Office of Inspector General

Audit Report

INFORMATION TECHNOLOGY

Review of Off-Site Consequence Analysis Information Management

Audit Report Number 2002-P-00006

March 22, 2002

Inspector General Division Conducting the Audit	**Information Technology Audits Staff, Washington, DC**
Region Covered	**Headquarters**
Program Office Involved	**Chemical Emergency Preparedness and Prevention Office**
Audit Team Members	**Edward Densmore** **Kelli Cooper** **Martin Bardak**

Abbreviations

CEPPO	Chemical Emergency Preparedness and Prevention Office
CSISSFRRA	Chemical Safety Information, Site Security and Fuels Regulatory Relief Act
EPA	U. S. Environmental Protection Agency
OCA	Off-Site Consequence Analysis
OIG	Office of Inspector General
RMP	Risk Management Plan
SRMP	System for Risk Management Plans

MEMORANDUM

SUBJECT: Final Report: Review of Off-Site Consequence
Analysis Information Management
Report No. 2002-P-00006

FROM: Edward Densmore, Project Manager
Information Technology Audits Staff (2421)

TO: Jim Makris, Director
Chemical Emergency Preparedness and Prevention Office (5104A)

Mark Day, Director
Office of Technology, Operations and Planning (2381)

Purpose

The objective of this audit was to review the release of Off-Site Consequence Analysis (OCA) information that was not authorized for public disclosure on the Chemical Emergency Preparedness and Prevention Office (CEPPO) website and determine the adequacy of controls over the collection, maintenance, and dissemination of OCA data. OCA information is used to help prevent chemical accidents, and provide an estimate of the potential consequences to a surrounding community of one or more hypothetical accidental chemical releases.

Background

CEPPO provides leadership, advocacy, and assistance to: (1) prevent and prepare for chemical emergencies; (2) respond to environmental crises; and (3) inform the public about chemical hazards in their community. To protect human health and the environment, CEPPO develops, implements, and coordinates regulatory and non-regulatory programs in partnership with all Environmental Protection Agency (EPA) regions, domestic and international organizations in the public and private sectors, and the general public.

In 1990, the Clean Air Act (Public Law 101-549) was amended in response to public concerns about what could be done to prevent chemical accidents from occurring in their communities. Regulations require industry to inform EPA and States on how they manage chemical risks and what they are doing to reduce risk to the community. Certain facilities are required to submit a Risk Management Plan (RMP) to EPA to document what they are doing to prevent accidents, and how they plan to manage their chemicals and operate in a safe and responsible manner. RMPs include facility registration information, OCA data, a 5-year accident history, and information on prevention and emergency response programs.

A contractor (hereafter referred to as the database contractor) receives the RMPs and compiles the information in the System for Risk Management Plans (SRMP). SRMP is an Oracle database developed by a second contractor (hereafter referred to as the program contractor), and the database is used to consolidate the RMPs. SRMP is comprised of six subsystems, including RMP*Info^{TM}, which contains summaries of facility RMPs in 50 separate downloadable State database files. These database files were made available to the public on EPA's website.

Public Law 106-40, the *Chemical Safety Information, Site Security and Fuels Regulatory Relief Act* (CSISSFRRA), enacted on August 5, 1999, required that OCA information be made available to authorized officials for emergency planning and response purposes. It included a provision to exempt OCA information from public disclosure for one year from the Act's inception, or until regulations were promulgated. EPA and the Department of Justice issued a rule in August 2000, entitled *Accidental Release Prevention Requirements; Risk Management Programs Under the Clean Air Act Section 112(r)(7); Distribution of Off-Site Consequence Analysis Information,* authorizing some OCA data elements to be made public.

In April 2001, OCA information was made available in downloadable state database files from CEPPO's website for the first time. However, the April 2001 files made some unauthorized elements of OCA information available for download. A CEPPO official detected the error on June 6, 2001, and took action to immediately have the information removed from the website. In June 2001, the Director of CEPPO requested the Office of Inspector General to examine the cause of the incident, the actions taken, and systemic changes necessary to prevent this type of an event from reoccurring.

