making and financial reporting because such weaknesses could compromise the reliability and availability of data that are recorded in or transmitted by NSF's financial management systems.

These vulnerabilities increase the risk of unauthorized viewing, modification, and deletion of financial and other sensitive data, accidentally or intentionally, by internal and external parties.

Recommendations

We recommend that NSF ensure that:

1. The security design framework for client server applications is further reviewed to assess the risk of unauthorized viewing, modification, and deletion of financial and other sensitive data. Options should then be evaluated to either correct the vulnerabilities noted or implement mitigating security controls;

2. Access controls to critical database tables, as well as their configuration, is strengthened;

3. Intrusion detection capabilities are further refined and implemented;

4. An entity-wide software patch management process is implemented whereby vulnerabilities are identified and related patches tested and applied in a timely manner;

5. File sharing and remote access policies prohibiting the use of unauthorized connections are established, enforced, and monitored;

6. Software libraries are protected from unauthorized viewing and modification of application source code;

7. An assessment of physical controls is performed utilizing a cost-benefit analysis to identify options to limit further the access to facilities and information system resources. Based on the option selected, implement the applicable controls to enhance NSF physical access; and

8. Access privileges to the facilities and information systems are revoked in a timely manner when a user leaves NSF.

Exhibit 2

Compliance with Laws and Regulations

FY 2001 Non-Compliance with Laws and Regulations

Federal Financial Management Improvement Act of 1996 (FFMIA): FFMIA requires NSF to implement and maintain a financial management system that complies substantially with: (1) Federal requirements for financial management systems; (2) applicable Federal accounting standards; and (3) requirements to post transactions to the United States Standard General Ledger at the transaction level. These requirements are detailed in OMB Circular A-127, *Policies and Standards for Financial Management Systems.* Section 7 of this Circular identifies the requirements or characteristics that Federal financial management systems should possess. Additionally, the *Revised Implementation Guidance for FFMIA*, dated January 4, 2001 issued by the Office of Management and Budget, provides factors in determining the level of compliance required by Federal agencies.

NSF's noncompliance with FFMIA requirements relates to Federal financial management system requirements. As discussed separately in the report on internal control, NSF has several weaknesses in its entity-wide security that contribute to noncompliance with OMB Circular A-130, *Management of Federal Information Resources.* As agreed with NSF management, the description herein of the issue does not address certain matters required by FFMIA Section 803 (b)(2) because of the sensitivity of such matters. These matters were provided in separate oral communications and a written communication to management dated December 7, 2001. NSF has been extremely responsive in initiating corrective actions for vulnerabilities identified during the audit. We have been informed that certain improvements to security were made subsequent to year-end, but we have not tested this assertion. The mainframe to client-server migration of NSF's financial applications, limited resources, and competing management priorities are some of the reasons for the noted vulnerabilities. NSF should continue to improve its security-related management control processes to better protect physical and logical assets from unauthorized access or improper use.

Recommendations

We recommend that NSF management institute appropriate procedures to ensure compliance with FFMIA requirements.

Status of FY 2000 Potential Non-Compliance with Laws and Regulations

Federal Appropriations Law: This instance of reportable potential noncompliance with Federal appropriations law arose from NSF expending funds from its Research and Related Activities appropriation to supplement potential shortfalls in its Major Research Equipment appropriation for a large international project. This potential noncompliance with law was identified in a report issued by the NSF Office of Inspector General in December 2000. This condition was resolved in FY 2001.

Attachment 1

Management's Response to Auditors' Report

February 26, 2001

To: Christine C. Boesz
Inspector General

From: Thomas Cooley
Chief Financial Officer

Subject Management's Response to Independent Auditors' Report
Fiscal Years 2001 and 2000

This memorandum and attachments transmit NSF management's response to KPMG LLP's audit report for fiscal years 2001 and 2000. We understand that our responses will be included as an attachment to your report.

SUMMARY

The auditors' report concluded that NSF's financial statements as of and for the years ended September 30, 2001 and 2000, are presented fairly, in all material respects, in conformity with generally accepted accounting principles in the United States of America.

Reportable Conditions

The auditors' report identified the following conditions that they consider to be reportable conditions.

- ***Post-Award Management*** - Adequate procedures for monitoring (i) awardees' administrative and financial management practices and compliance with laws and regulations, and (ii) NSF-owned property, plant and equipment in awardees' custody are not in place.

- ***Information Security*** - NSF has several weaknesses in its entity-wide information security that result in vulnerabilities in logical and physical access controls.

NSF Management Response*: NSF management believes that the identified conditions are not "significant deficiencies in the design or operation of the internal control over financial reporting that . . . could adversely affect NSF's ability to record, process, summarize, and report financial data consistent with the assertions by management in the financial statements". As detailed in Attachment 1, our procedures for grant monitoring are demonstratively effective and our comprehensive approach for assuring the security*

of information and assets includes layers of controls that mitigate the risk of a vulnerability that would result in a significant misstatement of the NSF Financial Statement that would also not be detected by systems controls or employees in the normal course of performing their functions.

