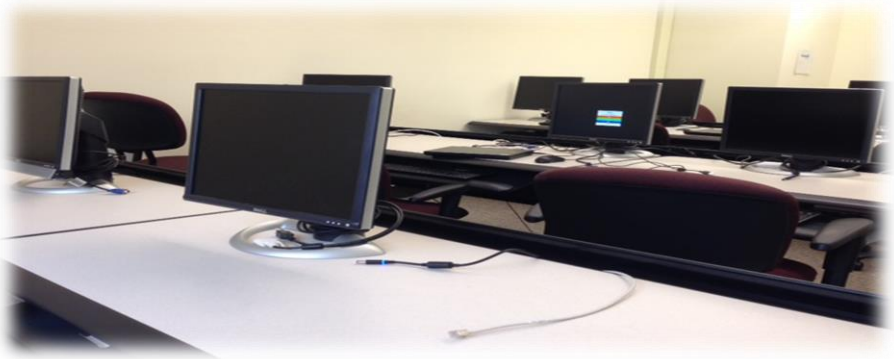
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

EPA Can Better Assure Continued Operations at National Computer Center Through Complete and Up-to-Date Documentation for Contingency Planning

Report No. 15-P-0136 **April 9, 2015**



Scan this mobile code to learn more about the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Neven Soliman

Abbreviations

BIA	Business Impact Analysis
DRP	Disaster Recovery Plan
EPA	U.S. Environmental Protection Agency
ISCP	Information Security Contingency Plan
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SP	Special Publication

Cover photo: Computers on the EPA's network. (EPA OIG photo)

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

More information at www.epa.gov/oig/hotline.html.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

15-P-0136
April 9, 2015

At a Glance

Why We Did This Review

We sought to determine whether the U.S. Environmental Protection Agency (EPA) established an enterprisewide business continuity/disaster recovery program that is consistent with federal requirements.

Information systems play a critical part in the EPA mission and business processes. As such, it is important that these systems operate effectively without excessive interruption. EPA's National Computer Center (NCC) provides the computing and data management support for a significant portion of the agency's administrative, programmatic and scientific applications. When a service interruption occurs, it is essential that the NCC efficiently restores critical applications important to helping the EPA achieve its mission to protect human health and the environment.

This report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

The full report is at: www.epa.gov/oig/reports/2015/20150409-15-P-0136.pdf

EPA Can Better Assure Continued Operations at National Computer Center Through Complete and Up-to-Date Documentation for Contingency Planning

What We Found

Timely recovery of NCC operations from a disaster may be hindered by the lack of documented information needed for the full functioning of all NCC operations.

We found that key NCC and information security system contingency planning documents were either not up to date or did not exist. These documents should contain the detailed guidance and procedures necessary for restoring a damaged system. Three NCC contingency plans had several required elements missing. The latest version of the NCC Disaster Recovery Plan was missing telephone numbers for some points of contact and had incorrect telephone numbers for others. In addition, we found that a contingency plan with recovery information specific to a system that maintains data on emergency equipment availability did not exist.

NCC has not made it a priority to put into place a process to keep its information security system contingency planning documents current. NCC has also not established processes to alert management that the Business Impact Analysis is outdated. Also, owners of a sampled application had not created a contingency plan that contains recovery information specific to the system. Without up-to-date contingency planning documents, NCC cannot identify and prioritize information systems and components critical for supporting the organization's mission and business processes, which could affect NCC's ability to respond timely and effectively to an unforeseen disaster.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Environmental Information develop and implement a process to keep the center's information security contingency planning documents current, update and communicate the status of the Business Impact Analysis that identifies and prioritizes information systems and components critical to supporting the EPA's mission, and develop and implement a process to ensure that all contact information for disaster recovery teams is kept up to date.

We also recommend that the Assistant Administrator for Solid Waste and Emergency Response develop a contingency plan for the Emergency Management Portal system that identifies system-specific recovery strategies.

The recommendation addressees agreed to take sufficient corrective action for all recommendations.

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

THE INSPECTOR GENERAL

April 9, 2015

MEMORANDUM

SUBJECT: EPA Can Better Assure Continued Operations at National Computer Center Through Complete and Up-to-Date Documentation for Contingency Planning
Report No. 15-P-0136

FROM: Arthur A. Elkins Jr.

TO: Ann Dunkin, Chief Information Officer
Office of Environmental Information

Mathy Stanislaus, Assistant Administrator
Office of Solid Waste and Emergency Response

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG 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.

