

# Memorandum



DATE: **SEP 22 2003**

REPLY TO: IG-34 (A03TG049)

Audit Report No.: OAS-L-03-21

SUBJECT: Evaluation of "The Federal Energy Regulatory Commission's Cyber Security Program-2003"

TO: Chairman, Federal Energy Regulatory Commission

The purpose of this report is to inform you of the results of our evaluation of the Federal Energy Regulatory Commission's (Commission) cyber security program. The evaluation was initiated in July 2003, and our fieldwork was conducted through September 2003. Our methodology is described in the attachment to this report.

## INTRODUCTION AND OBJECTIVE

As with other Federal organizations, the Commission is increasing its focus on the electronic delivery of information and services and plans to spend \$27 million in Fiscal Year (FY) 2003 on information technology to support its energy markets mission. As required by the President's Management Agenda, the Commission recently began a series of initiatives to develop and implement web-based applications to improve the energy regulatory process and streamline internal activities. These networked systems increase the risk that sensitive and critical data could be compromised or lost as various applications are accessed through the Internet. Increasingly, "hackers" attempt to exploit vulnerabilities and corrupt valuable government information technology resources.

In response to the continuing threat to Federal information resources, Congress enacted the Federal Information Security Management Act (FISMA) in 2002 to ensure that all organizations develop and maintain adequate cyber security controls to protect information resources. As required by FISMA, 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

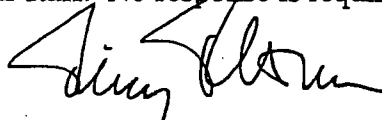
The Commission had made significant progress in resolving weaknesses reported during our 2002 evaluation. However, we observed that plans for maintaining or resuming critical operations in the event of an emergency or disaster had not been completed.

We found that the Commission had developed a comprehensive process for tracking and reporting the status of all previously identified cyber security weaknesses. We also

noted that the Commission had taken the following action to correct several weaknesses identified in 2002:

- The roles and authorities of the Chief Information Officer were clarified to include the development and implementation of a Commission-wide cyber security protection program;
- The Commission required all of its employees to receive cyber security awareness training. Furthermore, a core curriculum was developed for the individuals with significant security responsibilities;
- Several configuration management weaknesses were addressed, including maintaining current software updates, correcting the configuration of remote access and file transfer services, and correcting system server configurations to restrict unauthorized access; and,
- The Management, Administrative and Payroll System application was upgraded to enforce strengthened password policies.

Since our evaluation did not reveal new weaknesses and the Commission continues to make progress on correcting remaining problems, we made no new recommendations. We appreciate the cooperation of your staff. No response is required to this report.



Rickey R. Hass, 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

## Attachment

**SCOPE AND METHODOLOGY**

We performed our evaluation between July and September 2003. Our evaluation was primarily focused on the results of the Commission's corrective actions during FY 2003 to address previously identified weaknesses. In addition, we reviewed the Commission's progress in implementing its plan of action and milestones (POA&M) process.

We satisfied our objective by reviewing applicable laws and regulations pertaining to cyber security and information technology resources and reviewing the Commission's overall cyber security program management policies, procedures, and practices. In addition, we reviewed the Commission's corrective actions and their results to address previously reported weaknesses from prior cyber security evaluations. The review was performed 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 analysis and testing of general and application controls for systems and a review of system configurations in order to follow up on 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 16, 2003.

U. S. Department of Energy Office of Inspector General

All: Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as a part of the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.	
Bureau Name	FY03 IT Security Spending (\$ In thousands)
(No IG response required for this question)	
Agency Total	

U. S. Department of Energy Office of Inspector General

Independent Evaluation of FERC Unclassified Information Security - 2003

A.2a) Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and OIGs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, GAO shall also identify the total number of programs, systems and contractor operations or facilities that they evaluated in FY03.

Bureau Name	FY03 Programs		FY03 Systems		FY03 Contractor Operations or Facilities	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Federal Energy Regulatory Commission (FERC)						
<b>Agency Total</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections, agreed upon IT security requirements for contractor provided services or services provided by other agencies) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes					
c. If yes, what methods are used? If no, please explain why.	National Institute of Standards and Technology (NIST) 800-26 Security Self Assessment Guide for Information Technology (IT) Systems. Office of Inspector General (OIG) follow-up review.					
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes					
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	N/A					
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.	FERC completed its system inventory and has a total of 64 IT systems.					

U. S. Department of Energy Office of Inspector General  
 Independent Evaluation of FERC Unclassified Information Security - 2003

A-3: Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02; describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.				
Bureau Name	FY03 Material Weaknesses			
	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
FERC	0	0		
<b>Agency Total</b>	<b>0</b>	<b>0</b>		

U. S. Department of Energy Office of Inspector General  
 Independent Evaluation of FERC Unclassified Information Security - 2003

A4. This question is for ICS only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	Yes	No
Agency program officials develop, implement, and manage the plan of action and milestones (POA&M) for every system that they own and operate (systems that support their programs) that has an IT security weakness.	X	
Agency program officials report to the Chief Information Officer (CIO) on a regular basis (at least quarterly) on their remediation progress.	X	
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	X	
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	X	
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	X	
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in Office of Management and Budget (OMB) budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.		X
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.	X	
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.	X	

U. S. Department of Energy Office of Inspector General  
 Independent Evaluation of FERC Unclassified Information Security - 2003