Compliance with Laws and Regulations

Tests of compliance with certain provisions of laws and regulations, exclusive of those referred to in the Federal Financial Management Improvement Act (FFMIA) of 1996, disclosed no instance of noncompliance in Fiscal Year (FY) 2001. Tests of compliance with FFMIA Section 803(a) requirements, however, were believed to disclose instances where NSF's financial management systems did not substantially comply with Federal financial management systems requirements.

***NSF Management Response**: NSF management disagrees with the assertion that our financial management systems do not substantially comply with Federal financial management systems requirements. As noted above and detailed in Attachment 1, our comprehensive approach to information security is compliant with OMB Circular A-130, Management of Federal Information Resources, and with the FFMIA. Moreover, even if a reportable condition existed as to information security, under the guidance provided by OMB that does not justify a finding of noncompliance with the FFMIA. The Director of NSF has determined that the agency is in substantial compliance with the FFMIA.*

NSF management appreciates the cooperation extended by both the Office of Inspector General and KPMG throughout the audit process.

cc: Dr. Eamon M. Kelly

Attachment 1

Management's Responses to Auditors' Report

Management's Response to 01-01 Post-Award Management

NSF management does not agree that "[a]dequate procedures for monitoring (i) awardees' administrative and financial management practices and compliance with laws and regulations; and (ii) NSF-owned property, plant and equipment in awardees' custody are not in place" as asserted in the summary and expanded on later in the report. The assertion is unsupported by the record and does not accurately represent the processes, policies and procedures that govern NSF's award management system, including the documented internal controls that exist throughout that system. Indeed, NSF's post-award management internal controls are neither materially nor significantly weak; NSF post-award oversight of grants is as robust and effective as NSF pre-award and award oversight.

a. Financial Monitoring of Grant Awards

For fifty-two years the National Science Foundation has utilized an award management system that strikes a careful balance of invested resources and oversight. Through an integrated process involving programmatic, financial, and administrative staff, NSF monitors its awardees' expenditures. This approach has proved remarkably, though not surprisingly, effective.

The Office of Inspector General has tested NSF's award management over the past four years by auditing over $1.5 billion in grant awards. As a result of those audits for fiscal years 1998 - 2001, approximately .2% of audited award funds were "recovered" due to misspending. Given the likelihood that these audits were undertaken for NSF's higher risk activities, we believe that an audit of every dollar of funds awarded and managed by NSF would result in no higher a recovery. Based on this record alone, we do not agree that an award management system in which approximately 99.8 percent of financial assistance was properly spent can be reasonably characterized as having a significant deficiency in its design or operation.

Notwithstanding the de minimus level of misspending found by the Office of Inspector General, NSF seeks always to improve our processes. To that end, we are refining our award management process to include a more structured risk-based monitoring element. This effort includes the development of standard tools and protocols, specifically for on-site monitoring; an FTE analysis to identify additional staff resources needed; and a staff training component

Overview

Consistent with the government-wide purposes of Federal financial assistance programs, specific methods for monitoring and oversight are not codified in statute or regulation. Rather, award monitoring activity relies on individual agency policies and practices and is subject to established agency internal controls. In fact, the Administrative Requirements of OMB Circulars A-102 and A-110 vest primary responsibility for post-award financial oversight with the recipient of Federal funding. Loosely put, the overall purpose of Federal oversight is to provide accountability for Federal funds primarily by ensuring that the funding provided is used

in support of the respective programmatic effort described in the grant or cooperative agreement, consistent with any terms and conditions attached.

This does not mean, however, that there are not carefully-constructed government-wide mechanisms for assuring awardee compliance with the administrative and financial requirements imposed on all recipients of Federal assistance. Indeed, in recognition of the need for government-wide efficiency and in the interest of minimizing the reporting burden born by awardees, OMB implemented the A-133 process. By design, the A-133 process allows Federal awarding agencies to rely on a cognizant (or oversight) agency for audit responsibilities to oversee an awardee's financial and administrative processes. (See subpart D in the circular.) Most NSF awardees are overseen by either the Department of Health and Human Services or the Department of Defense. These agencies assure that awardees' systems fulfill Federal requirements.

The bedrock of NSF's post-award management is the program officer's certification that the funded science and engineering research and education has been demonstrated. Funds are not obligated absent this front-line review of substantive progress. This inherent control is fundamental to NSF's oversight process. NSF, the principal investigator and the grantee share a common interest in advancing the inquiry/education proposed by the principal investigator. A grantee cannot complete a proposed project without expending our funds properly — on researchers' salaries, equipment cost, and so forth. This process is described in chapter X, Award and Administration, of the Proposal and Award Manual and explained to all new program officers when they join the Foundation. The periodic reports on which the program officer's certification is based document both the grantee's progress and the program officer review.