The offices responsible for implementing this audit report's recommendations are the National Computer Center within the Office of Environmental Information and the Office of Emergency Management within the Office of Solid Waste and Emergency Response.

Action Required

In accordance with EPA Manual 2750, the offices provided acceptable and complete planned corrective actions in response to OIG recommendations. All recommendations are resolved and no final response to this report is therefore required.

We will post this report to our website at http://www.epa.gov/oig.

Table of Contents

Appendices

Purpose

We sought to determine whether the U.S. Environmental Protection Agency (EPA) established an enterprisewide business continuity/disaster recovery program that is consistent with the Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology (NIST) guidelines.

Background

Due to the criticality of information systems to the success of the EPA's mission and business processes, it is important that these systems 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.

This audit focused on the information security contingency planning efforts of the EPA's National Computer Center (NCC), which provides the computing and data management support for a significant portion of the agency's administrative, programmatic and scientific applications. Many of these applications are critical in supporting management decisions in support of EPA's mission. As such, being able to efficiently recovery operations when a disaster happens is essential to providing information systems that supports EPA's decision-making capabilities important in protecting human health and the environment.

To assist federal agencies in implementing federal mandated information system security controls, which includes contingency planning, NIST develops publications that are designed to help agencies cost-effectively implement mandated information system security requirements. In particular, NIST Special Publication (SP) 800-53, dated April 2013, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* provides a listing of security controls necessary for organizations to strengthen their information systems and the environments in which those systems operate. Among those controls are the contingency planning controls that specify the need for organizations to develop a contingency plan and what needs to be included.

NIST also published SP 800-34, dated May 2010, Revision 1, *Contingency Planning Guide for Federal Information Systems,* defines the types of contingency plans for organizations and states:

> Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, an organization would use a suite of plans to properly prepare response, recovery,

and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel, and the facility.

EPA also published guidance to help program and regional offices meet mandated contingency planning requirements. EPA Policy CIO 2150.3, *EPA Information Security Policy*, and EPA Procedure CIO-2150.3.P-06.1, *EPA Information Security - Interim Contingency Planning Procedures*, issued August 2012, covers contingency planning requirements for the EPA. The procedure identifies the required elements of the EPA contingency planning program. It also assigns specific roles and responsibilities to EPA system owners with regard to contingency plans for their assigned system. System owners are to ensure the contingency plan is developed, reviewed and updated annually.

System owners are to ensure that the contingency plan[1] is properly implemented and conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support exists during crisis situations.

Responsible Offices

The offices responsible for implementing this audit report's recommendations are the NCC, which is within the Office of Technology Operations and Planning under the Office of Environmental Information; and the Office of Emergency Management within the Office of Solid Waste and Emergency Response. However, during the course of this audit, we selected applications as part of our sample that fell under the purview of the Office of the Chief Financial Officer, Office of Administration and Resources Management, and the Office of Air and Radiation. This report's recommendations are only applicable to the Office of Environmental Information and the Office of Solid Waste and Emergency Response.

The Office of Technology Operations and Planning is the agency focal point for policy, management and implementation of EPA's information technology infrastructure; and oversight of federal and agency information technology statutes, regulations and standards. NCC is responsible for providing support to information technology professionals who use the services offered by the Office of Technology Operations and Planning. NCC has overall responsibility, including managing application deployment, maintenance and enhancements; and providing continuity of operations support and disaster recovery for applications and NCC infrastructure.

The Office of Emergency Management, as the system owner of one of the audited systems, is responsible for designating the System Sponsor, System Owner, System Manager, and Project Manager to support the software lifecycle

[1] The contingency plan, also known as a disaster recovery plan, contains detailed guidance and procedures for restoring a damaged system unique to the impacted system.

management process. The office must create documentation and/or artifacts required for each software lifecycle phase and then update them throughout the system's life cycle.

Scope and Methodology

We performed this audit from March 2014 to January 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our work to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We obtained the following three NCC Information Security Contingency Plan (ISCP) documents for major components of NCC's infrastructure and evaluated them for compliance against NIST and agency criteria:

- NCC Enterprise Server Contingency Plan.
- NCC Hosting System Contingency Plan.
- EPA Wide Area Network Contingency Plan.

