



United States Government

Department of Energy

# Memorandum

SEP 24 2004

DATE:

REPLY TO: IG-34 (A04TG032)

Audit Report No.: OAS-L-04-21

SUBJECT: Evaluation of "The Federal Energy Regulatory Commission's Cyber Security Program - 2004"

TO: Chairman, Federal Energy Regulatory Commission

The purpose of this report is to inform you of the results of our annual evaluation of the Federal Energy Regulatory Commission's unclassified cyber security program. This evaluation was initiated in June 2004 and our field work was conducted through September 2004. The evaluation methodology is described in the attachment to this report.

## Introduction and Objective

The Commission's increasing reliance on information technology (IT) is consistent with satisfying the President's Management Agenda initiative of expanding electronic government. The Commission expects to invest \$23.5 million on IT related activities in Fiscal Year 2004 to meet mission requirements of regulating interstate transmission of natural gas, oil and electricity, and regulating gas and hydropower projects.

As required by the Federal Information Security Management Act (FISMA) and the Office of Management and Budget (OMB) implementing guidance, the Office of Inspector General (OIG) performed an independent evaluation to determine whether the Commission's unclassified cyber security program protected data and information systems.

## Conclusions and Observations

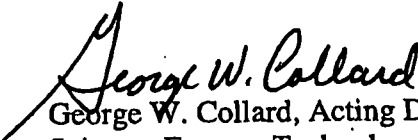
Our evaluation revealed that the Commission had made a number of improvements in its unclassified cyber security program. For instance, we found that the Commission had:

- Finalized a certification and accreditation methodology in March 2004 and recently completed the certification and accreditation process for all major applications and general support systems;
- Developed system-level contingency plans for all major systems; and,

- Utilized the National Institute of Standards and Technology (NIST) Security Self-Assessment Guide for IT Systems.

The above actions should continue to strengthen the Commission's cyber security program. However, we observed that the Commission had completely tested only one of five system-level contingency plans. Additionally, although the Commission used the NIST risk assessment methodology, it had yet to finalize a risk assessment methodology tailored to its needs--a key step in determining current security vulnerabilities within an organization and implementing mitigating controls. Successful completion of these ongoing initiatives should help correct remaining cyber security problems at the Commission.

Since no recommendations are being made in this letter report, a formal response is not required. We appreciate the cooperation of your staff throughout the audit.

  
George W. Collard, Acting Director  
Science, Energy, Technology,  
and Financial Audits  
Office of Audit Services  
Office of Inspector General

**Attachment**

cc: Executive Director, FERC  
Chief of Staff, DOE  
Chief Information Officer, DOE

## **SCOPE AND METHODOLOGY**

We performed our evaluation between June and September 2004. We evaluated controls over network operations to determine the effectiveness of access controls related to safeguarding information resources from unauthorized internal and external sources. The evaluation included a limited review of general and application controls in areas such as certification and accreditation, access controls, application software development and change controls, and contingency planning.

We satisfied our evaluation objective by reviewing applicable laws and regulations pertaining to cyber security and information technology resources, such as FISMA and OMB Circular A-130 (Appendix III), and reviewing the Commission's overall cyber security program management, policies, and procedures. We also reviewed applicable standards and guidance issued by the National Institute of Standards and Technology. The Commission's headquarters were evaluated in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG LLP, the Office of Inspector General contract auditor. Their review included limited analysis and testing of general and application controls for systems and a follow up review of the status of previously reported weaknesses.

We evaluated the Commission's implementation of the Government Performance Results Act of 1993 related to the establishment of performance measures for cyber security. We did not rely solely on computer-processed data to satisfy our objectives. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our review.

The review was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the objectives. We held an exit conference with management officials on September 23, 2004.

DOE F 1325.B  
(08-93)

United States Government

Department of Energy

# Memorandum

DATE: **SEP 30 2004**REPLY TO  
ATTN OF: IG-34 (A04TG032)SUBJECT: Final Report Package for Evaluation of "The Federal Energy Regulatory Commission's  
Cyber Security Program - 2004" Audit Report Number: OAS-L-04-21

TO: Rickey R. Hass, Assistant Inspector General for Audit Operations

Attached is the required final report package on the subject audit. The pertinent details are:

1. Actual Staff days: 67Actual Elapsed days: 95

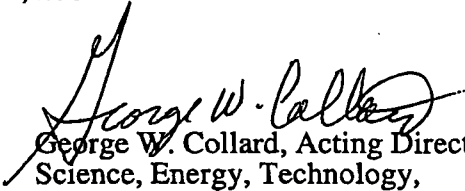
2. Names of OIG and/or contractor audit staff:

Assistant Director:	Kevin Majane
Team Leader:	Dan Weeber
Auditor-in-Charge:	Heather Lego
Audit Staff:	Mary Anthony and Chari Reines

To Steph  
Fm Sue  
4 pages

3. Coordination with Investigations and Inspections:

Investigations: Reginald France  
June 1, 2004Inspections: Fatima Pashaei  
June 1, 2004

  
George W. Collard, Acting Director  
Science, Energy, Technology,  
and Financial Audits  
Office of Audit Services  
Office of Inspector General

## Attachments:

1. Final Report
2. Monetary Impact Report
3. Audit Project Summary Report
4. Audit Database Information Sheet

**MONETARY IMPACT OF REPORT NO.: OAS-L-04-21**

1. Title of Audit: Evaluation of "The Federal Energy Regulatory Commission's Cyber Security Program -2004"

2. Division: Science, Energy, Technology, and Financial Audits Division

3. Project No.: A04TG032

4. Type of Audit:

Financial: \_\_\_\_\_ Performance: X  
 Financial Statement \_\_\_\_\_ Economy and Efficiency X  
 Financial Related \_\_\_\_\_ Program Results \_\_\_\_\_  
 Other (specify type): \_\_\_\_\_

5. Please report monetary savings identified in the report using applicable columns. Provide additional explanations of audited activities/locations in Section No. 6 - Remarks.

FINDING		COST AVOIDANCE		QUESTIONED COSTS				MGT. POSITION	POTENTIAL BUDGET IMPACT
(A)	(B) Title	(C) One Time	(D) Recurring Amount Per Year	(E) Questioned	(F) Unsupported	(G) Unresolved	(H) Total (E)+(F)+(G)	(I) C=Concur N=Noncon U=Undec	(J) Y=Yes N=No
	None								
TOTALS--ALL FINDINGS									

6. Remarks: Audit report contains no reportable potential monetary impact.

7. Contractor: \_\_\_\_\_  
 8. Contract No.: \_\_\_\_\_  
 9. Task Order No.: \_\_\_\_\_

10. Approvals:  
 Division Director/Date: [Signature] 9/30/04  
 Technical Advisor & Date: [Signature]

Office of the Inspector General (OIG)  
 Audit Project Office Summary (APS)

Report run on: September 29, 2004 11:08 AM

Audit#: A04TG032 Ofc: ATA Title: FERCS FEDERAL INFORMATION SECURITY MGT ACT

\*\*\*\* Milestones \*\*\*\*

	Planned	End of Survey	Revised	Actual
Entrance Conference:.....	01-OCT-03		21-JUN-04	21-JUN-04
Survey:.....				
Draft Report:.....				
Completed (With Report):.	30-SEP-04		17-SEP-04	24-SEP-04 ( R )
-----Elapsed Days:	365		88	95

Elap. Less Susp:

Date Suspended: Date Terminated:  
 Date Reactivated: Date Cancelled:  
 DaysSuspended(Cur/Tot): ( ) Report Number: OAS-L-04-21  
 Report Type: LTR LETTER REPORT

Rpt Title: EVALUATION OF "THE FEDERAL ENERGY REGULATORY COMMISSION'S CYBER SECURITY PROGRAM - 2004"

\*\*\*\* Audit Codes and Personnel \*\*\*\*

Class: PER PERFORMANCE  
 Program: Not Found  
 MgtChall: 005 NATIONAL SECURITY (F AD: 530 MAJANE  
 Site: SSA SINGLE-SITE AUDIT AIC: 725 LEGO  
 SecMiss: Not Found Team Ldr: 713 WEEBER  
 PresInit: EEG EXPANDED ELECTRONIC Tech Adv: 833 RUBB

\*\*\*\* Task Information \*\*\*\*

Task No:  
 Task Order Dt: CO Tech. Rep:  
 Orig Auth Hrs: Orig Auth Costs:  
 Current Auth: Current Auth Cost:  
 Tot Actl IPR Hr: Tot Actl Cost:

\*\*\*\* Time Charges \*\*\*\*

Emp/Cont Name	Numdays	Last Date
YI, J	3.1	18-SEP-04
WEEBER, D	11.0	18-SEP-04
REINES, C	17.3	18-SEP-04
LEGO, H	17.4	18-SEP-04
ANTHONY, M	18.0	04-SEP-04
Total:	66.8	