Programmatic grant oversight is complemented by the work of NSF's Budget, Finance, and Award Management staff (BFA) and Division of Grants and Agreements staff (DGA). For example, prior to approving continuing grant increments that involve changes to the original commitment amount, grants officers perform financial and administrative reviews for compliance with terms and conditions, including compliance with reporting requirements. In cooperation with program staff, BFA and DGA ensure that resources are used consistent with agency mission; that laws and regulations are followed; and that timely information is obtained and maintained. Policies and procedures governing these awards management activities are documented in the following:

- The Proposal and Award Manual
- The Grant Policy Manual
- DGA Standing Operating Guidance
- The Grant Proposal Guide
- NSF Bulletins

Not a Reportable Condition

OMB Bulletin 01-02 defines a "reportable condition" as a matter coming to the auditor's attention that, in the auditor's judgment, should be communicated because it represents a significant deficiency in the design or operation of internal control, that could adversely affect

the organization's ability to record, process, summarize, and report financial data consistent with the assertions by management in the financial statements. The fact that the Foundation's grant oversight procedures have consistently resulted in a de minimus level of misspending supports management's position that there are no significant deficiencies in the design or operation of our post-award monitoring processes. The risk that substantial funds could be misspent in any one project without timely detection by a Program Officer or Grants and Agreements Officer is very small. The risk that such misspending could occur under enough grants to total a significant sum is even smaller.

A specific discussion of the major points made in section 01-01.A and a fuller explanation of NSF's grant monitoring process follows.

1. The need for a comprehensive, risk-based internal grants management program to monitor grantee administrative and financial management

The auditors say that "NSF should improve post-award monitoring by establishing written policies and procedures to ensure awardees' financial and administrative compliance with award terms and conditions". They claim:

- There is no comprehensive risk-based program for financial monitoring of awards, which describes who will conduct the monitoring, the manner in which it will be performed, and when and what type of monitoring activities are planned;
- There are no systemic risk assessment processes in place to classify grantees into various risk categories, i.e., low, medium, and high; and
- Monitoring tools are not utilized to ensure that periodic and consistent review procedures are conducted to assess the financial management practices of grantees and to review financial information reported by grantees.

The auditors conclude from the above assertions that grantees' use of Federal funds may not be consistent with the objectives of the grant; programs and resources may not be protected from waste, fraud, and mismanagement; laws and regulations may not be followed, and reliable and timely information may not be obtained, reported, or used for decision-making.

NSF Management Response

During the past year, the Division of Grants and Agreements (DGA) within the Office of Budget, Finance and Award Management (BFA) has taken steps to increase its award monitoring activity particularly in the areas of post-award review, risk assessment methodology, and on-site reviews. We have presented our plan of action in a variety of forums over the past six months, and the Office of Inspector General has agreed to our approach, including the broad categories of risk we are targeting. These included presentations to the Audit and Oversight Committee of the National Science Board, the October 2001 Audit Control Committee meeting, the October 2001 Management Controls Committee Meeting, the Fall 2001 Business and Operations Advisory Committee and a recent January 2002 meeting between the Division Director, DGA and the Deputy Inspector General and IG staff.

The categories of risk we have developed include the following:

- Financial: including an assessment of accounting systems, cost sharing activity, and indirect cost application;
- Administrative: including type of awardee institution, property oversight, cognizant agency responsibility, reporting requirements, and assessment of compliance with terms and conditions of an award;
- Programmatic: addressing oversight needs for large multi-user facilities, new innovative project requirements, and specific ad-hoc review requests.

As further demonstration of management's commitment to instituting a formal risk assessment to post-award, on-site financial and administrative monitoring, DGA has established two positions focused on these efforts. DGA completed its recruitment for a Senior Advisor for Workforce Planning, Operations, and Risk Management established in October 2001. The incumbent is developing the comprehensive risk-based assessment methodology for financial and administrative monitoring of all awards which will be used to determine which awards require close monitoring as well as priority site visits. Data analysis is currently underway to identify the subset of awards that have a relatively higher risk potential and, thus, require a greater degree of oversight.

DGA has established and filled the position of the Advisor for Facilities Monitoring and Oversight. The incumbent has led the development of specialized tools that will be used in conducting Total Business System Reviews of all large facilities. The incumbent is also part of a Foundation effort to develop Oversight Policies and Procedures for Large Facilities.

In addition to these DGA positions, NSF is currently recruiting for a Large Facilities Project Deputy Director in BFA. This individual will be responsible for business oversight for large facilities, already identified by the OIG as NSF's highest risk awards, i.e., those with considerable costs, schedule, and performance issues. The targeted oversight contemplated through the Large Facilities staffing complement will substantially mitigate NSF's existing risk.

The Chief Financial Officer has provided additional staffing, training, and travel resources devoted to monitoring and oversight activities and has committed to increase those resources as we continue expansion of grant monitoring activities. We recognize the value to be gained by increasing our grant monitoring oversight activities and are taking steps to improve it.

Equally important is a contextual discussion of the long-standing risk assessment activities and internal controls that are currently integrated into NSF's awards management practices and system. This detailed discussion follows.

