UNITED STATES OF AMERICA

FEDERAL LABOR RELATIONS AUTHORITY

OFFICE OF THE INSPECTOR GENERAL

WASHINGTON, D.C. 20424-0001

FLRA Inspector General FY 2003 Evaluation of FLRA's Compliance With The Federal Information Security Management Act of 2002

Background: The Federal Information Security Management Act of 2002 requires Inspectors General to perform annual independent evaluations of Agency security programs and practices. The FLRA Inspector General performed a comprehensive Computer Information Security Audit in FY 2001 which revealed that the FLRA had substantial security vulnerabilities in its Computer Information Program and that management needed to immediately focus on its technology and computer information security programs to ensure protection of FLRA information as well as to be able to implement e-government in the future.

As a follow-up to the Inspector General audit recommendations, FLRA management engaged the services of a private sector consultants to perform a detailed review of the FLRA's information technology support structure which included specific assessments of the Information Resource Management Division (IRMD)organization, staffing resource levels, funding levels, strategies, information technology, and performance management. As a result of this consultation, FLRA management was provided detailed technically oriented recommendations to support the FLRA's Information Technology Program.

During this past year, FLRA management has focused on its computer information technology deficiencies identified by the FY 2001 Inspector General audit. This information is provided as an attachment. In FY2002, the Chairman, FLRA created and filled a Chief Information Officer position. The FLRA Chief Information Officer has drafted planning, policy and procedures which need to be approved by the Chairman, implemented and supported by management.

FISMA Reporting

FISMA requires that each agency's report include information regarding the following former GISRA requirements:

1) Agency risk assessments
2) Security policies and procedures.
3) Individual system security plans
4) Training
5) Annual testing and evaluation
6) Corrective Action Process
7) Security Incident Reporting
8) Continuity of Operations

FISMA also requires each Agency to develop specific system configuration requirements that meet their needs and ensure compliance with them with continuous monitoring and maintenance. This monitoring must include the testing of management, operational and technical controls. It must also assess risks, and identify systems which are not certified or accredited (NIST requirements.) FISMA also codifies an ongoing policy requirement that each system security

program have provisions for continuity of operations. FISMA requires that each agency have a senior Information Security Officer appointed by the agency CIO who reports to the CIO and carries out the security information responsibilities. The FLRA has not yet complied with these requirements. Although the Director, Information Resource Management (IRM) and the CIO have formulated a corrective action plan for previous FLRA Inspector General information security findings, they have not yet created an agency wide Plan of Action and Milestone (POA&M) Process which relates to performance measures and provides a quantitative rather than just narrative response. The CIO has worked with two contractors to develop information security policy and procedures, which will strengthen the FLRA's computer information security when implemented. This past year was a productive security information year in respect to planning and migrating to Windows 2000. Also, according to the FLRA CIO, the FLRA has responded to all external government wide information security information mandates and is in compliance with NIST.

Inspector General Comments:

Over this past year, the FLRA has focused on trying to improve its security information program. This program currently has several significant deficiencies which include not yet having a clear cut operational information security plan, not yet performing adequate annual program and system reviews, not providing standardized training for agency employees (and contractors) and not yet maintaining an agency-wide system POA&M (related to function). The FLRA still needs to improve its filter and patch management to reduce penetration risks and implement appropriate software to support penetration testing. Line authority (Information Resource Management Director, Chief Information Officer, and Security Officer) should interact and communicate with each other more to improve computer information security operations. The working relationship between the CIO and technical Information Resource Management Division staff needs to be improved by more informative and technical interaction between the contractors working for the CIO and IRM technical staff. Also, management must focus on assessing the need for implementing software that has been purchased if it is still viable to the FLRA systems. If this software is inappropriate, then after the CIO risk assessment, the new purchase of required software and its implementation should become a priority.

Over this next year, the FLRA must focus and improve its computer technology and information security, create an agency wide POA&M which relates to a mission and/or support FLRA functions. Policies and training need to be conducted and senior management needs to assess the extent of FLRA's ability and need to comply with e-government requirements.