Attachment 4

**AUDIT DATABASE INFORMATION SHEET**

1. Project No.: A04TG032
2. Title of Audit: Evaluation of "The Federal Energy Regulatory Commission's Cyber Security Program - 2004"
3. Report No./Date: OAS-L-04-21/September 24, 2004
4. Management Challenge Area: National Security
5. Presidential Mgmt Initiative: Expanded Electronic Government
6. Secretary Priority/Initiative: Information Technology Management
7. Program Code: Federal Energy Regulatory Commission
8. Location/Sites: Single-Site Audit/Federal Energy Regulatory Commission
9. Finding Summary: As required by the Federal Information Security Management Act (FISMA), we performed an independent evaluation to determine whether the Federal Energy Regulatory Commission's (Commission) unclassified cyber security program protected data and information systems. Our evaluation revealed that the Commission made a number of improvements in its cyber security program in areas such as certification and accreditation and contingency planning. However, we did note that the Commission had completely tested only one of five system-level contingency plans. Additionally, the Commission has not finalized its own risk assessment methodology.
10. Keywords: Federal Energy Regulatory Commission  
Federal Information Security Management Act  
Cyber Security  
Information Technology  
FERC  
FISMA

Draft Rpt

DOE F 1325.8  
(8-89)  
EFG (07-90)

United States Government

Department of Energy

# Memorandum

DATE: September 13, 2004  
REPLY TO: IG-34 (A04TG032) Audit Report No.: OAS-L-04-21  
SUBJECT: Evaluation of "The Federal Energy Regulatory Commission's Cyber Security Program - 2004"  
TO: Chairman, Federal Energy Regulatory Commission

The purpose of this report is to inform you of the results of our annual evaluation of the Federal Energy Regulatory Commission's (Commission) unclassified cyber security program. This evaluation was initiated in June 2004, and our field work was conducted through September 2004. The audit methodology is described in the attachment to the report.

## Introduction and Objective

The Commission's increasing reliance on information technology is consistent with satisfying the President's Management Agenda initiative of expanding electronic government. The Commission expects to invest \$23.5 million on information technology related activities in Fiscal Year 2004 to meet mission requirements of regulating interstate transmission of natural gas, oil and electricity, and regulating gas and hydropower projects.

As required by the Federal Information Security Management Act (FISMA) and the Office of Management and Budget (OMB) implementing guidance, the Office of Inspector General performed an independent evaluation to determine whether the Commission's unclassified cyber security program protected data and information systems.

## Conclusions and Observations

Our evaluation revealed that the Commission had made a number of improvements in its unclassified cyber security program. For instance, we found that the Commission had:

- Finalized a certification and accreditation methodology in March 2004 and began an effort to certify and accredit all major applications and general support systems;
- Utilized the National Institute of Standards and Technology Guide for self assessment of programs and systems; and,



- Established a formal capital planning and investment control process.

Despite these improvements, we noted that the Commission had not completed contingency planning, risk management, and certification and accreditation of systems. For example, the Commission had developed system-level contingency plans for only three of five major systems and had completely tested only one of the plans. Although the Commission used the National Institute of Standards and Technology risk assessment methodology as required by FISMA, it had yet to finalize a risk assessment methodology tailored to its needs--a key step in determining current security vulnerabilities within an organization and implementing mitigating controls. Additionally, at the time of our review the Commission had only completed the certification and accreditation process for three of its five major applications and general support systems. Successful completion of these ongoing initiatives should help correct remaining cyber security problems at the Commission.

Since no recommendations are being made in this letter report, a formal response is not required. We appreciate the cooperation of your staff throughout the audit.

/S/

George W. Collard, Acting Director  
Science, Energy, Technology,  
and Financial Audits  
Office of Audit Services  
Office of Inspector General

Attachment

cc: Executive Director, FERC  
Chief of Staff, Department of Energy  
Chief Information Officer, Department of Energy

## SCOPE AND METHODOLOGY

We performed our evaluation between June and September 2004. We evaluated controls over network operations to determine the effectiveness of access controls related to safeguarding information resources from unauthorized internal and external sources. The evaluation included a limited review of general and application controls in areas such as certification and accreditation, access controls, application software development and change controls, and contingency planning.

We satisfied our evaluation objective by reviewing applicable laws and regulations pertaining to cyber security and information technology resources, such as FISMA and OMB Circular A-130 (Appendix III), and reviewing the Commission's overall cyber security program management, policies, and procedures. We also reviewed applicable standards and guidance issued by the National Institute of Standards and Technology. The Commission's headquarters were evaluated in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG LLP, the OIG contract auditor. Their review included limited analysis and testing of general and application controls for systems and a follow up review of the status of previously reported weaknesses.

We evaluated the Commission's implementation of the Government Performance Results Act of 1993 related to the establishment of performance measures for cyber security. We did not rely solely on computer-processed data to satisfy our objectives. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our review.

The review was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the objectives. We held an exit conference with the management on September XX, 2004.