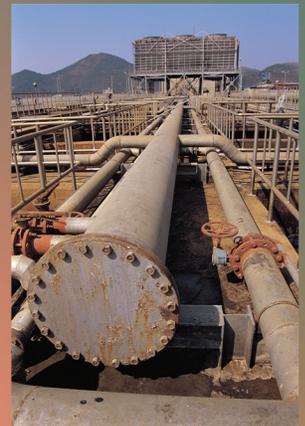


U.S. International Trade Commission

Inspector General Fiscal Year 2011 Annual Audit Plan



September 16, 2010



Office of Inspector General

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency that provides trade expertise to both the legislative and executive branches of government, determines the impact of imports on U.S. industries, and directs actions against certain unfair trade practices, such as patent, trademark, and copyright infringement. USITC analysts and economists investigate and publish reports on U.S. industries and the global trends that affect them. The agency also maintains and publishes the Harmonized Tariff Schedule of the United States.

Commissioners

Deanna Tanner Okun, Chairman

Charlotte R. Lane

Daniel R. Pearson

Shara L. Aranoff

Irving A. Williamson

Dean A. Pinkert

OFFICE OF INSPECTOR GENERAL



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

September 16, 2010

OIG-HH-025

Chairman Okun:

This memorandum transmits the Office of Inspector General Fiscal Year 2011 Annual Audit Plan. This document describes the fifteen reviews we plan to perform over the next twelve months to promote and preserve the efficiency, effectiveness, and integrity of the U.S. International Trade Commission.

Each review area has an individual audit plan that describes the background, criteria, objectives, benefits, and scope. The individual audit plans will be used to initiate communication with you, the Commissioners and responsible Office Directors. The plans may be revised as a result of these discussions to ensure that the work of this office is relevant and responsive to the priorities of the Commission.

I look forward to working with you in the upcoming fiscal year as we implement this plan.

A handwritten signature in blue ink, reading "Philip M. Heneghan".

Philip M. Heneghan
Inspector General

Table of Contents

1.0 Introduction.....	1
2.0 Mandatory Reviews	1
2.1 Audit of the Commission’s FY 2011 Financial Statement	1
2.2 Federal Information Security Management Act (FISMA) Review	2
3.0 Strategic Operation Review	2
3.1 Review of Title VII Investigations	2
4.0 Management Challenge Reviews.....	3
4.1 Internal Control Reviews	3
4.2 Information Technology Security Reviews	3
4.3 Financial Management.....	4
5.0 FY 2011 Individual Audit Plans	5
5.1 Financial Statement/Internal Control, Ref. 11-01	5
5.2 FISMA, Ref. 11-02	6
5.3 Title VII Preliminary Investigations, Ref. 11-03	7
5.4 Title VII Questionnaires, Ref. 11-04	8
5.5 Internal Control FMFIA, Ref. 11-05	9
5.6 FOIA, Ref. 11-06	10
5.7 Patching, Ref. 11-07	11
5.8 Penetration Testing, Ref. 11-08	12
5.9 Web Application Security, Ref. 11-09.....	13
5.10 Account Management, Ref. 11-10.....	14
5.11 Remote Access, Ref. 11-11	15
5.12 COOP, Ref. 11-12	16
5.13 Logging, Ref. 11-13	17
5.14 PP&E Follow-Up, Ref. 11-14	18
5.15 Purchase Card Process, Ref. 11-15	19

1.0 Introduction

The 2011 Annual Audit Plan outlines the anticipated reviews to be performed by the Office of Inspector General (OIG) for the fiscal year. The plan is developed prior to the start of the fiscal year and is based upon the most current version of the OIG Five Year Strategic Plan. The OIG Strategic Plan aligns the OIG activities to the strategic objectives, performance goals, and major challenges facing the Commission.

The plan is divided into three areas: mandatory reviews, program reviews, and management challenge reviews. Each area contains background information and review objectives. While the document outlines the planned activities, the OIG also recognizes that new initiatives, programs, issues, or other concerns may arise that require adjustments to the objective, priority, or schedule of the audits.

