OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Access Controls for Office of Enforcement and Compliance Assurance Systems Need Improvement

Report No. 2004-P-00015

April 26, 2004

Report Contributors:

Edward Densmore
Teresa Richardson
Debbie Hunter
Martin Bardak
Bill Coker

Abbreviations

EPA	Environmental Protection Agency
FTTS	Federal Insecticide, Fungicide, and Rodenticide Act/ Toxic Substance Control Act Tracking System
ICIS	Integrated Compliance Information System
OECA	Office of Enforcement and Compliance Assurance
OIG	Office of Inspector General
OMB	Office of Management and Budget
SSTS	Section Seven Tracking System

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

April 26, 2004

MEMORANDUM

SUBJECT: Access Controls for Office of Enforcement and Compliance Assurance Systems Need Improvement
Report No. 2004-P-00015

FROM: Patricia H. Hill, Director
Business Systems Audits (2421T)

TO: Michael M. Stahl, Director
Office of Compliance
Office of Enforcement and Compliance Assurance (2221A)

This is a our final report regarding implementation of authentication and identification controls. This audit report contains a finding that describes a problem the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA) has identified and the corrective action the OIG recommends. This report represents the opinion of the OIG, and the finding contained in this audit report does not necessarily represent the final EPA position. Final determinations on matters in this audit report will be made by EPA managers in accordance with established EPA audit resolution procedures.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to the finding and recommendation presented in this audit report within 90 days of the report date. You should include a corrective action plan for agreed upon actions, including milestone dates. We have no objection to the further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oig. If you or your staff have any questions regarding this report, please contact me at (202) 566-0894 or the Assignment Manager, Ed Densmore, at (202) 566-2565.

Purpose

On September 30, 2003, we issued Report No. 2003-P-00017, *EPA's Computer Security Self-Assessment Process Needs Improvement,* which identified weaknesses related to the EPA's self-assessment process and made recommendations to the Office of Environmental Information's Director for Technology, Operations and Planning. Among other things, the audit assessed whether: (1) computer security self-assessments were accurate and complete; (2) EPA identified all major applications; and (3) major application systems used authentication and identification controls to protect against unauthorized access and misuse.

During the prior audit, we had identified some access control weaknesses specific to three Office of Enforcement and Compliance Assurance (OECA) systems. This additional report addresses those OECA system-specific weaknesses we found during our review.

Background

The Federal Information Security Management Act and its predecessor, the Government Information Security Reform Act, require all Federal agencies to conduct annual reviews of their security program and to report the results of those assessments to the Office of Management and Budget (OMB). OMB reviews the assessment results to determine how well agencies implemented security requirements.

The OECA systems we reviewed are critical to EPA's enforcement and compliance activities of the Agency. These systems are:

- **Federal Insecticide, Fungicide, and Rodenticide Act/Toxic Substance Control Act Tracking System (FTTS).** FTTS supports the day-to-day tracking of inspections for pesticides, as well as compliance and enforcement under the applicable EPA laws.

- **Section Seven Tracking System (SSTS).** Similar to FTTS, SSTS supports the pesticides program by tracking pesticide-producing establishments, registration records of new establishments, and the types and amounts of pesticides produced at each establishment. This also contains Confidential Business Information, such as the addresses of the pesticide-producing establishments.

- **Integrated Compliance Information System (ICIS).** ICIS integrates the national compliance and enforcement data from numerous individual systems. This system is expected to eventually integrate data regarding all media that EPA regulates (e.g., air, toxics, pesticides, and hazardous waste).

Scope and Methodology

We conducted audit field work at EPA Headquarters and Regions 1, 2, 3, 5, and 6. To accomplish this audit objective, we used a variety of criteria, including:

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources.*
- National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*.
- EPA Directive 2195A1, *Information Security Manual*.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We reviewed system access listings and verified that users still needed access to the system. We also tested their respective levels of access to ensure they were appropriate. In addition, we reviewed system coordinator/administrator listings to determine whether adequate personnel had been assigned to ensure the availability of the systems to users.

Prior Audit Coverage

- **EPA OIG Report No. 2003-P-00017**, *EPA's Computer Security Self-Assessment Process Needs Improvement*, dated September 30, 2003: This report recommended implementing a systematic monitoring and evaluation program to increase the reliance management can place on the information technology security data it collects.

