U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

International Trade Administration

FY 2007 FISMA Assessment of Core Network General Support System (ITA-012)

Final Inspection Report No. OSE-18840/September 2007

PUBLIC RELEASE

Office of Systems Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

SEP 24 2007

MEMORANDUM FOR: Michelle O'Neill
Acting Under Secretary for International Trade

Judith J. Gordon

FROM: Judith J. Gordon
Assistant Inspector General for Systems Evaluation

SUBJECT: International Trade Administration
FY 2007 FISMA Assessment of Core Network General Support System (ITA-012)
Final Inspection Report No. OSE-18840

Attached is our final report on the results of our Federal Information Security Management Act (FISMA) review of ITA's certification and accreditation of the Core Network General Support System. We concluded that ITA used an effective control assessment process that provided the authorizing official with a clear understanding of remaining vulnerabilities.

In its written response to our draft report, ITA agreed with our findings and outlined actions for addressing the recommendations. We request that these actions be recorded on a plan of action and milestones (POA&M) as required by FISMA and provided to me within 60 calendar days.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you would like to discuss any of the issues raised in this report, please call me at (202) 482-5643.

Attachment

cc: Renee Macklin, Chief Information Officer, International Trade Administration
Barry C. West, Chief Information Officer, U.S. Department of Commerce

Listing of Abbreviated Terms & Acronyms

C&A	Certification and accreditation
IT	Information technology
ISA	Internet Security Acceleration
OMB	Office of Management and Budget
FISMA	Federal Information Security Management Act of 2002
PIX	Private Internet Exchange
RADIUS	Remote Authentication Dial-in User Server
SSL	Secure Sockets Layer
VPN	Virtual Private Network

Synopsis of Findings Both Positive and Requiring Management Attention

- Effective assessment process provides a clear understanding of remaining vulnerabilities and status of system security controls.
- Components outside of the accreditation boundary that provide security controls for the system were not evaluated.
- System contingency plan and contingency testing are inadequate.

Conclusions

- Certification testing adequately assessed the required security controls.
- Certification activities provided sufficient basis for authorizing official to make a credible, risk-based decision to approve system operation.

Summary of ITA's Response and OIG Comments

ITA concurred with all of our recommendations and identified actions it has taken or plans to take to address them. The actions described are responsive to our recommendations. ITA's written response is included in its entirety as appendix B of this report.

Findings and Recommendations

1. Effective Assessment Process Provides A Clear Understanding of Remaining Vulnerabilities and Status of System Security Controls.

- The assessment of ITA security controls was based on well defined procedures and expected results.

- Clear assessment results were provided for each assessment procedure.
    - Clarity and credibility of results is greatly enhanced because results data was provided for controls that were assessed by examination or manual testing.
    - Identification of the individual interviewed and summary of their response demonstrated that assessments based on interview involved the correct system owner staff and asked relevant and appropriate questions.

- By clearly defining assessment procedures and expected results, and thoroughly documenting assessment results the certification agent could accurately determine which security controls are implemented correctly, recommend specific corrective actions, and clearly present to the authorizing official the risks associated with the remaining vulnerabilities.

- Well documented test results assist in effective vulnerability mitigation because the system owner has a clear record of specific system vulnerabilities.

ITA had no comments on this finding.

2. Components Outside of The Accreditation Boundary that Provide Security Controls For the System Were Not Evaluated.

- The system security plan and the security test and evaluation report describe the following security controls and components that are outside the accreditation boundary:
    - AC-2 (Account Management): RADIUS is the centralized mechanism for managing system administrator accounts for the edge router and PIX firewall.
    - AC-13 (Supervision and Review): The external switch is protected by other boundary devices at a higher level in the network general support system.
    - AC-20 (Personally Owned Information Systems): Authorized users access the ITA network remotely via a Juniper SSL VPN appliance and system administrators access the ITA network via a Microsoft ISA server.

- During a follow-up meeting, ITA explained that the components are part of the ITA Network Security general support system, which was currently undergoing C&A and had not been tested at the time the ITA Core Network was undergoing C&A.

- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* defines the application of security controls from one system to another as common controls. The results from the assessment of common controls can be used to support the security C&A processes of the system where that control has been applied. However, because the devices providing these security controls had not been assessed, there are no assessment results to support the use of that control in the ITA Core Network.

Recommendation

ITA should ensure that all components that implement security controls for a system are assessed prior to or during certification and accreditation.

ITA's Response

ITA concurred with this recommendation and stated that it will ensure that any components that are not a part of an information system's accreditation boundary are assessed prior to completing the certification and accreditation for that system. ITA also stated that controls AC-2 (Account Management) and AC-20 (Personally Owned Information Systems) have been implemented and tested for all of its information systems.