2.0 Mandatory Reviews

This section identifies audits required by law, statute, or other regulation authority that the OIG must perform.

2.1 Audit of the Commission's FY 2011 Financial Statement

Background:

The Accountability of Tax Dollars Act of 2002, requires the Commission to prepare and submit to the Congress and the Director of the Office of Management and Budget, an audited financial statement for each fiscal year, covering all accounts and associated activities of each office, bureau, and activity of the agency.

Audit Objective:

The objective of this audit will be to express an opinion on the agency's financial statements and internal controls. The audit reference planning number for this objective is Ref. 11-01.

2.2 Federal Information Security Management Act (FISMA) Review

Background:

FISMA outlines information security management requirements for agencies, including the requirement for an annual review and annual independent assessment by agency inspectors general.

Review Objective:

The objective of this review is to determine the effectiveness of the Commissions overall security program. The audit reference planning number for this objective is Ref. 11-02.

3.0 Strategic Operation Review

This section will identify the planned audits of the strategic operations of the Commission.

3.1 Review of Title VII Investigations

Background

The strategic goal for import injury investigations is to produce high-quality and timely import injury determinations based on an effective exchange of information, appropriate investigative record, and transparent, fair and equitably-implemented procedures. The OIG intends to perform two reviews in this area.

Review Objectives:

- To determine if the Commission consistently follows standard procedures for preliminary Title VII investigations. Audit reference planning number for this objective is Ref. 11-03.
 - To determine if the Commission consistently follows standard procedures for creating and reviewing producer questionnaires. The audit reference planning number for this objective is Ref. 11-04.
-

4.0 Management Challenge Reviews

The Reports Consolidation Act of 2000, requires the Inspector General to identify and report on the most serious management challenges facing the Commission. The Inspector General identified three management challenges in the current OIG Strategic Plan in the areas of internal control, information technology security, and financial management.

4.1 Internal Control Reviews

Background

Internal control, which includes ongoing oversight, is a fundamental responsibility of management. Previous audits have identified systemic patterns, where management relied on informal systems instead of documented processes. The OIG intends to perform three audits on internal controls to determine the extent that the Commission has reasonable assurance of the effectiveness and efficiency of operations.

Review Objectives:

- Determine if the Commission's has effective FMFIA internal controls, consistent with OMB Circular A-123, *Management's Responsibility for Internal Control*. The audit reference planning number for this objective is Ref. 11-05.
- Determine if the Commission follows a standard process to respond to Freedom of Information Act Requests. The audit reference planning number for this objective is Ref. 11-06.
- Determine if the Commission's purchase card holders implement standard procedures for ordering and reconciling credit card purchases. The audit reference planning number for this objective is Ref. 11-15.

4.2 Information Technology Security Reviews

Background:

The OIG plans to assess the adequacy and effectiveness of controls over information security, and compliance with information security policies, procedures, standards, and guidelines. The reviews will include the following areas:

Review Objectives:

- Determine the effectiveness of the CIO's patching process for all systems on ITCNet. The audit reference planning number for this objective is Ref. 11-07.

U.S. International Trade Commission
Office of the Inspector General

- Determine the effectiveness of the Commission's security perimeter through external penetration test of ITCNet. The audit reference planning number for this objective is Ref. 11-08.
- Determine the effectiveness of security controls designed to protect USITC's web-based applications. The audit reference planning number for this objective is Ref. 11-09.
- Determine the effectiveness of the account provisioning lifecycle. The audit reference planning number for this objective is Ref. 11-10.
- Determine if the Commission's remote access systems provide the level of capabilities, performance, capacity, and redundancy required to support telework and COOP activities. The audit reference planning number for this objective is Ref. 11-11.
- Determine if the Commission's Business Continuity of Operations (COOP) Plan follows the guidance as provided in Federal Preparedness Circular 65. The audit reference planning number for this objective is Ref. 11-12.
- Determine whether logs are being used effectively by CIO staff to gain an understanding of the events taking place on the network. The audit reference planning number for this objective is Ref. 11-13.