- **EPA OIG Report No. 2002-S-00017**, *Government Information Security Reform Act: Status of EPA Computer Security Program*, dated September 16, 2002: This report noted that management must continue to seek improvements in the areas of risk assessments, effective oversight processes, and training employees with significant security responsibilities.

Results of Review

Access controls to three critical OECA systems (FTTS, SSTS, and ICIS) need improvement. Inadequate implementation of access controls increases the possibility of valid users not being able to gain access to these systems in a timely manner should a problem occur. Moreover, these vulnerabilities increase the potential for unauthorized changes to system data. These weaknesses occurred because user access lists were either not reconciled or not consistently reconciled. Specifically:

- We found that some regions did not have a backup system administrator/coordinator for FTTS and SSTS to ensure the proper administration and availability of the system. A system administrator has the ability to grant, remove, or change a user's access. A system coordinator begins the process of facilitating the granting, removing and changing of a user's access. An extended absence of a system administrator/coordinator could delay a valid user from being granted access to a system, and could impede the timely removal of users that no longer need access. We brought this finding to the attention of the responsible systems administrators/coordinators, and they granted system administrator/coordinator access to some users who will serve as backups to the primary system administrator/coordinator.

- We identified instances where users' access levels were not appropriate for their job functions. For example, we identified three SSTS users with system update ability who no longer needed access to the system to perform their duties. Management placed the system data in jeopardy of unauthorized alteration by not promptly removing this access. In addition, we found an ICIS user who unnecessarily possessed system administrator rights, thereby allowing this user to add, delete, or alter data, as well as grant this access to other individuals. This user confirmed system administrator rights were no longer needed. System administrator access should be strictly controlled and, in this instance, there were an adequate number of ICIS users with this ability. After bringing this weakness to the attention of OECA officials, the system access levels for the users involved were appropriately changed.

These systems contain confidential or enforcement sensitive data that is critical to the compliance/enforcement activities of the Agency. Therefore, adequate access controls are vital to ensure the availability and integrity of the compliance and enforcement data in these systems.

The noted weaknesses occurred because the systems' user access lists either were not reconciled or were not consistently reconciled, as required by Agency policy. EPA's Information Security Manual stipulates that managers of major applications must ensure access controls are reviewed monthly. In particular, information managers should verify that the system access lists reflect only valid users and the appropriate levels of access for them to perform their jobs. During our audit, we found no indication that system administrators conducted reconciliations of the access listings for FTTS and ICIS. System administrators said they added and removed users based on an informal process and were not performing any reconciliations. We also found reconciliations were not occurring consistently with the SSTS access listings; frequent changes in SSTS system coordinators caused the reconciliation process to be overlooked as new coordinators familiarized themselves with their duties.