Scope and Methodology

This audit examined the incident involving the unauthorized OCA data being made available for download on the CEPPO website. As part of our review, we examined CEPPO's oversight of the contractors responsible for making programmatic changes to the RMP program and running the SRMP. We also reviewed EPA's procedures to make information available on the website. Finally, we examined the RMP*Info download logs from April 2001 through June 2001.

We conducted our audit fieldwork from July 2001 to December 2001 at EPA Headquarters in Washington, DC. We interviewed CEPPO and Office of Environmental Information officials within EPA, and contractor personnel responsible for programming and maintaining the SRMP.

Our review included identifying who downloaded information from the CEPPO website, reviewing statements of work for the contractors, and the change control process for making changes to the SRMP. In addition, we reviewed and analyzed policies, standards, and procedures specifically related to the audit objectives. There was no prior audit coverage relating to the CEPPO office or the SRMP. We conducted this audit in accordance with "Government Auditing Standards", issued by the Comptroller General of the United States.

Results of Review

Unauthorized OCA information was inadvertently made available for download on the EPA website from April to June 2001. As a result of this information being made available for download on EPA's website, unauthorized individuals had access to sensitive OCA data. This occurred due to a lack of management oversight over the software testing of program changes to the SRMP. Specifically, CEPPO did not adequately oversee the database and program contractors responsible for maintaining the SRMP system, and processing the RMPs submitted to EPA.

Unauthorized Information Available on EPA's Website

OCA information, not authorized for public disclosure on the Internet, was unintentionally made available for downloading on EPA's website from April to June 2001. The Clean Air Act requires facilities to submit RMPs to EPA if they have specific toxic and/or flammable chemicals greater than the established thresholds. The RMP information is received by the database contractor, who inputs the RMP information into SRMP. This contractor then provides the consolidated information to EPA, and the information is then made available for download from the website, as required by CSISSFRRA.

The August 1999 enactment of CSISSFRRA exempted OCA information from disclosure under the Freedom of Information Act, and limited public availability for at least one year. OCA data could be made available to Federal, State, and local officials, including members of Local Emergency Planning Committees, as well as qualified researchers. However, these individuals were prohibited from releasing the OCA information to the public in the specific form of the RMP. In August 2000, EPA and the Department of Justice jointly issued a rule stating that portions of the OCA information (e.g., concentration of chemical released, duration of release, wind speed, etc.) should be included on the Internet as publicly accessible information.

In April 2001, the program contractor provided the database contractor an upgrade to include the OCA information in the downloadable files for the first time. The database contractor used the upgrade to create the April 2001 release of downloadable files. The database contractor provided the files to EPA, and they were made available for download on the website. However, this release included some unauthorized elements of OCA information. Specifically, Alternative Release Scenario information, such as the radius of the vulnerable zone and the estimated population effected by the chemical release, were included. The subsequent releases in May and June 2001 also included the unauthorized elements of OCA information.

As a result of this information being made available for download on EPA's website, unauthorized individuals had access to sensitive OCA information. Specifically, OCA information provides a general account of the consequences of a chemical release in terms of the damage that might be inflicted on a facility's surrounding community. This includes a rough sketch of what is involved in triggering a release from an RMP facility, including the name of the chemical involved, the projected quantity of chemical released, and the duration of the release. In addition, a map or graphic of the alternative release scenario, may be included. This information could be used by terrorist organizations to identify and prioritize target facilities that would have the greatest catastrophic impact.

Improvements Needed in Oversight of Software Testing

CEPPO management did not ensure that adequate testing was performed for program changes to the RMP database. The CEPPO project manager stated that prior to the incident, testing and quality assurance were performed by the database contractor for the input of data, not for the output. CEPPO personnel, as well as the database contractor, did not pay close enough attention to the RMP downloads to determine whether the data was sensitive. They became too comfortable with the work of the program contractor because of the high quality and reliability of prior software changes. Consequently, testing performed by the program contractor responsible for making changes to the SRMP was not adequately reviewed by CEPPO to ensure the data fields reflected information authorized for release.