4.3 Financial Management

Background:

The Federal Managers Financial Integrity Act (FMFIA) requires agencies to establish internal control and financial systems that provide reasonable assurance that the integrity of federal programs and operations are protected.

Review Objectives:

- Determine if the Commission documents and follows policies and procedures to ensure Property, Plant, and Equipment is being capitalized, depreciated, monitored, and reported. The audit reference planning number for this objective is Ref. 11-14.
-

U.S. International Trade Commission
Office of the Inspector General

5.0 FY 2011 Individual Audit Plans

This section describes in further detail the proposed review areas.

5.1 Financial Statement/Internal Control, Ref. 11-01

Office/Program Area	Office of Finance
Target Start Date (Month/Year)	July 2011

BACKGROUND:

The Accountability of Tax Dollars Act of 2002, require all executive agencies with a budget authority in excess of \$25 million to prepare audited financial statements and subject those statements to an independent audit. These audited statements are required to be submitted to the Congress and the Office of Management and Budget (OMB). In order to comply with these requirements, the Commission needs a system to prepare a complete set of financial statements on a timely basis in accordance with U.S. generally accepted accounting principles. The statements are to result from an accounting system that is an integral part of an integrated financial management system containing sufficient structure, effective internal control and reliable data. Financial reporting also consists of the policies and procedures related to the processing and summarizing of accounting entries, and the preparation of financial statements.

5.1.2 CRITERIA:

- OMB Bulletin 07-04, Audit Requirements for Federal Financial Statements.

5.1.3 PROPOSED OBJECTIVE(S):

The objectives are:

- To render an opinion on whether the USITC's consolidated financial statements are presented fairly in all material respects
- To issue conclusions based on the testing of internal controls
- To determine the extent of the Commission's compliance with laws and regulations.

5.1.4 BENEFIT(s):

To provide reasonable assurance to the Commission that it is properly managing and reporting financial transactions, and can accurately produce end of year financial statements and ensure that the transactions and adjustments reported are properly supported.

U.S. International Trade Commission
Office of the Inspector General

5.1.5 SCOPE:

The OIG will contract this work to an independent auditor to conduct an audit of, and report on the USITC's consolidated financial statements for FY2011 in accordance with OMB Bulletin 07-04. The auditor will test the Commission's financial statements preparation.

5.2 FISMA, Ref. 11-02

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	August 2011

BACKGROUND:

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to establish agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, plans for remedial action, security incident response, and continuity of operation. FISMA also requires annual independent evaluation of federal agency information security programs and practices. Agency information security activities are guided by Office of Management and Budget policy and information security standards developed by the National Institute of Standards and Technology (NIST). This review will build on knowledge done on other audits in the information technology area.

5.2.2 CRITERIA:

- FISMA
- NIST Special Publications 800-100, 800-115, 800-128, 800-18, 800-53
- OMB Circular A-130, Management of Federal Information Resources
- OMB Policy Memoranda

5.2.3 PROPOSED OBJECTIVE(S):

Assess the adequacy of controls over information security and compliance with information security policies, procedures, standards, and guidelines. The review will include tests of the effectiveness of information security control techniques.

U.S. International Trade Commission
Office of the Inspector General

5.2.4 BENEFIT(s):

To provide assurance to the Commission that the controls implemented to protect its information security are effective, and that the description of the Commission's information systems being provided to the Office of Management and Budget by the Office of the CIO is comprehensive and accurate.

5.2.5 SCOPE:

The OIG will select elements from the policies, guidelines, and standards identified in the criteria and determine the extent of effectiveness of the security controls tested.

5.3 Title VII Preliminary Investigations, Ref. 11-03

Office/Program Area	Operations 1
Target Start Date (Month/Year)	November 2011

5.3.1 BACKGROUND:

Strategic Operation 1, Import Injury Investigations, provides support to the Commission by performing investigations into the effects of unfairly traded imports. In each investigation, the Commission and an investigative staff team develop a thorough record of the conditions of competition within the domestic market of the industry under investigation. The Commission relies on this data to make the preliminary determination under a "reasonable indication" standard within 45 days of the filing of the petition.