2. Grantee compliance through internal oversight, including risk-based site visits and a review of OMB Circular A-133 audit reports

"NSF is responsible for ensuring that grantees comply with applicable laws and regulations related to the administration of the respective grant awards, including those related to Federal cash management requirements. . . . [A] combination of an internal program of grantee

oversight, including risk-based site visits to review grantee financial management compliance, and review of OMB Circular A-133 audit reports, is required to ensure effective grantee oversight is maintained."

NSF Management Response

NSF management agrees there is a need to increase risk-based, on-site grant monitoring and agrees with its categorization as a management challenge. Our earlier discussion of the NSF risk assessment plan for on-site financial monitoring describes the broad categories of risk that motivate the plan. These on-site activities will supplement our current awards management system that includes a substantial financial and administrative monitoring component, including the submission of financial status reports, throughout the award continuum.

The risk assessment methodology being employed to develop DGA's on-site monitoring plan is merely an extension of existing agency protocols. The awards management continuum and the internal controls that safeguard Federal funds is a thoroughly documented business system. In addition, the business rules and internal controls that are programmed into the automated award system implement these official NSF policies and procedures and document each transaction, by institution and award.

Financial and administrative management integrating risk assessment begins pre-award, with the assignment of each pending action to an appropriately warranted DGA specialist. The specialist warrant level, I-IV, limits those actions by type and dollar value that the respective grants officer may process, review, and sign. Warrant levels are memorialized in the official "Delegation of Grants Officer Authority" and they are recorded in the awards system User Profile that ensures the proper exercise of delegated authority to obligate Federal funds.

Grants officers analyze 100% of proposed project budgets to ensure compliance with the OMB circulars governing cost principles. In order to make a determination on the type of award instrument with appropriate terms and conditions consistent with Federal law and guidelines and NSF policy, the grants officer analyzes such risk factors as institutional type, proposed dollar amount and project type. Consistent with chapter 63 of title 31 of the United States Code (originally enacted as the "Federal Grant and Cooperative Agreement Act of 1977"), grant agreements are used to support respective programmatic efforts when no substantial Federal involvement is contemplated. Funding is provided through cooperative agreements for those projects where substantial Federal involvement is contemplated.

When special conditions concerning such items as equipment or indirect cost rates are attached to an award, special attention flags are set in the award system. Prior to award close-out, these conditions must be satisfied.

Grants officers, with Cost Analysis and Audit Resolution (CAAR) staff, conduct an additional level of review for all new awardees in order to assess financial capability and business system adequacy. DGA may determine, as a result of these reviews, that specialized award language to limit expenditures must be applied to higher risk awards. This would trigger post award review and oversight, prior to the release of additional funds.

These pre-award monitoring processes provide the foundation for the integrity of NSF's post-award oversight.

The procedures for all of the foregoing financial and administrative award management activities are fully documented in NSF policy documents and DGA standing operating guidelines. These, in turn, are consistent with all applicable OMB Circulars governing the award and management of Federal financial assistance.

BFA has the responsibility for A-133 audit review and resolution. This Federal Government-wide required process supplements our award management activities. The $300,000 threshold for A-133 audit review is a government-wide threshold of acceptable risk. This threshold was established after careful consideration of cost efficiency and effectiveness. Based on studies done by the General Accounting Office (GAO), the audit threshold of $300,000 captures more than 90% of Federal awards expended. We do not intend to review those awards not subject to A-133 audit requirements unless they possess characteristics identified through application of the risk-based criteria.

b. Monitoring of Assets Owned by NSF in the Custody of Other Entities

Management disagrees with the finding in section 01-01.B that the monitoring of assets owned by NSF in the custody of other entities is a reportable condition.

Overview

NSF takes title to property purchased under a grant for a number of reasons, but always with the intention that it remain in the custody of the grantee for its useful life and be used by researchers. The continued existence and usefulness of such property is continually attested to by our receipt of proposed research projects employing it. We can rely on our grantee to inform us, through a request for upgrade or replacement, when the property deteriorates, even if only compared to newly-available devices. We have no need to track the historic or current value of NSF-owned property because we never depreciate or sell it. As discussed below, the annual addition to this total value is immaterial. Although the total value of such property might seem significant, it is actually a "sunk cost".

Not a Reportable Condition

Again, OMB Bulletin 01-02 defines a "reportable condition" as a matter coming to the auditor's attention that, in the auditor's judgment, should be communicated because it represents a significant deficiency in the design or operation of internal control, that could adversely affect the organization's ability to record, process, summarize, and report financial data consistent with the assertions by management in the financial statements.

A specific discussion of the major points made in section 01-01.B and a fuller explanation of NSF's property monitoring process follows.

1. Current procedures are inadequate to ensure that all of NSF grantees…that have custody of NSF assets report the relevant information to NSF, as required by grant agreements. …NSF was unable to disclose the value of NSF owned property in the custody of colleges and universities and other non-profit entities in Fiscal Year 2001 as required due to the lack of such information.