OMB has specifically identified FISMA reporting requirements for agencies and Inspectors General. I am attaching the Inspector General review for inclusion in the Agency submission. I have also provided a copy of Inspector General defined vulnerabilities from the 2001 Security Audit and their current status.

Audit of Computer Information			**1 a. Fund, develop, implement an information security**
Security February 2001	**program that complies with OMB Circulars A-123, and A-130.**	**Revised date to be determined**	**9/30/2002 Open A-127,**
	1 b. Establish senior management oversight committee to Demonstrate senior management's commitment to and Support of an effective, efficient security program.	1/2002	9/30/20/02 Closed
	1.c. Ensure procedures are established to monitor/report FLRA's progress in resolving weaknesses and developing an efficient/effective information system security system.		9/30/02 Closed
	2 a. Establish a security awareness program that all employees must attend annually.	**Revised date to be determined**	**2/30/02 Open**
	2b. Delegate authority to IRMD that clearly assigns responsibilities and requirements; coordinate information Security control with systems outside IRMD and assist/control with other Program offices during development and implementation if new systems and enhancements to existing systems.	**Revised date to be determined**	**9/30/2002 Open**
	2.c. Revise current instructions for HRD and BFD to include security administration responsibilities for respective systems & require coordination with IRMD.	**Revised date to be determined**.	**9/30/2002 Open**
	perform periodic risk and vulnerability assessments	**Revised date to**	**2d. Ensure that system owners and program offices 9/30/2002 Open**

and certify systems.		**be determined.**
2e. Develop & establish agency-wide information security policy through the consolidation of existing instructions.	**9/30/2002**	**Open Revised date to be determined.**
2f. Centralize management responsibilities for development of security policy procedures and practices, but retain daily security administration with program offices.	9/30/2002	Closed
2g. Develop procedures to maintain a current inventory of authorized users for each system and for remote access.	**9/30//2002**	**Open Revised date to be determined**
2h. Define rules of behavior for each system based in management's defined level of acceptable risk.	**9/30/2002**	**Open Revised date to be determined**
2i. Develop procedures to ensure that security Officials, systems, and data owners establish and formalize procedures for granting appropriate access and system privileges.	**9/30/2002**	**Open Revised date to be determined**
2j. Conduct an agency-wide assessment Of information contained within the various systems to identify/classify the sensitivity of information an the security level needed.	9/30/2002	Closed

2k. Formalize incident response procedures and processes to identify/report on apparent/actual security breaches. Include instructions on proper procedures for reacting to security breaches in security awareness program.	**9/30/2002 Open Revised date to be determined**
2l. Develop procedures for periodically evaluating User privileges and in granting initial access and privileges to systems software and data.	**12/30/2002 Open Revised date to be determined**
2m. Obtain new remote access software sufficient to preclude unlimited remote dial in access to FLRA network.	**3/31/02 Open Revised to 09/30/2002**
2n. Obtain new software to monitor eternal access to the network and alert IRMD security Personnel of suspicious activities.	3/31/2002 Closed
2o. Dedicate funding to identify, review, and evaluate critical business functions for developing a business contingency and recovery plan.	**4/30/03 Open Revised date to be determined**
3a. Document procedures for programmers' access to the production environment and management's compensating controls to detect unauthorized activities.	**12/30/01 Open Revised to 12/31/2002 Revised target date to be determined**
3b. Document the network configuration: hardware4, software, and security controls; client server and Oracle databases; and systems security controls.	**4/30/03 Open Revised to 6/30/2003**
3c. Develop a System Develop Life Cycle requirements for developing new systems and enhancing existing systems	**4/30/2003 Open Methodology compliant with OMB and NIST Revised date to Be determined**
4a. Review costs and benefits of relocating the computer used for Entering and authorizing	Closed