During the past two years, the Commission has seen a dramatic increase in the number of preliminary antidumping and countervailing duty investigations. Due to the increased workload it is important to provide assurances to the Commission that the investigative team has maintained the integrity of the investigative process in meeting the statutory deadlines.

5.3.2 CRITERIA:

- Title VII of the Tariff Act of 1930

5.3.3 PROPOSED OBJECTIVE(S):

The objective is to determine if the Commission consistently follows standard procedures when performing preliminary investigations.

U.S. International Trade Commission
Office of the Inspector General

5.3.4 BENEFIT(s):

To provide assurance to the Commission that investigative records are developed appropriately and in a consistent manner for each preliminary investigation determination.

5.3.5 SCOPE:

The OIG will review processes, procedures and a sample of files, to evaluate the Commission's activities from the time an antidumping or countervailing duty petition is received through the time a preliminary determination has been concluded.

5.4 Title VII Questionnaires, Ref. 11-04

Office/Program Area	Operations 1
Target Start Date (Month/Year)	March 2011

5.4.1 BACKGROUND:

Import injury investigations at the Commission include antidumping and countervailing duty investigations under Title VII of the Tariff Act of 1930. The Commissioners base their determinations in import injury investigations on the requirements of the appropriate law and the factual record built in each investigation.

The USITC staff uses a variety of fact-gathering techniques to develop a thorough record of the conditions of competition within the domestic market of the industry under investigation. One of the fact-gathering techniques is to develop and review industry-specific questionnaires. The OIG will be reviewing the questionnaire development process to provide assurance to the Commission that they are developed in a consistent manner following a standard procedure.

5.4.2 CRITERIA:

- Tariff Act of 1930
- USITC Policies, Procedures, Guidelines

5.4.3 PROPOSED OBJECTIVE(S):

The objective is to determine if the Commission consistently follows standard procedures for creating and reviewing questionnaire used in Title VII investigations.

U.S. International Trade Commission
Office of the Inspector General

5.4.4 BENEFIT(s):

To provide assurance to the Commission that the questionnaires used to support antidumping and countervailing duty investigations are created fairly and equitably.

5.4.5 SCOPE:

The OIG will review the process and procedures to develop questionnaires and evaluate these against the final products in the files.

5.5 Internal Control FMFIA, Ref. 11-05

Office/Program Area	Commission
Target Start Date (Month/Year)	July 2011

5.5.1 BACKGROUND:

The Federal Managers' Financial Integrity Act (FMFIA), requires that internal accounting and administrative control standards be developed by the General Accountability Office (GAO) and that annual evaluations be conducted by each executive agency of its system of internal accounting and administrative controls in accordance with guidelines established by the Director of OMB; and annual statements of internal controls be included in the annual Performance and Accountability Report (PAR).

5.5.2 CRITERIA:

- Federal Managers' Financial Integrity Act
- Office of Management and Budget Circular A-123, Management's Responsibility for Internal Control (OMB Circular A-123).

5.5.3 PROPOSED OBJECTIVE(S):

The OIG will perform a review to ensure the Commission has met the requirements of FMFIA. The objectives will be to:

- Determine if the Commissions compliance with FMFIA and OMB A-123.
- Provide an opinion of reasonable assurance on the Commissions statement of internal controls in the PAR.

U.S. International Trade Commission
Office of the Inspector General

5.5.4 BENEFIT(s):

To provide assurance to the Commission on the validity of the status of agency internal controls as reported in the annual Performance and Accountability Report.

5.5.5 SCOPE:

The OIG intends on obtaining independent auditors to perform this review. The auditors will perform a review to determine to the extent of compliance with laws and regulations in order to provide an opinion on the Commissions statement of assurance on internal control as reported in the PAR.

5.6 FOIA, Ref. 11-06

Office/Program Area	Office of the Secretary
Target Start Date (Month/Year)	October 2010

5.6.1 BACKGROUND:

The Freedom of Information Act requires federal agencies to make their records promptly available to any person who makes a proper request for them. The OPEN Government Act of 2007 amended several procedural aspects of the FOIA, statutorily mandating existing practices that assist requesters and facilitate the processing of FOIA requests.