OIG Comment

ITA's corrective actions are responsive to our recommendation.

3. System Contingency Plan and Contingency Testing are Inadequate

- An annual test of the contingency plan was not conducted.
  - Certification test results indicate that the last test of the system contingency plan was conducted in June 2006 and note that the contingency test results can not be found.
  - The certification test results also indicate that the contingency plan was not used as the basis to assess system contingency readiness. Instead, the assessment was conducted using Federal Emergency Management Agency defined tests and exercise scenarios.

- The contingency plan does not address the procedures and activities required to restore operations after a disruption or failure as required by Department policy and NIST SP 800-53.
  - The contingency plan was created in January 2007 and addresses ITA's Enterprise Network system, which includes the Core Network system.
  - System recovery procedures are referenced, but not included in the plan. ITA subsequently provided the OIG a document titled *Network Shutdown Procedures and Network Restore Procedures*. However, the document only addressed procedures for network shutdown and restart but does not provide other important procedures to restore operations after a disruption or failure.
  - The contingency plan also fails to specify the emergency scenarios that require annual testing.

Recommendations

ITA should ensure that:

1. Procedures and activities to restore operations after a failure or disruption are incorporated into the system contingency plan in accordance with Department policy.

2. ITA conducts annual contingency plan testing in accordance with Department policy and that contingency test documentation contains detailed information regarding the scope, test procedures, test scenarios, and a summary of the results.

ITA's Response

ITA concurred with these recommendations and stated that it is developing procedures to restore operations after a failure or disruption of its systems and that changes to operations are being instituted to ensure that network operations can be restored after a failure or disruption. ITA noted that the test of its Enterprise Network Contingency Plan will be completed by the end of calendar year 2007 and will include detailed agency-defined test scenarios and a summary of all test results.

OIG Comment

ITA's corrective actions are responsive to our recommendation.

Appendix A: Objectives, Scope, and Methodology

To meet the FY 2007 FISMA reporting requirements, we evaluated ITA's certification and accreditation for the core network general support system (ITA-012).

Security certification and accreditation packages contain three elements, which form the basis of an authorizing official's decision to accredit a system.

- The **system security plan** describes the system, the requirements for security controls, and the details of how the requirements are being met. As such, the security plan provides a basis for assessing security controls. Per Department policy, the security plan also includes other documents such as the system risk assessment and contingency plan.
- The **security assessment report** presents the results of the security assessment and recommendations for correcting control deficiencies or mitigating identified vulnerabilities. This report is prepared by the certification agent.
- The **plan of action & milestones** is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

Commerce's *IT Security Program Policy and Minimum Implementation Standards* requires that C&A packages contain a certification documentation package of supporting evidence of the adequacy of the security assessment. Two important components of this documentation are:

- The **certification test plan**, which documents the scope and procedures for testing (assessing) the system's ability to meet control requirements.
- The **certification test results,** which is the raw data collected during the assessment.