NSF Management Response

The Foundation supports the scientific infrastructure at academic institutions by providing equipment to support these activities. Title to this property remains vested with the institution in accordance with established Federal administrative requirements governing grant-funded property. The institutions are required to inventory this equipment and maintain this inventory for review. These inventories have been site tested and we have relied on A-133 audit system reviews to insure that appropriate processes and procedures are in place to insure compliance with the requirement.

However, during the pre-award monitoring review, there are a few instances where a program identifies certain items of equipment for which the Government should retain title. Specifically, title to equipment purchased by profit makers, by policy, rests with the Government. Appropriate terms and conditions are applied to the award requiring awardee notification to NSF of the item of equipment. These instances are flagged in our database. A recent review of the database indicates that there are currently nine active grant awards (other than the Federally Funded Research and Development Centers (FFDRC), large facility activities, and contracts) with government-owned property requirements. These include five profit makers, one non-profit, and three academic institutions. The total amount of equipment budgeted in these awards amounts to less than $500,000 out of almost $334 million funded for equipment in FY 2001. There are some cases that have expired and are in the process of being reviewed for disposition. The equipment budget amount for these represents $1.8 million — that is less than 1% of the universe of equipment dollars awarded in FY 2001. In our opinion, this does not rise to the level of significance and no problem with it would have a significant effect on our financial or performance reporting or compliance with applicable laws or regulations.

We should point out that there is no current requirement for recordation as an asset in NSF's financial statements for NSF owned property in the custody of colleges, universities, and other nonprofit organizations. The interim guidance provided us by the Federal Accounting Standards Advisory Board merely says we should disclose that information if it is available.

2. There are no procedures within NSF to assess the accuracy of the inventory listings of NSF-owned property that are submitted by grantees or to assess the existence and condition of these assets.

NSF Management Response

We do monitor inventories of our FFRDCs and have included totals for government owned property in our financial statements. Government owned property maintained by the FFRDCs totals almost $202 million. We have conducted periodic site visit reviews to test the inventories

listings and have included these reviews as part of our developing Total Business System Review (TBSR) protocols that will be used for our large centers and facilities. Finally, we have identified on-site property review in our risk assessment protocol and our business review instrument to ensure compliance with A-110 requirements.

NSF Management Response to Recommendations in 01-01

We appreciate the substance of the four recommendations on Financial Monitoring of Grant Awards, as they relate to risk-based monitoring. As the Office of the Inspector General is fully aware, the Division of Grants and Agreements is diligently developing a comprehensive methodology. Those efforts have been substantiated in the foregoing discussion. Nonetheless, we invite OIG's participation in the review of our risk assessment methodology and procedures beginning in April 2002. Furthermore, many of the documentation issues within the recommendations are being addressed in the electronic jacket initiative.

Management agrees with your recommendations to develop effective monitoring tools to ensure compliance with property reporting requirements, and we will put in place additional internal procedures to review the annual listing from awardees for accuracy and reasonableness. We have also identified on-site property review in our risk assessment protocol and our business review instrument to ensure compliance with A-110 requirements.

Management's Response to 01-02 Information Security

Management strongly disagrees with the finding that the items mentioned as weaknesses represent significant deficiencies that rise to the level of a "reportable condition." NSF has a comprehensive approach for assuring the security of its information and assets. Layers of controls mitigate the risk of a vulnerability that would result in a significant misstatement of the NSF Financial Statement that would also not be detected by systems controls or employees in the normal course of performing their functions. The auditors' report fails to demonstrate any significant deficiencies in the design or operation of NSF's security controls.

Specifically, the FFMIA – Computer Security Act Requirements that are the subject of the finding and recommendations are part of a larger Information Technology Security program at the National Science Foundation. The National Science Foundation is focused on assuring that NSF infrastructure and critical assets are appropriately protected while maintaining an open and collaborative environment for scientific research and discovery. We have established a strong and comprehensive Information Technology Security program that is consistent with Government-wide guidance and patterned after industry best practices. The majority of NSF's significant information technology assets are managed within the Office of Information and Resource Management, which is thus the organizational focus of NSF's Information Technology Security program. OIRM administers NSF's sophisticated technological infrastructure, providing the hardware, software and support systems necessary to manage the Foundation's grant-making process and to maintain advanced financial and accounting systems. The NSF Chief Information Officer (CIO) provides overall leadership for the Information Technology Security Program, and ensures that policy, procedures, and activities are coordinated among OIRM Divisions and other NSF program management and research initiatives.

NSF's information security approach is based on a fundamental philosophy of risk management where Information Technology Security risks are assessed, understood, and mitigated appropriately. This approach allows NSF to implement appropriate layers of protective measures and controls to ensure the privacy, integrity, and security of information and information technology resources needed by NSF and the broader research community while allowing appropriate access and availability to users. This layered approach effectively reduces the risk of unauthorized access to systems and information using various manual and automated checkpoints and controls.

NSF's Information Technology Security program encompasses all aspects of information security, including policy and procedures, risk assessments and security plans, managed intrusion detection services, vulnerability assessments, and technical and management security controls, as highlighted below.