5.6.2 CRITERIA:

- Freedom of Information Act
- OPEN Government Act

5.6.3 PROPOSED OBJECTIVE(S):

The objective is to determine if the Commission has the appropriate internal controls in place for receiving and responding to FOIA requests as required by the Act.

5.6.4 BENEFIT(s):

To provide reasonable assurance to the Commission on the validity of the statistical data provided in the annual FOIA report.

U.S. International Trade Commission
Office of the Inspector General

5.6.5 SCOPE:

The OIG will review the internal controls relevant on how the USITC receives, tracks, responds and reports FOIA requests.

5.7 Patching, Ref. 11-07

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	May 2011

5.7.1 BACKGROUND:

The protection of the Commission's Information Systems is dependent on maintaining a secure, patched state of applications and operating systems on all networked devices. Because patches are continuously released, an effective patch management program implements a system to continuously monitor patch levels and apply required patches to all networked devices. Systems that remain unpatched present a material risk to the Commission.

5.7.2 CRITERIA:

- NIST 800-40 and US-CERT

5.7.3 PROPOSED OBJECTIVE(S):

The objective of this audit is to assess the effectiveness of the CIO's patching process for all systems on ITCNet.

5.7.4 BENEFIT(s):

To provide assurance to the Commission that its risk due to known exploits is being mitigated through the comprehensive and timely application of software patches.

5.7.5 SCOPE:

This audit will encompass all possible nodes on ITCNet to determine the update/patch state of all software, including operating systems and both major and minor applications. The device list shall include but is not limited to all servers, workstations, routers, printers, email gateways, firewalls and any other network or security devices on ITCNet.

U.S. International Trade Commission
Office of the Inspector General

5.8 Penetration Testing, Ref. 11-08

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	July 2011

5.8.1 BACKGROUND:

The external perimeter of a network serves as the primary defense against attack. The perimeter typically consists of border routers, firewalls, web servers, email servers, anti-spam appliances, DNS servers, and other devices. No matter how well a given system may have been developed, the nature of today's complex systems with large volumes of code, complex internal interactions, interoperability with uncertain external components, unknown interdependencies means that exploitable flaws will always be present or surface over time. Accordingly, security testing must fill the gap between the state of the art in system development and actual operation of these systems. Security testing is important for understanding, calibrating, and documenting the operational security posture of an organization. Organizations that have an organized, systematic, comprehensive, on-going, and priority driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their systems.

5.8.2 CRITERIA:

- NIST SP 800-42, 800-53A (Appendix G), 800-115, 800-81

5.8.3 PROPOSED OBJECTIVE(S):

Determine the effectiveness of the Commission's security perimeter through external penetration testing of ITCNet.

5.8.4 BENEFIT(s):

To provide assurance to the Commission that it is implementing effective controls to protect its perimeter.

U.S. International Trade Commission
Office of the Inspector General

5.8.5 SCOPE:

This audit will include all externally available nodes on ITCNet. The device list shall include but is not limited to all servers, workstations, routers, email gateways and firewalls. The access types attempted will include login attempts for the purposes of information gathering, privilege escalation, and establishment of jumping points to other areas of ITCNet infrastructure.

5.9 Web Application Security, Ref. 11-09

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	August 2011

5.9.1 BACKGROUND:

The Commission provides data to the public through web-based applications. It is important to insure that this data retains its integrity, and cannot be modified by unauthorized means. No matter how well a given system may have been developed, the nature of today's complex systems with large volumes of code, complex internal interactions, interoperability with uncertain external components, unknown interdependencies means that exploitable flaws will always be present or surface over time. Accordingly, security testing must fill the gap between the state of the art in system development and actual operation of these systems. Security testing is important for understanding, calibrating, and documenting the operational security posture of an organization. Organizations that have an organized, systematic, comprehensive, on-going, and priority driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their systems.

5.9.2 CRITERIA:

- NIST Special Publications 800-28, 800-95, 800-42, 800-53A (Appendix G), 800-115, 800-81

5.9.3 PROPOSED OBJECTIVE(S):

The objective is to determine effectiveness of security controls designed to protect USITC's web-based applications.

