U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Briefing Report

ECHO Data Quality Audit – Phase I Results: The Integrated Compliance Information System Needs Security Controls to Protect Significant Non-Compliance Data

Report No. 09-P-0226

August 31, 2009

Abbreviations

DMR	Discharge Monitoring Report
ECHO	Enforcement and Compliance History Online
EPA	U.S. Environmental Protection Agency
ICIS	Integrated Compliance Information System
IDEA	Integrated Data for Enforcement Analysis
NPDES	National Pollutant Discharge Elimination System
OECA	Office of Enforcement and Compliance Assurance
OIG	Office of Inspector General
PCS	Permit Compliance System
SNC	Significant Non-Compliance

U.S. Environmental Protection Agency
Office of Inspector General

At a Glance

Catalyst for Improving the Environment

ECHO Data Quality Audit – Phase I Results: The Integrated Compliance Information System Needs Security Controls to Protect Significant Non-Compliance Data

What KPMG Found

End users of the Permit Compliance System and Integrated Compliance Information System National Pollutant Discharge Elimination System (ICIS-NPDES) can override the Significant Non-Compliance (SNC) data field without additional access controls. This occurs because EPA has not implemented database security features to restrict access to this field. Further, the ICIS-NPDES database edit checks do not prevent access to the SNC field. As a result, users can change original data without authorization, which could directly affect ICIS-NPDES data made available to the public via ECHO.

Other than the above weakness, KPMG noted that EPA implemented many effective processes designed to populate the Integrated Data for Enforcement Analysis (IDEA) database, which the ECHO system uses to create reports for its users. KPMG noted that many of the EPA systems that feed data to IDEA have front-end edit checks designed to help ensure data quality. Further, KPMG noted that making data available through ECHO is a very complex process that involves many data systems. KPMG noted that EPA has developed a methodology to manage the States' data conversions. KPMG noted that EPA's data mapping and system life-cycle documentation, data migration tools, and lessons learned processes are effective in managing this complex data conversion process.

What KPMG Recommends

The Director, Office of Compliance, Office of Enforcement and Compliance Assurance (OECA), should implement database security features to limit the end users' ability to change the SNC code in ICIS-NPDES.

On August 6, 2009, the EPA Office of Inspector General met with OECA to provide a briefing report of KPMG's work to date and discuss the SNC code finding. OECA provided informal comments on the finding. OECA plans to explore additional options to restrict manual SNC code override in ICIS-NPDES.

August 31, 2009

MEMORANDUM

SUBJECT: ECHO Data Quality Audit – Phase I Results:
The Integrated Compliance Information System Needs
Security Controls to Protect Significant Non-Compliance Data
Report No. 09-P-0226

FROM: Rudolph M. Brevard   *Rudolph M. Brevard*
Director, Information Resources Management Assessments
Office of Mission Systems

TO: Cynthia Giles
Assistant Administrator
Office of Enforcement and Compliance Assurance

Attached is the briefing report for the first phase of the data quality audit of the Enforcement and Compliance History Online system. KPMG, LLP, conducted this audit on behalf of the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems KPMG identified and corrective actions KPMG recommends. This report represents the opinion of KPMG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

KPMG conducted this portion of the audit from July 2008 to June 2009 at EPA Headquarters in Washington, DC, in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. These standards require planning and performing the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions. KPMG believes that the evidence obtained provides a reasonable basis for the findings and recommendations.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report. We are requesting your response within 90 calendar days. You should include a corrective actions plan for agreed upon actions, including milestone dates.

We would like to thank your staff for their cooperation. We have no objections to the further release of this report to the public. This report will be available at http://www.epa.gov/oig.

If you or your staff has any questions regarding this report, please contact me at (202) 566-0893 or brevard.rudy@epa.gov; or Harry Kaplan, Project Manager, at (202) 566-0898 or kaplan.harry@epa.gov.

cc:
Lisa C. Lund
Gwendolyn Spriggs

ECHO Data Quality Audit – Phase I Results: The Integrated Compliance Information System Needs Security Controls to Protect Significant Non-Compliance Data

KPMG

Agenda

- Objective and Scope

- Progress To Date

- Planned Tasks

- Observations and Recommendations

- Questions & Answers

KPMG

Objective and Scope

The overall audit objective is to evaluate the processes and controls used to support the quality of data that is ultimately presented through Enforcement Compliance History Online (ECHO) system queries.