We found testing was performed using only six test RMPs that were internally generated by the program contractor for testing software changes. The SRMP, which is designed to maintain thousands of RMPs and allow for various queries of all compiled data, should have been tested with a larger sample. Also, the contractor did not test for the differentiation of the fields for public and non-public OCA data. CEPPO did not identify this as a potential deficiency with the testing. The program contractor stated they did not test for these differentiations, nor focus close enough attention to the potential for unauthorized OCA data being disclosed.

Actions Taken By CEPPO

On June 6, 2001, a CEPPO official identified that unauthorized information was available for download from the EPA website, and immediately notified both the program and database contractors. Within a few hours, the program contractor delivered to the database contractor two programs. One program was to correct the problem; the second was to monitor and ensure unauthorized OCA data would not be viewable to the general public once the RMP databases were again made available on EPA's website. Since the discovery of the unauthorized OCA information, CEPPO implemented new practices to ensure sensitive data will not be erroneously released. Specifically, CEPPO personnel now closely review the RMP database output to ensure only authorized public information is released. In addition, CEPPO wrote programs that they run against the RMP downloads to ensure unauthorized OCA data is not included on EPA's website.

Actions Taken by Contractors

The program contractor now requires peer reviews and more thorough levels of testing throughout the project life cycle. The database contractor's procedures now include testing of input, as well as ensuring unauthorized OCA data is not included in the releases provided to EPA. The database contractor also runs a program that reviews the RMP databases to ensure only information that should be disclosed through EPA's website is accessible. Finally, the database contractor manually reviews at least five records before the data is released to EPA.

Recommendations

We recommend the Director of the Chemical Emergency Preparedness and Prevention Office:

1. Establish a policy requiring that the downloadable database files are reviewed to ensure only authorized elements of OCA data are made available to the public.

2. Require current and future RMP database outputs be reviewed to ensure only authorized public information is released.

3. Establish requirements for testing SRMP programing changes to:

    a. Include steps to ensure OCA information, not authorized for public disclosure on the Internet, is not made available for download.

    b. Verify that adequate testing of changes for the SRMP database are performed and documented.

EPA Response

The March 19, 2002, response from the Office of Solid Waste and Emergency Response (OSWER) indicated that CEPPO agrees with the above-stated recommendations (see Attachment 1). Specifically, CEPPO completed modifications to the SRMP, to ensure protection of OCA information. The software development contractor performed extensive testing on these modifications, and the controls CEPPO instituted will remain a permanent part of the operating procedures. The CEPPO project manager verifies that adequate testing of changes to the SRMP database has been performed and documented. Finally, CEPPO will provide actual OCA data to the development contractor for testing system modifications.

The Office of Technology Operations and Planning (OTOP) responded to the draft report on March 14, 2002, and had no comments (see Attachment 2).

OIG Evaluation

In our opinion, the actions taken by CEPPO will assist in safeguarding non-public OCA information from public disclosure. The modifications made to the SRMP eliminates the ‘placeholders’ for non-public OCA data in the files made available for download. However, CEPPO needs to ensure, when future modifications are made to the SRMP, only public OCA information is released. CEPPO should establish a policy requiring downloadable files to be reviewed to confirm only OCA information suitable for public disclosure is made available. In addition, while we agree with the actions taken by CEPPO project management to verify testing has been performed and documented, requirements need to be established to ensure verification and documentation of testing will continue.

Action Required

This audit report contains findings that describe problems the OIG has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG and the findings contained in this audit report do 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 audit resolution procedures.

In accordance with EPA Order 2750, you, as the action official, are required to provide us with a written response to the audit report within 90 days of the final audit report date. For corrective actions planned but not completed by the response date, reference to specific milestone dates will assist us in deciding whether to close this report.