U.S. International Trade Commission
Office of the Inspector General

5.9.4 BENEFIT(s):

To provide assurance to the Commission that it is implementing effective controls to protect its perimeter.

5.9.5 SCOPE:

This audit will focus on a selected externally available Web-based application, and shall focus on the related systems, subsystems, and the GSS supporting the security of this application.

5.10 Account Management, Ref. 11-10

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	October 2010

5.10.1 BACKGROUND:

Network accounts are used for access in a number of different ways, including provisioning of access to standard users, and for the purpose of the administration of various devices and applications on ITCNet. Each account should have a lifecycle, which begins when their role requires a user or administrator to have access to network assets, and ends when this user or administrator's role changes, and this access is no longer required. A well run network will demonstrate an effective process for account provisioning and maintenance, and will show a responsive track record of rapidly and efficiently provisioning and removing access to its assets.

5.10.2 CRITERIA:

- FISMA
- NIST Special Publication 800-53
- OMB Circular A-130, Management of Federal Information Resource

5.10.3 PROPOSED OBJECTIVE(S):

Assess account provisioning and current network accounts to identify effectiveness of the account provisioning lifecycle.

U.S. International Trade Commission
Office of the Inspector General

5.10.4 BENEFIT(s):

To provide assurance to the Commission that the processes to manage user accounts are effective, and that unauthorized access due to improperly enabled accounts is not taking place.

5.10.5 SCOPE:

The OIG will assess several classes of authentication systems in the Commission, including but not limited to the ITCNet Active Directory Domain, EDIS, and network infrastructure to determine the effectiveness of procedures to manage account provisioning.

5.11 Remote Access, Ref. 11-11

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	November 2010

5.11.1 BACKGROUND:

Increasing emphasis is being placed on expanding the use of telework in Federal agencies. An effective telework program will provide a means to efficiently accomplish their work in a location-independent scenario. It would also serve as a means to allow continuity of operations for a range of scenarios that result in limited access to USITC's facilities, such as the recent example of snow days in the Washington metro region. An effective telework system would include access to both data and voice systems that will allow staff to work efficiently even when not in the office.

5.11.2 CRITERIA:

- FISMA
- NIST Special Publication 800-46, 800-114
- OMB Circular A-130, Management of Federal Information Resources
- OMB Policy Memorandum
- Pending Telework Legislation, H.R. 1722.

U.S. International Trade Commission
Office of the Inspector General

5.11.3 PROPOSED OBJECTIVE(S):

Assess whether the Commission's remote access systems provide the level of capabilities, performance, capacity, and redundancy required to support telework and COOP activities.

5.11.4 BENEFIT(s):

To provide assurance to the Commission that its telework systems effectively enable its staff to extend their workplace beyond the parameters of the physical building, allowing them to work efficiently from alternate locations.

5.11.5 SCOPE:

The OIG will employ technical testing, design review, test data, and user interviews to assess the capabilities and performance of the technologies used at the Commission to provide remote access to its staff.

5.12 COOP, Ref. 11-12

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	February 2011

5.12.1 BACKGROUND:

Information systems are vital elements in most mission/business functions. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

5.12.2 CRITERIA:

- FISMA
- NIST Special Publications 800-114, 800-34, 800-46
- OMB Circular A-130, Management of Federal Information Resources
- Federal Preparedness Circular 65

U.S. International Trade Commission
Office of the Inspector General

5.12.3 PROPOSED OBJECTIVE(S):

Determine if the Commission’s Business Continuity of Operations (COOP) Plan follows the guidance as provided in Federal Preparedness Circular 65.

5.12.4 BENEFIT(s):

To provide assurance to the Commission that it has a tested, viable capability to provide mission-critical applications for its staff to continue their work in the event of a contingency.

5.12.5 SCOPE:

The OIG will conduct document and design review as well as interviews to determine the state of the Commission’s preparedness to continue all critical operations in the event of a contingency.