Recommendation

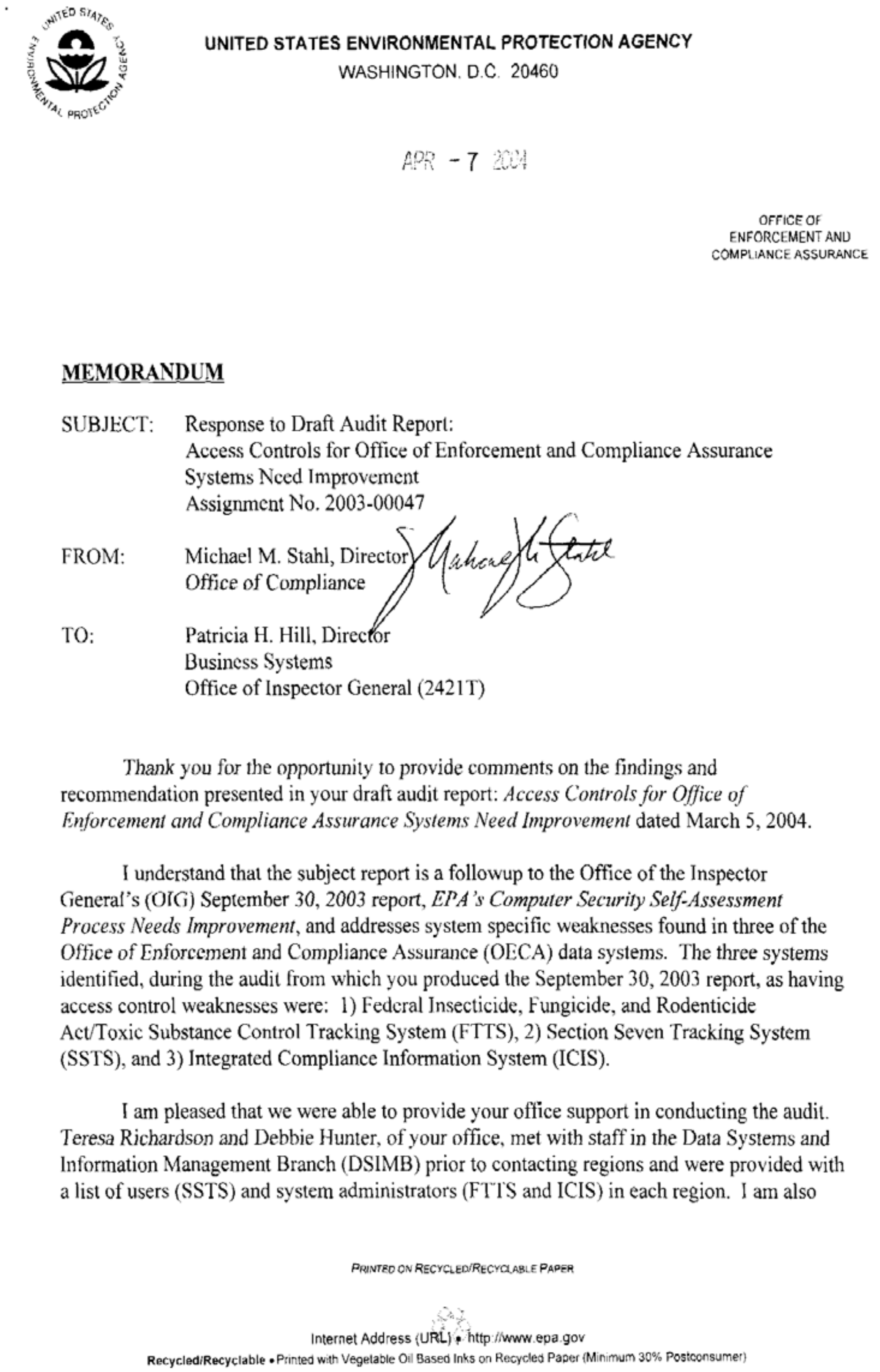
We recommend that OECA's Director for Compliance:

1. Reiterate to information managers their responsibilities in EPA's *Information Security Manual* requiring them to verify (i.e., reconcile) that access lists reflect only valid users and the appropriate access levels commensurate with the users' current job functions.

Agency Comments and OIG Evaluation

In a memorandum dated April 7, 2004, OECA's Director for the Office of Compliance responded to our draft report (see Appendix A) and concurred with our recommendation. However, OECA disagreed with our statement that "Access to three critical OECA systems (FTTS, SSTS, and ICIS) was not *adequately* controlled," and asserted that procedures have been in place and access to the systems is controlled. We do not dispute that controls exist, but believe that our statement is accurate because the weaknesses identified were caused by inadequately implemented controls. Nevertheless, we modified the report so that it cannot be interpreted that no controls are in place. OECA also stated that these weaknesses were not identified at Headquarters, and we agree. Although we did not state in our draft report where the weaknesses were identified, we clarified the report to indicate the weaknesses were found in the regions.

Appendix A



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

APR - 7 2004

OFFICE OF
ENFORCEMENT AND
COMPLIANCE ASSURANCE

MEMORANDUM

SUBJECT: Response to Draft Audit Report:
Access Controls for Office of Enforcement and Compliance Assurance
Systems Need Improvement
Assignment No. 2003-00047

FROM: Michael M. Stahl, Director
Office of Compliance

TO: Patricia H. Hill, Director
Business Systems
Office of Inspector General (2421T)

Thank you for the opportunity to provide comments on the findings and recommendation presented in your draft audit report: *Access Controls for Office of Enforcement and Compliance Assurance Systems Need Improvement* dated March 5, 2004.

I understand that the subject report is a followup to the Office of the Inspector General's (OIG) September 30, 2003 report, *EPA's Computer Security Self-Assessment Process Needs Improvement*, and addresses system specific weaknesses found in three of the Office of Enforcement and Compliance Assurance (OECA) data systems. The three systems identified, during the audit from which you produced the September 30, 2003 report, as having access control weaknesses were: 1) Federal Insecticide, Fungicide, and Rodenticide Act/Toxic Substance Control Tracking System (FTTS), 2) Section Seven Tracking System (SSTS), and 3) Integrated Compliance Information System (ICIS).