We also judgmentally selected and evaluated a sample of three systems during this review:

Table 1: Systems reviewed

System	Responsible EPA offices
Emergency Management Portal	Office of Solid Waste and Emergency Response
*PeoplePlus	Office of the Chief Financial Officer and Office of Administration and Resources Management
*Clean Air Markets Division Business System	Office of Air and Radiation

* System supported by NCC's Disaster Recovery Services.

Source: OIG-compiled data.

We requested and evaluated any contingency planning documents given for the three systems to determine compliance with NIST and agency criteria. We also requested the NCC's Disaster Recovery Plan (DRP) and evaluated it for compliance with federal and agency contingency planning requirements.

We met with NCC representatives to obtain information, and with several representatives from NCC's five branches to discuss issues identified with regard to the NCC contingency planning documents. We met with system representatives of the three sampled systems to collect additional documentation and obtain clarification regarding their offices' contingency planning practices.

Results of Review

We found that several key NCC and system contingency planning documents either had several missing required elements, lacked complete information, or did not exist. Specifically:

- Three NCC contingency plans did not contain all elements required by NIST and agency guidance.
- The latest version of the NCC DRP was missing telephone numbers for several points of contact and had incorrect telephone numbers for others.
- A contingency plan with recovery information specific to the system did not exist for the Emergency Management Portal system.

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems,* states that, "To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies." The NCC has not made it a priority to put in place a process to keep NCC ISCP documents current. The current and only existing NCC Business Impact Analysis (BIA)[2] relied on for NCC's ISCP was 8 years old, and NCC had not established processes to alert management that the BIA is out of date. Without up-to-date contingency planning documents, NCC cannot identify and prioritize information systems and components critical for supporting its mission and business processes. Ultimately, this could affect NCC's ability to respond timely and effectively to a disaster.

NCC Contingency Planning Documents Were Missing Several Required Elements

Applications contingency planning documents for major infrastructure components at NCC were missing several critical elements required by federal and EPA criteria. We compared the content of the three ISCPs for compliance with requirements outlined in both EPA and NIST guidance. Our analysis disclosed that the ISCPs lacked:

- A BIA for two of the three ISCPs, and an updated one for the third.
- An exercise and testing schedule for each of the three ISCPs.
- Preventive controls.
- Costs associated with the recovery strategies.
- Detailed information on annual contingency plan reviews done.
- Distribution information.
- Tracking of weaknesses via a Plan of Actions and Milestones.

[2] The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes.

We met with NCC representatives to discuss the missing elements and provided a listing of those missing elements as a follow-up to our meeting. In response, the NCC representatives indicated that they will update all ISCPs in accordance with applicable requirements, and provided us an updated ISCP. Upon further review, we noted the updated ISCP was still missing required information on how to maintain mission and business functions, and an updated BIA. Additionally, the only BIA included for all three ISCPs was 8 years old. The NCC was responsible for maintaining the BIA. However, the NCC had neither made it a priority to put into place a process to keep its BIA current, nor put into place processes to alert management of hosted applications that the BIA is close to 8 years old.

Without up-to-date contingency planning documents, the NCC cannot identify and prioritize information systems and components critical for supporting the organization's mission and business processes. A current BIA is essential to helping the agency prioritize its resources and reduce redundancies in the contingency planning process.

NCC DRP Contains Incomplete and Outdated Contact Information

We found that telephone numbers for several points of contact listed in the latest version of the NCC DRP, dated April 2013, were either not correct or were missing. Appendix B of the plan contained telephone directories of disaster recovery teams, services and vendors. We selected a sample of 10 contacts out of a population of 296 contacts. Upon calling the contact numbers—which included work, home and cell phone numbers—we found that five of the 10 contacts' numbers were disconnected, belonged to someone else, or was a fax number. One of the five contacts indicated that she has not been with the EPA since 2011. Our analysis also disclosed that 10.5 percent (31) of the 296 contacts had no afterhours contact phone number and, in some cases, no contact numbers at all.

According to NIST 800-34, "A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency." The NCC DRP provided states that "the disaster recovery plan will be kept current and stored in multiple off-site locations at all times." However, The NCC has not put into place a process to ensure contact information listed in the DRP for DRP personnel was kept up-to-date.

Having incorrect and missing personnel contact information in the NCC's DRP can hinder the NCC's ability to address any unforeseen disaster because NCC may not be able to reach trained disaster recovery team members needed to aid in recovery operations.