- Policies and Procedures. NSF has established Information Technology Security policy, which is consistent with law, regulation, best practices, and NSF's particular requirements. NSF systems are constructed to maximize the protection of sensitive information such as the names of scientific reviewers and confidential proposal information. Operational procedures and controls are also in place to ensure the security, reliability, and integrity of information technology resources that support NSF operations.

- Security Assessments, Plans, and Controls. NSF has a comprehensive framework for establishing appropriate safeguards and controls and ensuring that they are integrated into existing and new information technology assets and resources. These include requirements for managers of mission critical systems to perform self-assessments of their systems' security posture, conduct risk assessments and develop commensurate security in accordance with OMB Circular A-130, "Management of Federal Information Resources," and have their systems certified and accredited. In the unlikely event of a major disaster, NSF has comprehensive disaster recovery plans and capabilities, which are tested on an annual basis at a hot-site location.

- Incident Detection and Response. NSF has implemented technologies and processes to ensure it is alert to intrusion attempts and is positioned to take effective action to thwart them. These include a comprehensive firewall architecture, strong network and application authentication, virus protection services, general systems security and administration and a Computer Incident Response Team (CIRT) and CIRT procedures. This team is composed of managerial and technical contacts throughout the agency who work collaboratively to respond immediately to security alerts. In FY01, NSF contracted with an independent vendor to provide managed-intrusion detection services. NSF routinely monitors security alerts from the General Services Administration FedCIRC, and the Federal Bureau of Investigation's National Information Protection Center to identify new and emerging vulnerabilities and ensure that NSF has necessary protection against threats to Information Technology Security infrastructure.

- Audits and Penetration Tests. NSF has proactively implemented scheduled vulnerability scans, penetration testing and a new intrusion detection system capability as part of the overall Information Technology Security program. These proactive measures are in addition to the annual OIG assessment using the Federal Information System Controls Audit Manual (FISCAM) and independent penetration test. Information gained from these activities and lessons learned are incorporated into ongoing operational processes and protocols.

- Training and Education. This year, NSF established computer security awareness training and made it available for all employees and on-site contractors and provided specialized courses that focused on NT and Unix security. As part of the security awareness campaign, NSF also conducted a Computer Security Awareness Day that all employees were invited to attend, brown bag seminars on various Information Technology Security related issues, and managed an ongoing security communications and outreach program for NSF employees and on-site contractors.

While much has been accomplished in each of the above areas, the Information Technology Security program must continue to be diligent and evolve to meet the inevitable threats to NSF assets and resources. Security is a global issue affecting all organizations. For example, a survey of 538 companies, universities, and government agencies by the Computer Security Institute and the FBI said that 85% of the networks were breached in the previous year ("Implementing an Information Security Program" by Kevin L. Nichols, August 2001). NSF continues to assess and evaluate improvements that can be made to improve its overall security posture. We continue to appreciate the close coordination with the OIG and its assistance in working with NSF to identify areas where improvements are appropriate, and to identify steps

that can be taken to reasonably address any areas of significant risk. Our approach is to focus on the areas which we believe are the highest risk – and to take prudent steps to mitigate them.

The presence of some vulnerabilities or risks does not necessarily constitute a "reportable condition" – rather it is an unfortunate reality of today's environment. In fact, in a recent report by the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations of the House Committee on Government Reform, two-thirds of all federal agencies were given a failing grade for efforts to secure information systems — a worse showing than last year. NSF's program was rated the best in the Federal Government, with an overall grade of "B+." This assessment, which used standard criteria across all major Government organizations, demonstrates the strength of NSF's program. The grade of "B+" also shows that we are not perfect and that there are still areas where improvements should be made. The key is to focus resources on establishing and maintaining prudent protections for those assets that are most valuable and reducing or mitigating risk to a level that is acceptable.

In addition to our position that our IT security program is comprehensive, credible, and effective, we do not believe the findings in NFR 01-02 demonstrate a "reportable condition." In OMB Bulletin No. 01-02, "Audit Requirements for Federal Financial Statements," (Dated October 16, 2000), the definition of a reportable condition is:

> "Reportable conditions" are matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal control, that could adversely affect the organization's ability to meet the objectives in paragraph 2.g. of this Bulletin.

In a document titled, "DRAFT –Sensitive Details Supporting Vulnerabilities in FISCAM 01-01, titled 'Physical and Logical Access Controls to Restrict Unauthorized Access Need Improvement'", the auditors provided information on eight vulnerabilities identified during their assessment of NSF's information systems environment. Those eight vulnerabilities formed the basis for this reportable condition finding. For a finding to be classified as a "reportable condition," there must be a showing of "… significant deficiencies in the design or operation of internal control …". While the auditors identify particular vulnerabilities, they fail to demonstrate that the vulnerabilities are the result of " significant deficiencies in the design or operation of internal control". . Specifically, the eight vulnerabilities identified are:

1) Application security design. The auditors found that the design of a third-party, commercial, off-the-shelf product allowed access to certain information. To identify this flaw, the auditors required significant knowledge of the NSF infrastructure and detailed knowledge of the NSF environment. Significant, unencumbered, internal access over a long period of time would have been required to attempt to successfully exploit this flaw. This flaw has already been permanently fixed. NSF does not consider this flaw in the third-party software to be a part of, "…significant deficiencies in the (NSF) design or operation of internal control …".