5.13 Logging, Ref. 11-13

Office / Program Area	Office of the Chief Information Officer
Target Start Date (Month/Year)	December 2010

5.13.1 BACKGROUND:

A log is a record of the events occurring within an organization’s systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Originally, logs were used primarily for troubleshooting problems, but logs now serve many functions within most organizations, such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating malicious activity. Logs have evolved to contain information related to many different types of events occurring within networks and systems. Within an organization, many logs contain records related to computer security; common examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks. This guide addresses only those logs that typically contain computer security-related information.

Because of the widespread deployment of networked servers, workstations, and other computing devices, and the ever-increasing number of threats against networks and systems, the number, volume, and variety of computer security logs has increased greatly. This has created the need for computer security log management, which is the process for generating, transmitting, storing, analyzing, and disposing of computer security log data.

U.S. International Trade Commission
Office of the Inspector General

5.13.1 CRITERIA:

- FISMA
- NIST Special Publications 800-100, 800-115, 800-128, 800-18, 800-92
- OMB Circular A-130, Management of Federal Information Resources
- OMB Policy Memorandum

5.13.2 PROPOSED OBJECTIVE(S):

Determine whether logs are being used effectively by CIO staff to gain an understanding of the events taking place on the network.

5.13.3 BENEFIT(s):

To provide assurance to the Commission that it knows what is happening on its network, and that appropriate tools are being used to allow CIO staff to efficiently gather and analyze events generating log entries.

5.13.4 SCOPE:

This audit will assess logging capabilities and usage for systems including Active Directory, web applications, and network infrastructure.

5.14 PP&E Follow-Up, Ref. 11-14

Office/Program Area	Office of Finance
Target Start Date (Month/Year)	March 2011

5.14.1 BACKGROUND:

Audit Reports OIG-AR-02-10 and OIG-AR-07-10 both identified repeated weaknesses related to the policy, procedure and quarterly reconciliation of assets as reported on the Property, Plant, and Equipment Account (PP&E).

This will be a follow-up review to determine if the Commission has implemented the appropriate corrective actions to resolve the weaknesses related to the quarterly reconciliation of the PP&E account statements.

U.S. International Trade Commission
Office of the Inspector General

5.14.2 CRITERIA:

- Statement of Federal Financial Accounting Standard No. 6, Accounting for Property, Plant and Equipment (SFFAS No.6) and FMFIA

5.14.3 PROPOSED OBJECTIVE(S):

To confirm that the Commission has the appropriate internal controls in place to substantiate the balance of the PP&E account on the 2010 financial statement.

5.14.4 BENEFIT(s):

To provide reasonable assurance to the Commission that corrective action, related to weaknesses identified in the reconciliation of the PP&E account, have been implemented and have effectively resolved the reported problem.

5.14.5 SCOPE:

The OIG will interview key personnel, review policies and procedures, obtain and test completeness of account balances, and examine documentation to support the PP&E balances.

5.15 Purchase Card Process, Ref. 11-15

Office/Program Area	Office of Procurement
Target Start Date (Month/Year)	April 2011

5.15.1 BACKGROUND:

The federal government purchase card program was established to streamline acquisition processes by providing a low-cost, efficient vehicle for obtaining goods and services directly from vendors. Each agency is responsible for developing their own internal procedures and establishing processing and internal controls to prevent improper and abusive purchase card transactions.

5.15.2 CRITERIA:

- USITC Procurement Policy
- USITC Purchase Card Handbook
- Federal Acquisition Regulation

U.S. International Trade Commission
Office of the Inspector General

5.15.3 PROPOSED OBJECTIVE(S):

The proposed objectives will be to assess the adequacy USITC's internal controls for the Purchase Card Program to:

- Determine if purchase card holders implement standard procedures for ordering and reconciling credit card purchases.
- Determine if controls are in place to reasonably prevent purchase card misuse.
- Determine if internal controls for card deactivation are adequate.

5.15.4 BENEFIT(s):

To provide assurance to the Commission that the purchase card program is operating in an effective manner and it is not vulnerable to significant fraudulent, improper, or abusive purchases.