	vendor payments to the Department of Treasury to a more secure location away from the General work area into an area of limited access.		
Audit of Computer Information			**1 a. Fund, develop, implement an information security program that complies with OMB Circulars A-123, A-127, and A-130.**
Security			**9/30/2002**
February 2001			**Open Revised date to be determined**
	1 b. Establish senior management oversight committee to Demonstrate senior management's commitment to and Support of an effective, efficient security program.	1/2002	9/30/20/02 Closed
	1.c. Ensure procedures are established to monitor/report FLRA's progress in resolving weaknesses and developing an efficient/effective information system security system.		9/30/02 Closed
	2 a. Establish a security awareness program that all employees must attend annually.		**2/30/02 Open Revised date to be determined**
	2b. Delegate authority to IRMD that clearly assigns responsibilities and requirements; coordinate information Security control with systems outside IRMD and assist/control with other Program offices during development and implementation if new systems and enhancements to existing systems.	**Revised date to be determined**	**9/30/2002 Open**
	2.c. Revise current instructions for HRD and BFD to include security administration responsibilities for respective systems & require coordination with IRMD.	**Revised date to be determined.**	**9/30/2002 Open**
	2d. Ensure that system owners and program offices perform periodic risk and vulnerability assessments and certify systems.	**Revised date to be determined.**	**9/30/2002 Open**
	2e. Develop & establish agency-wide information		**9/30/2002**

security policy through the consolidation of existing instructions.			**Open Revised date to be determined.**
2f. Centralize management responsibilities for development of security policy procedures and practices, but retain daily security administration with program offices.		9/30/2002	Closed
2g. Develop procedures to maintain a current inventory of authorized users for each system and for remote access.		**9/30//2002**	**Open Revised date to be determined**
2h. Define rules of behavior for each system based in management's defined level of acceptable risk.		**9/30/2002**	**Open Revised date to be determined**
2i. Develop procedures to ensure that security Officials, systems, and data owners establish and formalize procedures for granting appropriate access and system privileges.		**9/30/2002**	**Open Revised date to be determined**
2j. Conduct an agency-wide assessment Of information contained within the various systems to identify/classify the sensitivity of information an the security level needed.		9/30/2002	Closed
2k. Formalize incident response procedures and processes to identify/report on apparent/actual security breaches. Include instructions on proper procedures for reacting to security breaches in security awareness program.		**9/30/2002**	**Open Revised date to be determined**
2l. Develop procedures for periodically evaluating User privileges and in granting initial access and privileges to systems software and data.		**12/30/2002**	**Open Revised date to be determined**
2m. Obtain new remote access software sufficient to preclude unlimited remote dial in access to FLRA network.	**Revised to 09/30/2002 to be determined**	**3/31/02**	**Open**
2n. Obtain new software to monitor eternal			

				access
				3/31/2002
				9/2001Closed
	to the network and alert IRMD security Personnel of suspicious activities.			
	2o. Dedicate funding to identify, review, and evaluate			**4/30/03**
	critical business functions for developing a business contingency and recovery plan.		**Open Revised date to be determined**	
	3a. Document procedures for programmers'			
				12/30/01
	access to the production environment and		**Open Revised to 12/31/2002**	
	management's compensating controls to detect unauthorized activities.		**Revised target date to be determined**	
	3b. Document the network configuration:			
				4/30/03
	hardware4, software, and security controls; client server and Oracle databases; and systems security controls.		**Open Revised to 6/30/2003**	
				3c. Develop a System Develop Life Cycle
				4/30/2003
	requirements for developing new systems and enhancing existing systems		**Open Methodology compliant with OMB and NIST Revised date to Be determined**	
	4a. Review costs and benefits of relocating			
				12/30/01
	the computer used for Entering and authorizing vendor payments to the Department of Treasury to a more secure location away from the General work area into an area of limited access.		Revised to 3/17/2003	Closed 9/31/03
Internal Review of the <u>Office of the General Counsel's</u>				
	3. To acknowledge and comply with			
				10/02
				3/02
				Closed

information security and assurance, case files should be marked with “For Official Use Only” or“Confidential” and be locked after hours and during major time absences of investigation agents to protect confidentiality/sensitivity of information.			
6. Refrain from using e-mail to transmit any type of investigation documentation. Until software is encrypted or other appropriate information Security software is installed unless parties are aware of potential disclosure and agree to use the e-mail even though there is the possibility of information disclosure/compromise.		**9/02**	**Open** **Awaiting decision of new General Counsel**

A.1.Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should 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)**
Agency Total	

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 CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, Igs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.