2) Database security. In this vulnerability, the auditors found that if a person were able to obtain information as a result of the flaw discussed above, they might be able to access additional information. Because of the structure of the NSF environment and the layers

of security involved, successfully using this information to carry out nefarious acts would be a difficult task. Again, this flaw has already been permanently fixed. NSF does not consider this flaw to be a part of, "…significant deficiencies in the (NSF) design or operation of internal control …".

3) Intrusion Detection. The auditors noted that the Intrusion Detection System used at NSF was not as robust as it should be. During the audit, NSF was in the midst of replacing the existing Intrusion Detection System with its first sophisticated Intrusion Detection System. The contractor encountered technical problems that delayed transition to a production status. To reduce risk further, NSF required additional work to assure that the System was adequately configured and tested for the NSF environment. While this delayed implementation for a short time, the Intrusion Detection System has been fully implemented and is working as expected, providing additional levels of defense for NSF systems. In short, the system critiqued by the auditors was being replaced during the audit by a more robust system that addresses the auditors' concerns. NSF's Intrusion Detection System is not a "…significant deficiency in the (NSF) design or operation of internal control …".

4) Network infrastructure security. This vulnerability identified by the auditors involved security upgrades provided by vendors not being installed on various systems throughout NSF on a timely basis. With over 100 servers at NSF and hundreds of third-party security flaws being fixed annually, the auditors identified eight upgrades that had not been installed on one or more systems. Of the systems identified, only four were accessible from outside NSF. On each of these systems, it would have been difficult, if not impossible to successfully exploit the vulnerability. The limited number of vulnerabilities, the extremely small risk that any of the vulnerabilities could or would be exploited, and the ability of the Intrusion Detection System to identify these types of problems indicate that this vulnerability is not a, "… significant deficiency in the design or operation of internal control …".

5) File sharing and remote access. Of the more than 1500 staff and contractors at NSF, the auditors identified one person who was not following established NSF policy, which resulted in a potential vulnerability. The one potential problem found, which was in violation of NSF policy, does not represent a, "…significant deficiency in the design or operation of internal control …".

6) Read and write access to certain application source code. The auditors stated that more Information Technology staff and contractors than was necessary had access to certain application source code. Access was given to staff and contractors based on their potential needs to access the information and to facilitate software development efforts. As a result of the auditors' recommendation, we have further limited the number of staff and contractors having access. The fact that staff and contractors may have inadvertently had access to more items than was absolutely necessary to do their job does not represent a, "… significant deficiency in the design or operation of internal control …".

7) Physical access. The auditors reference three problems that they identified regarding physical access to the NSF facilities in Ballston. Physical security is a problem for every

organization. A GAO study found that virtually every Federal Government building, even those with the tightest security, could be easily accessed. Improvements to the physical security of the NSF buildings have been made each of the last several years. Many physical security measures that are found to have problems are a result of human error. While training and education can help reduce the potential vulnerabilities, it will be extremely difficult and expensive to eliminate them. Each of the problems identified by the auditors were the result of human error that was in violation of existing NSF policy. This does not represent a, "… significant deficiency in the design or operation of internal control …".

8) Administration of access privileges to information systems and facilities. The auditors found access to NSF systems was not immediately revoked for a few persons when they stopped working for the agency. This is in comparison to hundreds of staff and contractors who leave the agency annually. In the past year, NSF has taken many measures to improve the procedures. In this year's assessment, the number of problems identified had been reduced substantially from previous years. We plan to implement stronger automated processes in an attempt to reduce the human errors that are the source of the remaining problems. The fact that a few former staff and contractors did not have all of their various accesses immediately revoked is not a, "… significant deficiency in the design or operation of internal control …".

We are pleased to report that corrective action has already been taken to minimize or eliminate each of the specific vulnerabilities mentioned. Where appropriate, additional procedures will be implemented during FY02 to limit the possibility of similar vulnerabilities occurring in the future.

NSF management believes that our systems' multi-layered controls (such as network access controls, systems access controls, inter-system access controls, database access controls, user access controls, file access controls, segregation of duties controls, application systems logical access controls, and others) ensure the reliability and availability of data that are recorded or transmitted by NSF's financial management systems.

For example, in their discussion of vulnerabilities from an outsider, the KPMG auditors state,

> While we exploited these vulnerabilities, mitigating controls, including a firewall team that reviews security logs and the NSF's outsourced intrusion detection system, exist thereby reducing the risks of unauthorized access occurring without NSF detection.