The audit scope includes two phases:

◆ **Phase I --** Data integrity review of processes and controls used to populate the Integrated Data for Enforcement Analysis (IDEA)

◆ **Phase II --** Data quality processes and controls for select source systems that feed IDEA

We selected and reviewed the Permit Compliance System (PCS) and Integrate Compliance Information System National Pollutant Discharge Elimination System (ICIS-NPDES) as the source systems for this project.

Progress Update

◆ We have conducted meetings with officials from:

➢ Office of Enforcement and Compliance Assurance

➢ Office of Environmental Information

➢ Veterans Affairs Office of Inspector General to discuss system mainframe controls

➢ State of Georgia to discuss ICIS-NPDES

➢ Region IV to discuss PCS and ICIS-NPDES

KPMG

Progress Update (cont)

♦ We have gained an understanding of the process used to populate IDEA and ECHO.

♦ We have gained an understanding of the PCS and ICIS-NPDES data elements and related data quality processes.

♦ We have gained an understanding of the State conversion process from PCS to ICIS-NPDES.

KPMG

Planned Tasks

- Perform testing of key PCS and ICIS-NPDES business rules to validate data logic.

- Trace a sample of PCS and ICIS-NPDES data elements into IDEA to test IDEA data quality.

- Review select supporting source documentation (e.g., DMRs) supporting PCS and ICIS-NPDES, and ultimately IDEA.

- Review select PCS and ICIS-NPDES controls over data field security.

- Test controls over the conversion process from PCS to ICIS-NPDES

KPMG

Observations and Recommendations

◆ **Observation #1**:

EPA appears to have effective processes designed to populate IDEA from the source systems.

KPMG

Observations and Recommendations

◆ **Observation #2**:

With such a large and complex data conversion, EPA has developed a methodology for the States conversion process that includes mapping documentation, system development life-cycle documentation, migration tools, and a lessons learned process after each state conversion that is used to update the methodology for future conversions.

Some key parts of this process

➢ Workgroup meeting and conference calls;

➢ Test runs for the data conversion;

➢ Data element mapping from PCS to ICIS-NPDES

Observations and Recommendations (cont)

◆ **Observation #3:**

ICIS-NPDES has front end edit checks designed to help ensure data quality. For example, we noted that ICIS-NPDES provides warnings if DMR data exceeds authorized limits. Note that we have not yet tested the full effectiveness of the edit check controls.

KPMG

Observations and Recommendations (cont)

◆ **Observation #3:** *(Continued)*

During our ICIS-NPDES demonstration that the Georgia data steward showed us, there appears to be strong front end edit checks that are designed to ensure data quality. The data steward told us that the new screen layout made data entry "user friendly" and more intuitive

Information from the DMR is the source for information entered into ICIS-NPDES.

When data is entered into the data field, it is checked to ensure it is the correct data type (i.e. alpha, numeric). If the correct data type is not entered the data entry clerk will be alerted to this when they move to the next field.

KPMG

Observations and Recommendations (cont)

◆ **Observation #3:** *(Continued)*

If the DMR amount is greater than the permit amount allowed, a warning screen informs the data entry clerk that the amount exceeds the limit. At this point the data entry clerk will then review the input and if a correction is needed will make the correction and if nothing is required will continue with data entry.

KPMG

Observations and Recommendations (cont)

◆ **Observation #4:**

End users can override the ICIS-NPDES Significant Non-Compliance (SNC) data field without additional access controls. There are compensating detective controls, such as audit trails that document who changed the SNC field, however, these are only effective if the audit logs are actively reviewed on a regular basis.

Management has not fully implemented database security features to restrict access to this field to authorized users. ICIS-NPDES also does not have any business rules to prevent this from happening.

KPMG

Observations and Recommendations (cont)

◆ **Observation #4:** *(Continued)*

The lack of a preventative control around the SNC data field allows users to change original data without authorization that could directly impact the data quality of this element in ICIS-NPDES which are then passed onto Integrated Data for Enforcement Analysis (IDEA) and ECHO.

◆ **Recommendation: The Director, Office of Compliance should:**

1. Implement ICIS database security features to limit the end users' ability to change the SNC code.

KPMG