Bureau Name	**FY 03 Programs**		**FY03 Systems**		**FY 03 Contractor Operations or Facilities**	
Office of the Inspector General Federal Labor Relations Authority	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Programs	6		8		2	0
	OSHA Compliance Case Processing Human Capital Fair Act Compliance FISMA Compliance Financial Reports, Central Services Fund and Budget Formulations				These will be reviewed in detail during the FY 2004 audit.	
Agency Total	6		8		2	

b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections) 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?	The FLRA IG completed a comprehensive computer information security audit in FY 2001 and is currently in the process of contracting out a comprehensive Security Program audit which will be completed during FY 2004. This audit will address FLRA compliance with FISMA, OMB and NIST rquirerments as well as national security and FLRA's policy. The FLRA CIO position was established this past year and initially focused on creating information security strategic			

	planning and policy formulation. The CIO had two contracted technical assistants working with her to create Agency security information technology policies and plans which would comply with NIST guidelines, OMB policy and FEDCirc. No formal CIO assessments of contractor information has yet been performed, The FLRA CIO relies significantly on the contractors input which is based on NIST guidelines Yes			
c. If yes, what methods are used? If no, please explain why.				
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	NIST self assessments were performed in FY 01 and FY 02. As of August 1, 2003, no NIST assessment has yet been conducted this year. 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		N/A	

A.3. Identify all material weaknesses 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 FY 02, describe each material weakness, and indicate whether POA&Ms have been developed for all material weaknesses.

Bureau Name	FY 03 Material Weaknesses			POA&Ms developed? **Y/N**
	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	
	No material weaknesses have been identified.	48 computer information security vulnerabilities were identified by the FY 2001 IG Audit. As of August 1, 2003, 14 had been corrected and have been closed. (Corrective actions are attached)		A corrective action plan was created in FY 2001 related to the significant vulnerabilities identified by a previous IG Computer Information security audit. Management is addressing these vulnerabilities. An Agency wide POA&M has not yet been issued but is being worked upon by the CIO.
Agency Total	0	0		0

A.4. This question is for Igs 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 POA&Ms for every system that they own and operated (systems that support their programs) that has an IT security weakness.		An Agency wide POA&M relating to all systems owned and operated are in the process of being formulated. The technology staff is in the process of evolving all Agency systems into Windows 2000. The Agency must define its technology needs and systems (according to functions,) create an agency wide POA&M for each system and define related performance metrics so that it can be integrated into budget formulation.
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.		The CIO has been meeting with Agency program officials on an annual basis. Once the POA&Ms are developed and the remediation requirements are defined, these meetings should increase. FLRA program officials have not received standardized information technology training and have different levels of evaluation of information security issues..
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.		POA&Ms for each system are currently being formulated.
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.		Explanation same as above.
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		POA&Ms are in the process of being developed, therefore the IG does not have this management tool. However, continuing discussions by IG with the CIO and Information Resource Management Division staff on a continuous basis keep the IG aware of agency actions and security weaknesses snf corrections.
System-level POA&Ms are tied directly to the system budget request through the IT business cases as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.		POA&Ms are in the process of being developed. Identified critical needs are currently tied to internal budget formulation and need to be approved by the Chairman. Management has been aware of some computer systems' vulnerabilities but hasn't been able to address

A.4. This question is for Igs 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
		them all because of its small staff and funding restrictions.
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		POA&Ms are currently being developed. The FLRA IG has been kept informed of information security developments by the CIO.
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		The CIO is currently identifying and proposing corrective actions for critical security weaknesses. The FLRA has implemented a state of the art firewall, has identified needed security devices, is working with OMB and implementing security devices identified by CISCO. The Agency is also beginning to integrate its information security with physical security and has continuing interaction with the Agency's Security Officer.