For any significant fraudulent financial transaction to not be noticed by employees in the normal course of performing their assigned functions would be extremely difficult. NSF has a series of internal controls that are used to assess any potential problems with financial management information. The controls include FAS-provided on-line management reports used by offices to monitor financial transactions as well as timely reconciliation of financial transactions made by DFM. Both are sufficient to detect any inconsistencies with the NSF financial system. Offices routinely review obligations made against their allocations and would alert DFM to potential inconstancies within their Budget Execution Plans. This would result in quick detection of any potential misuse of funds. Also, to accomplish a fraudulent NSF payment transaction, someone

must have both the Treasury certification knowledge, access, and passwords controls as well as detailed knowledge of NSF financial systems. The multi-layered nature of controls among various systems contributes to the adequacy of the design and operation of NSF's logical and physical access controls.

There is a low level of risk of a serious incident occurring. Any serious incident would be noticed by those responsible for the many layers of controls that are in place. While the audit identified some vulnerabilities in certain layers of controls, other layers of controls are in place and functioning properly to detect and mitigate this. We will continue to monitor and strengthen these controls.

In 01-02, the auditors state the seriousness of all the problems they identified by saying in summary,

> "As a result, information security weaknesses could adversely affect NSF's ability to produce accurate data for decision-making and financial reporting because such weaknesses could compromise the reliability and availability of data that are recorded in or transmitted by NSF's financial management systems."

and,

> "These vulnerabilities increase the risk of unauthorized viewing, modification, and deletion of financial and other sensitive data, accidentally or intentionally, by internal or external parties."

These statements do not identify or discuss any significant deficiencies in the design or operation of internal controls. They simply assert that security weaknesses can lead to problems. This seems to be the standard to which NSF is being held – that any security weakness can lead to problems that might be significant. Thus, it seems the auditors have classified the presence of any security weaknesses as a "significant deficiency" and therefore, a "reportable condition."

The National Science Foundation remains committed to a reliable and secure information technology infrastructure. We will continue to expand and refine the program to provide even better safeguards in the future. We appreciate all of the work that was done by the Office of the Inspector General as part of this year's assessment of the information technology environment. This work is extremely valuable to the agency in assisting in the identification of any problems that may not have yet been resolved. The results are very beneficial to NSF and have already resulted in an improved infrastructure.

NSF Management Response to Recommendations in 01-02

Because of the sensitive nature of management's response to the auditors' recommendations, they have been provided under separate cover to the Office of the Inspector General.

Management Response to Non-Compliance with Laws and Regulations

NSF management disagrees with the assertion that several weaknesses in the Foundation's entity-wide security render the agency noncompliant with OMB Circular A-130, Management of Federal Information Resources, and therefore the Federal Financial Management Improvement Act of 1996 (FFMIA). As detailed in our response to the material in 01-02 Information Security, NSF's information security program is comprehensive, credible, and effective and substantially complies with all relevant requirements.

The auditors' report fails to support its assertion of noncompliance. The report simply states that NSF's noncompliance "relates to Federal financial management system requirements" and then concludes, "NSF has several weaknesses in its entity-wide security that contribute to noncompliance with OMB Circular A-130". The report references the weaknesses that provide the basis for the auditors' reportable condition finding but fails to link those particular vulnerabilities to the finding of noncompliance. As discussed in Management's Response to 01-02 Information Security, the auditors have identified eight information security vulnerabilities, but they have not identified a failed or missing management control.

OMB's *Revised Implementation Guidance for FFMIA*, issued January 4, 2001, specifically addresses A-130 compliance, and lists the presence of the following four elements as indicators of compliance with A-130 and therefore FFMIA: (1) Assign Responsibility for Security; (2) System Security Plan; (3) Review of Security Controls; and (4) Authorize Processing. The Guidance makes clear that the presence of these four elements renders an agency A-130 compliant. This standard carefully tracks the A-130 Appendix III definition for a "deficiency". Section B. 3) provides in part, "[W]eaknesses identified during the review of **security controls** (emphasis added) should be reported as deficiencies in accordance with OMB Circular No. A-123 …. In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a deficiency." None of these management controls is missing at NSF, and OIG's audit report does not suggest otherwise.

A finding that information security is a reportable condition does not lead to a determination of FFMIA noncompliance. Three of the four agencies, besides NSF, determined to be substantially compliant with the statute last year (Department of Energy, General Services Administration, and Small Business Administration) had information security as a reportable condition. Only if the reportable condition prevents the agency from (1) preparing financial statements, (2) providing reliable and timely financial information for managing current operations, (3) properly protecting its assets from loss, misappropriation, or destruction — all in a way that is consistent with Federal accounting standards and the Standard General Ledger — will an agency not be in substantial compliance with FFMIA.

NSF firmly believes that its financial management systems substantially comply with FFMIA; but strongly supports and continues to work toward additional improvements in these systems. Because we find the auditors' finding of noncompliance unconvincing, NSF management can determine that the Foundation is in substantial compliance with FFMIA and does so in the Director's Statement of Assurance for FY 2001. As always, NSF will continue to

work professionally and diligently with OIG in improving the agency's financial management systems, and we look forward to continuing our substantial compliance with FFMIA requirements.