System-Specific Contingency Planning Document Did Not Exist for a Critical System

The EPA's Office of Emergency Management—within the Office of Solid Waste and Emergency Response—did not create a contingency plan with recovery information specific to the Emergency Management Portal system. According to NIST 800-34, "The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements."

EPA indicated that PeoplePlus and the Clean Air Markets Division Business System subscribed to the NCC's disaster recovery services and, therefore, we consider these two systems to have sufficient contingency planning documents in place. However, when we requested contingency planning documentation for the Emergency Management Portal system that is not supported by NCC's disaster recovery services, the Office of Emergency Management provided us a generic template ISCP. This ISCP template is used by applications hosted at the NCC. However, upon review, we discovered that the Office of Emergency Management did not complete the template and the template did not contain recovery information specifically related to the Emergency Management Portal system. The lack of thorough recovery strategies for the Emergency Management Portal system hinders the EPA's ability to ensure that the system may be recovered quickly and effectively following a disruption, especially when the system houses data on the availability of emergency equipment.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

1. Develop and implement a process to keep the center's ISCP documents current.

2. Update the center's BIA and communicate with management on the status of this document on a continuous basis.

3. Develop and implement a process to ensure that all contact information for disaster recovery teams within the center's DRP is kept up to date.

We recommend that the Assistant Administrator for Solid Waste and Emergency Response:

4. Develop and implement a contingency plan for the Emergency Management Portal system that identifies system-specific recovery strategies.

Agency Comments and OIG Evaluation

NCC and the Office of Emergency Management concurred with our report and recommendations. Management provided estimated dates when they would take corrective action to complete each recommendation. We consider these recommendations resolved with corrective actions pending.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	**Page No.**	**Subject**	**Status[1]**	**Action Official**	**Planned Completion Date**	**Claimed Amount**	**Agreed-To Amount**
1	6	Develop and implement a process to keep the center's ISCP documents current.	O	Assistant Administrator for Environmental Information	9/30/15		
2	6	Update the center's BIA and communicate with management on the status of this document on a continuous basis.	O	Assistant Administrator for Environmental Information	9/30/15		
3	6	Develop and implement a process to ensure that all contact information for disaster recovery teams within the center's DRP is kept up to date.	O	Assistant Administrator for Environmental Information	6/30/15		
4	6	Develop and implement a contingency plan for the Emergency Management Portal system that identifies system-specific recovery strategies.	O	Assistant Administrator for Solid Waste and Emergency Response	12/31/15		

[1] O = Recommendation is open with agreed-to corrective actions pending.
C = Recommendation is closed with all agreed-to actions completed.
U = Recommendation is unresolved with resolution efforts in progress.

Response From Office of Environmental Information

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
REASEARCH TRAINGLE PARK, NC 27711

OFFICE OF
ENVIRONMENTAL INFORMATION

February 19, 2015

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY14-0135, "Disaster Contingency Planning Documents for EPA's National Computer Center and Select Applications Need to Be Updated Regularly," dated January 29, 2015

FROM: Tim Thorpe, Acting Director
National Computer Center
Office of Technology Operations and Planning

TO: Rudolph M. Brevard, Director
Information Resources Management Audits
Office of Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Following is a summary of my overall position, along with my position on each of the report recommendations for which my Division has the lead.

For those report recommendations with which I agree, I have provided either high-level intended corrective actions and estimated completion dates to the extent I can or reasons why I am unable to provide high-level intended corrective actions and estimated completion dates at this time. For those report recommendations with which I do not agree, I have explained my position, and proposed alternatives to recommendations.

OTOP/NCC OVERALL POSITION

NCC concurs with the three recommendations affecting resources under its purview. NCC does, however, note this observation regarding the finding for the NCC DRP. NCC believes that maintaining 100% accuracy for a contact population of 296 individual contributors is an untenable and impractical requirement, given the constant shift in personnel, roles and

responsibilities. As such, NCC intends to re-fresh this contact listing to focus on the key functional leadership and decision-makers that are necessary to initially respond and participate in a disaster event.