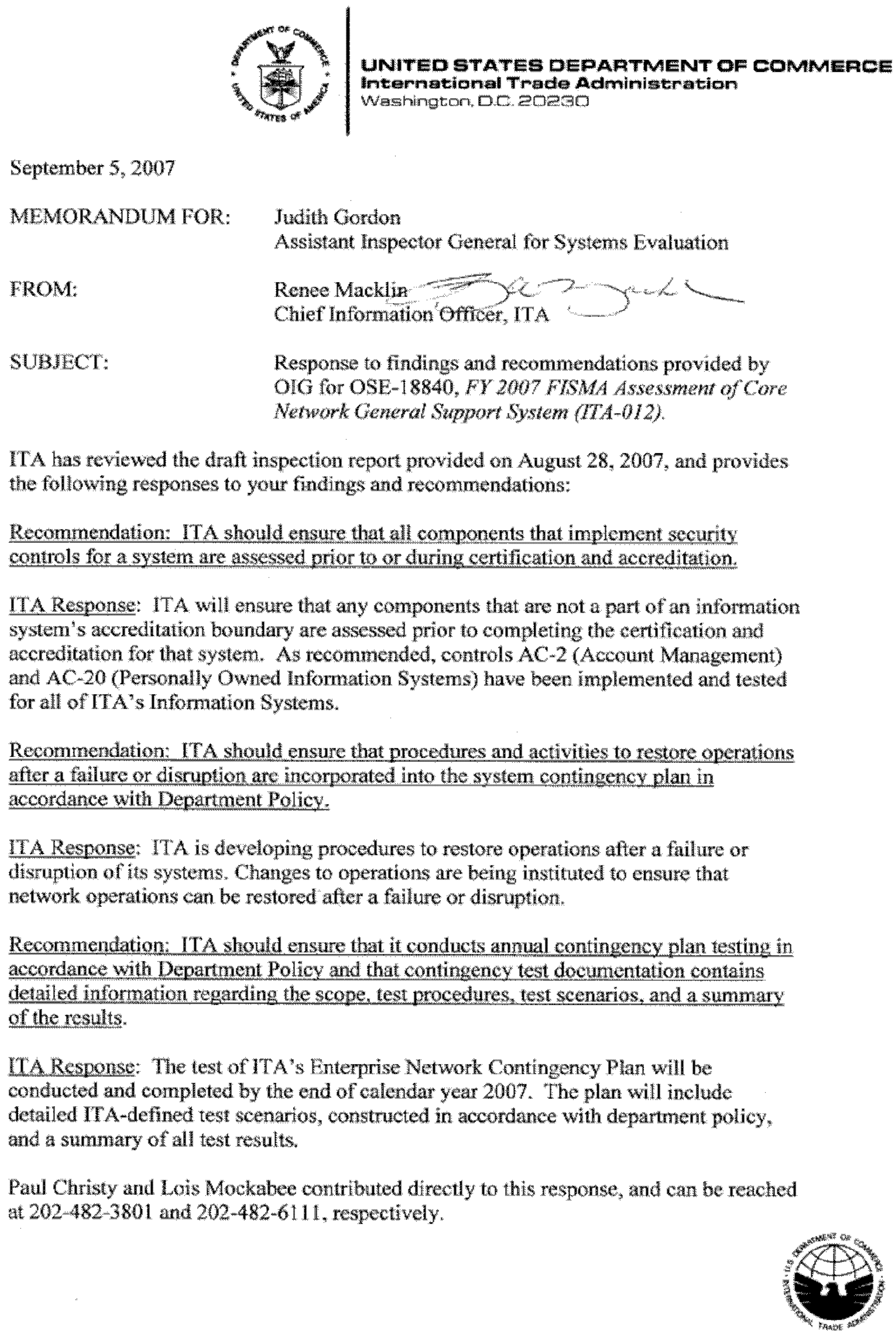
To evaluate the C&A package, we reviewed all components of the package and interviewed ITA staff to clarify any apparent omissions or discrepancies in the documentation and gain further insight on the extent of the security assessment. We give substantial weight to the evidence that supports the rigor of the security assessment when reporting our findings to OMB.

We used the following review criteria:

- Federal Information Security Management Act of 2002 (FISMA)
- U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards*
- NIST's Federal Information Processing Standards (FIPS)
    - Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
    - Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications:
    - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
    - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
    - 800-42, *Guideline on Network Security Testing*
    - 800-53, *Recommended Security Controls for Federal Information Systems*
    - 800-70, *Security Configuration Checklists Program for IT Products*

We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency in January 2005.

Appendix B
ITA's Response



UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D.C. 20230

September 5, 2007

MEMORANDUM FOR: Judith Gordon
Assistant Inspector General for Systems Evaluation

FROM: Renee Macklin
Chief Information Officer, ITA

SUBJECT: Response to findings and recommendations provided by OIG for OSE-18840, *FY 2007 FISMA Assessment of Core Network General Support System (ITA-012).*

ITA has reviewed the draft inspection report provided on August 28, 2007, and provides the following responses to your findings and recommendations:

Recommendation: ITA should ensure that all components that implement security controls for a system are assessed prior to or during certification and accreditation.

ITA Response: ITA will ensure that any components that are not a part of an information system's accreditation boundary are assessed prior to completing the certification and accreditation for that system. As recommended, controls AC-2 (Account Management) and AC-20 (Personally Owned Information Systems) have been implemented and tested for all of ITA's Information Systems.

Recommendation: ITA should ensure that procedures and activities to restore operations after a failure or disruption are incorporated into the system contingency plan in accordance with Department Policy.

ITA Response: ITA is developing procedures to restore operations after a failure or disruption of its systems. Changes to operations are being instituted to ensure that network operations can be restored after a failure or disruption.

Recommendation: ITA should ensure that it conducts annual contingency plan testing in accordance with Department Policy and that contingency test documentation contains detailed information regarding the scope, test procedures, test scenarios, and a summary of the results.

ITA Response: The test of ITA's Enterprise Network Contingency Plan will be conducted and completed by the end of calendar year 2007. The plan will include detailed ITA-defined test scenarios, constructed in accordance with department policy, and a summary of all test results.

Paul Christy and Lois Mockabee contributed directly to this response, and can be reached at 202-482-3801 and 202-482-6111, respectively.