5.15.5 SCOPE:

The OIG will review USITC policies and procedures, obtain a listing of USITC's credit card holders, perform interviews, and review purchase card files for completeness, and accuracy.

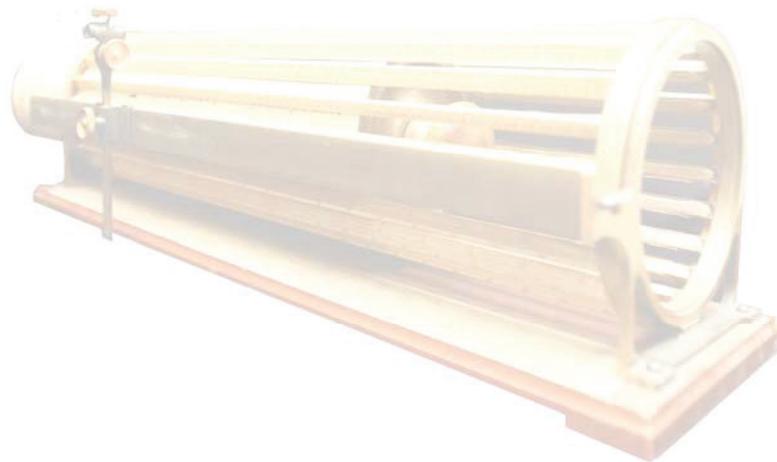
U.S. International Trade Commission
Office of the Inspector General

Table 1: OIG FY 2011 Annual Audit/Review Schedule

FY 2011 Estimated Audit/Review Schedule			
Ref.	Office or Operational Area	Proposed Objective	Target Start Date
11-01	Office of Finance	Provide an opinion on the agency's financial statements and internal controls.	07/2011
11-02	Office of the Chief Information Officer	Determine the effectiveness of the Commission's information system security program.	08/2011
11-03	Operations 1	Determine if the Commission consistently follows standard procedures for preliminary Title VII investigations.	11/2011
11-04	Operations 1	Determine if the Commission consistently follows standard procedures for creating and reviewing producer questionnaires.	03/2011
11-05	Chairman	Determine if the Commission's has effective FMFIA internal controls, consistent with OMB Circular A-123, <i>Management's Responsibility for Internal Control</i> .	07/2011
11-06	Office of Secretary	Determine if the Commission follows a standard process to respond to Freedom of Information Act Requests.	10/2010
11-07	Office of the Chief Information Officer	Determine if the Commission's ITCNet Patching Program is effectively reducing risks.	05/2011
11-08	Office of the Chief Information Officer	Determine the effectiveness of the Commission's security perimeter through external penetration test of ITCNet.	07/2011
11-09	Office of the Chief Information Officer	Determine if the Commission has established effective policy and implemented adequate controls for web application security.	08/2011
11-10	Office of the Chief Information Officer	Determine if the Commission has established effective policy and implemented adequate controls for user account management	10/2010
11-11	Office of the Chief Information Officer	Determine if the effectiveness and adequacy of security access controls for remote access to prevent unauthorized access to ITCNet.	11/2010
11-12	Office of the Chief Information Officer	Determine if the Commission's Business Continuity of Operations (COOP) Plan follows the guidance as provided in Federal Preparedness Circular 65.	02/2011

U.S. International Trade Commission
Office of the Inspector General

11-13	Office of the Chief Information Officer	Determine if the Commission's log collection and review is effectively adequate to detect security violations, performance problems, and flaws in applications.	12/2010
11-14	Office of Finance	Determine if the Commission documents and follows policies and procedures to ensure Property, Plant, and Equipment is being capitalized, depreciated, monitored, and reported.	03/2011
11-15	Office of Procurement	Determine the adequacy of the internal controls for the Commission's purchase card program.	04/2011



“Thacher’s Calculating Instrument” developed by Edwin Thacher in the late 1870’s. It is a cylindrical, rotating slide rule able to perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission



U.S. International Trade Commission
Office of Inspector General
500 E Street, SW
Washington, DC 20436

Office: 202-205-2210
Fax: 202-205-1859
Hotline: 877-358-8530
OIGHotline@USITC.gov