B. Responsibilities of Agency Head

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to the following questions:

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	The Chairman, FLRA created a Chief Information Officer position during this past fiscal year. The CIO was directed to create information security policy and planning in compliance with Federal requirements as well as define FLRA technical requirements, and review and clean up the existing systems. The latter has been completed. The Chairman, FLRA has also assigned the CIO the responsibility to perform a risk assessment on the Agency's systems which is currently in progress. The Chairman has also directed the formulation of an action plan which will comply with FISMA requirements. Also the Chairman has placed a priority on security training for FLRA officials and managers as well as personnel.
B.2 Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	No, the Chairman must approve the decision.
B.3. 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?	The migration of all systems to Windows 2000 is currently being implemented. Once this and the risk assessment are completed and an Agency wide POA&M is established, the Agency Head will address the creation and implementation of a life cycle security plans for each system of the Agency.
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?	The Chairman has not yet taken specific and/or direct actions to oversee the performance of agency officials since the current security focus is to re-implement FLRA security programs that focus on contemporary needs and requirements. The FLRA CIO is meeting annually with program managers and will be responsible for reporting information security compliance of the Agency's program managers when the lifecycle POA&M for all systems is implemented.
B.5. 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)?	The FLRA is currently in the process of integrating its information and information technology security program with its other security programs. The FLRA Inspector General will be conducting an audit this fall on this very subject. The FLRA has not yet created a Continuity of Operations because it must first implement proper operations, but the Chairman is aware of its importance.
B.6. Does the agency have separate staffs devoted to other security program under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	The FLRA has separate security and computer security information staffs who are under the authority of different agency officials who report to the Chairman.

B.7. 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 critical operations and assets, including their interdependencies and interrelationships?	Yes The FLRA has identified its critical operations and security is one that interrelates to all operations, programs and resources	No	
b. If yes, describe the steps the agency has taken as a result of the review.	The Chairman has directed the Agency CIO to perform a risk assessment of the computer information systems. The FLRA Inspector General plans		

	to commence an audit of all FLRA security programs during FY 2004.		
If no, explain why			

B.8. 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?

a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).		Procedures currently exist for reporting physical security incidents. The CIO will draft policy and procedures for reporting computer information security incidents in the near future.
b. Total number of agency components or bureaus.		8
c. Number of agency components with incident handling and response capability.		8 Physical security
d. Number of agency components that report to FedCIRC.		1
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?		No serious information security incident has occurred.
f. What is the required average time to report to the agency and FedCIRC following an incident?		FLRA policy has not yet ben established. The IG would recommend immediate reporting as soon as possible, and definitely not beyond 8 hours of the incident
g. How does the agency, including the programs within the major components, confirm that patches have been tested and installed in a timely manner?		Policy needs to be developed for program installations and related testing to ensure security . Currently, the FLRA has no testing capability.
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?		Currently, one Information Resource Management technical team leader has applied for Agency membership
i. If yes, how many active users does the agency have for this service?		2 (CIO and IRM)
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?		The FLRA is currently assessing its configuration needs.
k. Do these configuration requirements address patching of security vulnerabilities?		Yes

B.9 Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.		
Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC or law enforcement
		No incidents reported externally to FEDCIRC or law enforcement.

C. Responsibility of Agency Program Officials and Agency Chief Information Officers

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to identify and describe the performance of agency program officials and the agency CIO in fulfilling their IT security responsibilities.

C.1. Have agency program officials and the agency CIO: 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 systems supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY 03 according to the measures and in the format provided below for the number and percentage of total systems.

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level of risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of Systems w/security controls costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems w/a contingency plan		Number of systems for which contingency plans have been tested	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
	275 (approx.)														
		0- no plan developed yet.		0		0		0		* 0		0		0	
Agency Total															

*** Will be performed by FY2004 Audit**

C.2. 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?
N Not yet implemented		IT security programs not yet implemented.	No	Programs not yet created.

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?						
Total number fo agency employees in FY 03	Agency employees that received IT training in FY 03		Total Number of agency employees w/significant IT security responsibilities	Agency employees w/significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	No.	%		No.	%		
			No specific training was provided by the CIO during FY 2003.				

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in exhibit 53) submitted by the agency to OMB?				
Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT 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
	This information was not available at the time of the evaluation.			