OTOP/NCC RESPONSE TO REPORT RECOMMENDATIONS

Agreements

No.	Recommendation	High Level Intended Corrective Action	Estimated Completion Date
1	Direct the NCC to develop and implement a process to keep the center's ISCP documents current.	OTOP/NCC will: • Practice and review its ISCP documents on an annual basis, per NIST SP 800-53 Rev. 4. • ISCP documents will be updated yearly or as required by any changes and/or results from practice exercises. • Artifacts and documentation updates will be included in Xacta following completion of the practice exercises.	4th quarter FY15
2	Direct the NCC to update the center's BIA and communicate with management on the status of this document on a continuous basis.	OTOP/NCC will: • Update its BIA(s) as informed by NIST SP 800-34 Rev. 1 and notify stakeholders of changes. • Include a separate BIA for each of its General Support Systems as part of each ISCP. • Identify necessary changes and update yearly as required following yearly ISCP practice exercises.	4th quarter FY15

3	Direct the NCC to develop and implement a process to ensure that all contact information for disaster recovery teams within the center's DRP is kept up to date.	OTOP/NCC will: • Re-assess the granularity of reach-back requirements during a disaster event to identify critical functional leadership and oversight • Update the DRP Personnel Contact page as a result of the above assessment. • Review the DRP Personnel Contact page on a quarterly basis, to include sampling tests to confirm accuracy. The complete contact list will be confirmed each year.	3rd quarter FY15

CONTACT INFORMATION

If you have any questions regarding this response, please contact me at (919) 541-0613 or John Gibson (919) 541-0112.

cc: Iesha Alexander, Acting OTOP Audit Coordinator
Wayne Eason, Acting Associate Director, NCC
John Gibson, Chief, Security & Business Management Branch

Appendix B

Response From Office of Solid Waste and Emergency Response

February 25, 2015

MEMORANDUM

SUBJECT: Response to "Discussion Draft Report: Disaster Contingency Planning Documents for EPA's National Computer Center and Select Applications Need to Be Updated Regularly (Project No OA-FY14-0135)"

FROM: Reggie Cheatham, Acting Director
Office of Emergency Management

TO: Rudy Brevard
Director, IRM Audits
Office of Inspector General

This memorandum is in response to the *Discussion Draft Report: Disaster Contingency Planning Documents for EPA's National Computer Center and Select Applications Need to Be Updated Regularly (Project No OA-FY14-0135*) issued on January 29, 2015, by the Office of the Inspector General (OIG). We appreciate OIG's assessment and are committed to taking timely corrective action.

The Report states: "Emergency Management Portal system owners have not created a process for creating a contingency plan that contains recovery information specific to the system that would be used in the recovery of the system during any unforeseen disruption. The lack of thorough recovery strategies for the Emergency Management Portal system hinders the EPA's ability to ensure that the system may be recovered quickly and effectively following a disruption, especially when the system houses data on the availability of emergency equipment."

To address this situation, the report recommend that EPA's Assistant Administrator for Solid Waste and Emergency Response:

- Direct the system owners of the agency's Emergency Management Portal to develop a contingency plan for the portal's system that identifies system-specific recovery strategies.

Based on the Report, OSWER/OEM will take the following actions:

1. Develop a system-specific ISCP plan for the Emergency Management Portal as required by NIST 800-34 Revision 1; EPA Policy CIO 2150.3; and EPA Procedure CIO-2150.3.P-06.1 in the EPA-approved template.
2. Practice and review its ISCP document(s) on an annual basis, per NIST SP 800-53 Rev. 4.

3. Update the ISCP document(s) yearly as required by any changes and/or results from risk analyses or practice exercises.
4. Include artifacts and documentation updates in Xacta.

The completion/compliance date for these actions will be 1st Quarter FY 2016 (Dec 31, 2015.)

We share the OIG concerns and will work to ensure that the identified issues are addressed as quickly as possible. Should you have any questions or concerns regarding this response, please contact the OECA Audit Liaison, Gwendolyn Spriggs, at 202-564-2439.

Cc: Rudolph M. Brevard, OIG
Barry Breen, OSWER
Mathy Stanislaus, OEM
Dana Tulis, OSWER/OEM
Victoria VanRoden, OSWER/OEM
Lynn Beasley, OSWER/OEM

Appendix C

Distribution

Office of the Administrator
Chief Information Officer, Office of Environmental Information
Assistant Administrator for Solid Waste and Emergency Response
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal Deputy Assistant Administrator for Environmental Information
Principal Deputy Assistant Administrator for Solid Waste and Emergency Response
Director, Office of Technology Operations and Planning, Office of Environmental Information
Director, National Computer Center, Office of Environmental Information
Director, Office of Emergency Management, Office of Solid Waste and Emergency Response
Senior Agency Information Security Officer, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Solid Waste and Emergency Response