We appreciate your positive response to the recommendations presented in the report and the actions you and your staff have taken to ensure security over the release of OCA data. We have no objections to the further release of this report to the public. Should you or your staff have any questions regarding this report, please contact Kelli Cooper, Auditor-In-Charge, at (202) 260-8981.

Attachments

cc: Kathy Jones, Associate Director of Program Implementation and Coordination Staff
Peter Gattuso, Information Management Specialist
Dorothy McManus, Program Analyst

Attachment 1

OSWER Comments to Draft Report

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

MAR 19 2002

OFFICE OF
SOLID WASTE AND EMERGENCY
RESPONSE

MEMORANDUM

SUBJECT: Response to OIG Draft Report "Review of Off-Site Consequences Analysis Information Management Audit Number 2001-001308"

FROM: Marianne Lamont Horinko
Assistant Administrator

TO: Edward Densmore, IT Audit Manager
Information Technology Audits Staff (2421)

We have reviewed the subject draft report, and we have no additional comments regarding the factual accuracy of the report. However, in response to the recommendations, we have taken the following corrective actions.

OIG Recommendation

Establish a policy requiring that the downloadable database files are reviewed to ensure only authorized elements of Off-Site Consequence Analysis (OCA) data are made available to the public.

OSWER Response

The Chemical Emergency Preparedness and Prevention Office (CEPPO) has completed modifications to its Systems for Risk Management Plans (SRMP) that will ensure protection of OCA information. Specifically, after the accidental posting of download files, including OCA data last June, CEPPO proposed the elimination of the placeholders or slots for non-public OCA in those files that could be distributed to the public. This change makes it impossible for non-public OCA data to be released in those files. These database and software changes were completed and put into production for the Risk Management Plan (RMP) files we received in February, 2002.

The software development contractor performed extensive testing to ensure that our enhanced requirements were fully met. In addition, the redundant checks that we instituted at the Reporting Center remain in place as a permanent part of the operating procedures. As a final step, CEPPO project managers will confirm that the non-public OCA slots are indeed no longer part of the data files.

OIG Recommendation

Require current and future RMP database outputs be reviewed to ensure only authorized public information is released.

OSWER Response

As indicated above, the Reporting Center is required to perform a number of redundant checks as part of their normal operating procedures. Additionally, CEPPO confirms that RMP database outputs do not include the non-public OCA data. Since September 11th, CEPPO has not posted download files on the Internet.

OIG Recommendation

Establish requirements for testing SRMP programming changes to:

a. Include steps to ensure OCA information, not authorized for public disclosure on the Internet, is not made available for download; and

b. Verify that adequate testing of changes for the SRMP database are performed and documented.