<p><b>E1. Identify and describe any specific steps taken by the agency head, the agency, and program officials on the FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?</b></p>	<p>The Commission's Cyber Security Action Plan sets forth roles and responsibilities for the cyber security program and the Federal Information Security Management Act of 2002 (FISMA). Program elements are responsible for implementing cyber security policy. The CIO has responsibility for program monitoring, oversight, and enforcement.</p>
<p><b>E2. Can a head of operating component of the agency make an investment decision without the buy-by and concurrence of the agency CIO?</b></p>	<p>No.</p>
<p><b>E3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?</b></p>	<p>The Cyber Security Action Plan includes cyber security provisions applicable to all of the Commission's information systems, including systems in the development and maintenance phase. However, the Commission has not established any performance measures or metrics that would ensure the security plan is practiced throughout the lifecycle of the system.</p>
<p><b>E4. With the report in paragraph 2, did the agency head take any specific and direct actions to ensure the participation of (1) agency program officials and (2) the CIO, in the report which officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please describe.</b></p>	<p>During the reporting period, the Commission approved a site-wide Cyber Security Action Plan. However, individual systems do not have cyber security plans.</p>
<p><b>E5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.</b></p>	<p>No, the agency did not fully integrate its IT security program with its critical infrastructure protection responsibilities. Work is ongoing in this area. The Commission does not currently have an approved continuity of operations plan or tested disaster recovery plans.</p>
<p><b>E6. Does the agency have separate staff devoted to other security programs, and if so, what specific actions have been taken by the agency head or other officials to eliminate unnecessary duplication of activities, costs and ensure that policies and procedures are consistent and complementary across the various programs and disciplines?</b></p>	<p>No, the agency does not have separate staff devoted to other security programs. There is minimal duplication of costs or effort within the Commission's various security programs. It is a small agency and some individuals do have multiple responsibilities.</p>



U. S. Department of Energy Office of Inspector General  
 Independent Evaluation of FERC Unclassified Information Security - 2003

B7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its national critical operations and assets?	NA			
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	NA			
c. Has the agency fully identified its mission critical operations and assets?	Yes			
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?			No	
e. If yes, describe the steps the agency has taken as a result of the review.				
f. If no, please explain why.	While the Commission had identified all of its IT systems, it had not fully identified interdependencies and interrelationships of mission critical operations and assets because work on the Continuity of Operations Plan is not complete.			

NA = Not applicable because FERC has no national critical operations or assets.

**U. S. Department of Energy Office of Inspector General  
Independent Evaluation of FERC Unclassified Information Security - 2003**

<b>ER1: How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?</b>	
<b>a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).</b>	The Director for Security, Systems Assurance & Information Management (SSA&IM) coordinates computer security efforts within the agency and coordinates with law enforcement authorities and FedCIRC.
<b>b. Total number of agency components or bureaus.</b>	1
<b>c. Number of agency components with incident handling and response capability.</b>	1
<b>d. Number of agency components that report to FedCIRC.</b>	1
<b>e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?</b>	Yes
<b>f. What is the required average time to report to the agency and FedCIRC following an incident?</b>	Close of Business
<b>g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?</b>	While FERC's Cyber Security Action Plan briefly discusses patches and FERC has a flowchart for the patch process, FERC's IT documentation does not provide detailed procedures on monitoring or confirming the timely installation of security patches.
<b>h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?</b>	Yes
<b>i. If yes, how many active users does the agency have for this service?</b>	3
<b>j. Has the agency developed and complied with specific configuration requirements that meet their own needs?</b>	Yes
<b>k. Do these configuration requirements address patching of security vulnerabilities?</b>	Yes

**U. S. Department of Energy Office of Inspector General  
Independent Evaluation of FERC Unclassified Information Security - 2003**

By identity by bureau the number of incidents (e.g., successful and unsuccessful network penetrations, root of user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedSIRG or law enforcement.			
Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement
FERC	762,976	7	0

U. S. Department of Energy Office of Inspector General

Independent Evaluation of FERC Unclassified Information Security - 2003

6.1. Have agency program officials and the agency (IOE: 1) assessed the risk to operations and assets under their control, 2) determined the level of security appropriate to protect such operations and assets, 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control, and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated in total agency total identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

a. Bureau Name	b. Total Number of Systems	c. Number of systems assessed for risk and assigned a level or risk		d. Number of systems that have an up-to-date IT security plan		e. Number of systems certified and accredited		f. Number of systems with security control costs integrated into the life cycle of the system		g. Number of systems for which security controls have been tested and evaluated in the last year		h. Number of systems with a contingency plan		i. Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
FERC	64	59	92	0	0	0	0	0	0	1	1	0	0	0	0
<b>Agency Total</b>	<b>64</b>	<b>59</b>	<b>92</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

**U. S. Department of Energy Office of Inspector General  
Independent Evaluation of FERC Unclassified Information Security - 2003**

c. 24 Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.				
Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
Y	Y	The Executive Director centrally manages cyber security.	Y	Y

U. S. Department of Energy Office of Inspector General  
**Independent Evaluation of FERC Unclassified Information Security - 2003**

Q-3: Has the agency G O ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?							
Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
1,316	1032	78	8	7	87	Office of Personnel Management Online Learning Karta library for IT security and IT technical employees. Also, the Commission has in-house FISMA and NIST assessment training.	\$14,000

**U. S. Department of Energy Office of Inspector General  
Independent Evaluation of FERC Unclassified Information Security - 2003**

<small>Q4: Has the agency CIO fully integrated security into the agency's capital planning and investment management process? Were all security requirements and costs reported on the FY05 business case (as well as in the exhibit 53 submitted with the agency to OMB)?</small>				
Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
FERC	3 Submitted to OMB on September 9, 2003.	Yes. However, one of the business cases did not show evidence of budgeting for cyber security.	Yes. However, one of the business cases did not show evidence of budgeting for cyber security.	Yes. However, in one instance FERC is reporting an IT investment in a system owned by another agency. FERC does not show any IT security costs for this investment.