I am pleased that we were able to provide your office support in conducting the audit. Teresa Richardson and Debbie Hunter, of your office, met with staff in the Data Systems and Information Management Branch (DSIMB) prior to contacting regions and were provided with a list of users (SSTS) and system administrators (FTTS and ICIS) in each region. I am also pleased that DSIMB provided continued support to the OIG as the audit progressed from region to region.

OECA concurs with the recommendations of the March 5, 2004 draft audit report to: "Reiterate to information managers their responsibilities in EPA's *Information Security Manual* requiring them to verify (i.e., reconcile) that access lists reflect only valid users and the appropriate access levels commensurate with the users' current job functions." However, we believe some of the findings are inaccurately documented in the report. Specifically, in the *Results of Review* section of the draft report the inaccuracies stated are:

1) The first sentence of the *Results of Review* section states: "Access to three critical OECA systems (FTTS, SSTS, and ICIS) was not adequately controlled."

OECA disagrees with this statement. While additional control may be required, procedures have been in place and access to the systems is controlled. As documented in the System Security Plans, all system administrators are given the rules of behavior to be provided and discussed with each user.

2) An inaccuracy appears in the first bullet within the *Results of Review* section, where it is stated: "Neither FTTS nor SSTS had a backup system administrator ..."

FTTS is a stand alone system that resides in each region and in Headquarters (Office of Regulatory Enforcement (ORE)). The statement may be true for some of the regional instances of FTTS, but it is inaccurate for Headquarters. There are system administrator backups identified for the Headquarters instance of FTTS. SSTS is a Headquarters only system and backups are identified.

3) Also within the first bullet of the *Results of Review* section it is stated: "An extended absence of a system administrator could delay a valid user from being granted access..."

This may be misleading as there is an extended process to gain or remove user access. The system administrator plays a pivotal role, but the extended process is not solely dependent on the immediate availability of the system administrator. The headquarters and regional document control office, the regional division director or equivalent, and the FIFRA security officer play a major role in the process. Also, the statement is not relevant to SSTS as backup system administrators are identified.

4) In the second bullet of the *Results of Review* section it is stated: "We identified instances where users' access levels were not appropriate for their job functions."

System Administrators periodically review user ids and account information to determine if users require access to the system. At Headquarters, the System Administrator periodically checks the mainframe computer security access privileges (known as Resource Access Control Facility (RACF)) for users and compares this with access privileges for the SSTS system. If no RACF privileges exist, the user access to SSTS is removed.

OECA considers security and controlling access to the data systems a top priority and a serious matter. A number of ongoing efforts are underway to ensure access control is managed and adequately controlled for these data systems.

First, with regard to FTTS, when the System Manager within OECA conducts training in the regions he makes a point of verifying access controls with the regional FTTS coordinator and with the regional Local Area Network (LAN) Administrator. On the initial day of a training trip he works with both parties to install training software and reconcile the user access list.

Second, with regard to SSTS, the following documents have been provided to the regional System Administrators: the FIFRA CBI Security Briefing, the FIFRA Access Authorization Agreement For Trade Secrets and CBI, and the FIFRA Information Security Manual. The System Manager within OECA assists the regional System Administrators in using these documents to ensure secure access controls.

Third, with regard to ICIS, training is conducted on the roles and responsibilities of ICIS users during the annual ICIS National Meeting where all System Administrators are expected to be present. Also, a separate document specifying the roles and responsibilities of the ICIS System Administrators is being developed. In addition, the roster of ICIS System Administrators will be reviewed periodically by Headquarters to confirm the continued appropriateness of the designation of System Administrators.

If we can provide any additional assistance with this audit, please contact John Hovell, Chief of the Data Systems and Information Management Branch, at 202-564-5018, or at email address hovell.john@epa.gov.

cc: David Hindin, OECA
Greg Marion, OECA

Appendix B

Distribution

Director, Office of Compliance (221A)
Branch Chief, Data System and Information Management Branch (2222A)
Audit Liaison, Office of Enforcement and Compliance Assurance (2201A)
Comptroller (2731A)
Agency Followup Official (the CFO) (2710A)
Agency Audit Followup Coordinator (2724A)
Associate Administrator for Congressional and Intergovernmental Relations (1301A)
Associate Administrator, Office of Public Affairs (1101A)
Inspector General (2410)