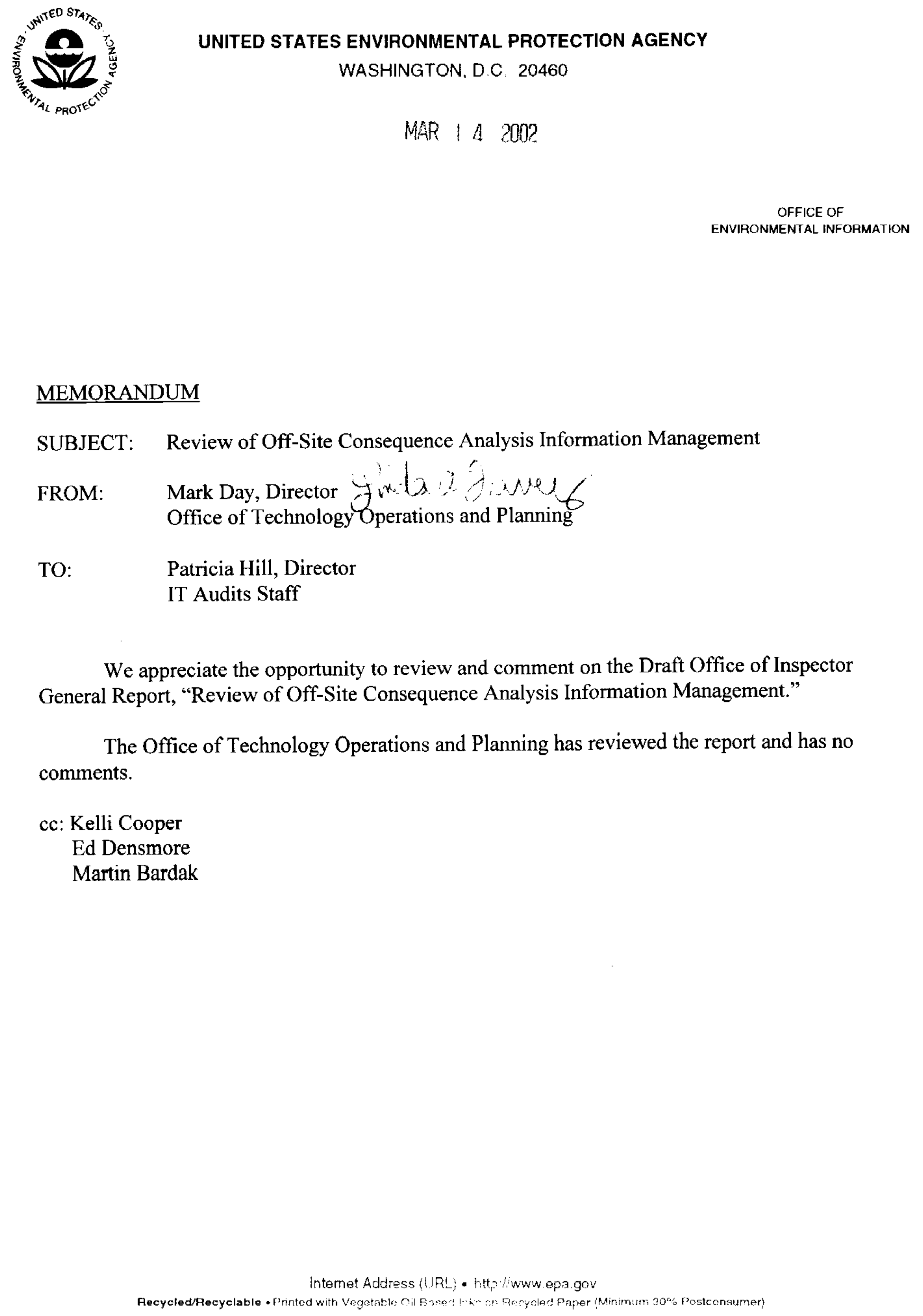
OSWER Response

The software development contractor has always been required to provide extensive testing. To ensure that changes involving OCA data are appropriately tested, CEPPO will now provide actual OCA data to the development contractor to ensure optimum testing. Prior to implementing these programming changes, the CEPPO project manager will verify that the testing has been performed and documented.

If you have any questions regarding this response, please contact Kathy Jones at (202) 564-8353 or Johnsie Webster, OSWER Audit Liaison, at (202) 260-4475.

Attachment 2

OTOP Comments to Draft Report



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

MAR 14 2002

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: Review of Off-Site Consequence Analysis Information Management

FROM: Mark Day, Director
Office of Technology Operations and Planning

TO: Patricia Hill, Director
IT Audits Staff

We appreciate the opportunity to review and comment on the Draft Office of Inspector General Report, "Review of Off-Site Consequence Analysis Information Management."

The Office of Technology Operations and Planning has reviewed the report and has no comments.

cc: Kelli Cooper
Ed Densmore
Martin Bardak

Attachment 3

Report Distribution

Office of Inspector General

Inspector General (2410)

Headquarters Offices

Assistant Administrator, OSWER (5101)
Director, CEPPO (5104A)
Director, OTOP (2381)
Comptroller (2731A)
Agency Followup Official (2710A)
Audit Liaison, OSWER (5103)
Audit Liaison, OEI (2811R)
Agency Audit Followup Coordinator (2724A)
Associate Administrator for Congressional and Intergovernmental Relations (1301A)
Associate Administrator for Communications, Education, and Media Relations (1101A)