UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

FINAL REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT: UNAUTHORIZED ACCESS TO MULTIPLE EPA SERVERS (LAS VEGAS) OCI-AR-2011-CAC-2772

TABLE OF CONTENTS

Distribution:
File

Approvals:

[redacted]
Senior Special Agent
Electronic Crimes Division

[redacted]
Special Agent in Charge
Electronic Crimes Division

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2011-CAC-2772	**DATE OPENED:**	3/25/2011
CASE TITLE:	UNKNOWN SUBJECT: UNAUTHORIZED ACCESS TO MULTIPLE EPA SERVERS (LAS VEGAS)	**CASE AGENT:**	[redacted]
CASE CATEGORY:	COMPUTER INTRUSION	**OFFICE:**	OFFICE OF INVESTIGATIONS ELECTRONIC CRIMES DIVISION
JOINT AGENCIES:	None		
JURISDICTION:	NEVADA		

SECTION A - NARRATIVE

Predication

This investigation was opened on March, 25, 2011, The Office of Cyber Investigations and Homeland Security (OCI) received notification that suspicious network logins to EPA financial payment systems were occurring on several servers in Las Vegas, Nevada. The systems included in the reported suspicious activity were [redacted]

Possible violations:

1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

Impact/Dollar Loss

This incident had the potential to impact all EPA financial systems and the physical security of environmental incident response and research facilities.

Synopsis

The investigation failed to determine the source of the unauthorized user account activity identified in the Las Vegas Finance center computer systems. Anomalies found in the system logs by EPA IT administrators compared with other available data failed to uncover the source or cause of the activity.

Forensic analysis of data available discovered an unidentified encrypted file that was unable to be opened for further analysis.

Details

Allegations: Violation of TITLE 18 United States Code Section 1030(a)-(4), Fraud and related activity in connection with computers, exceeding authorized access by a detailed Public Health Service employee

Allegations Findings: Investigation was unable to substantiate the allegation. No conclusive evidence of criminal activity could be determined.

Disposition

Due to the lack of conclusive evidence of criminal activity, no referral for prosecution or any course of legal action was made.

SECTION B – ENTITIES AND INDIVIDUALS

Name of Person: Unknown
Title & Company:
Role: Subject
Business Address:
Business Phone:
EPA Employee: N

SECTION C – PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): NONE

EXHIBITS

DESCRIPTION	EXHIBIT
Memorandum of Activity for Imaging, Dated February 3, 2011	1
Memorandum of Interview for [redacted], Dated February 4, 2011	2
Memorandum of Activity for Network Monitoring, Dated February 5, 2011	3
Memorandum of Activity for Imaging, Dated February 5, 2011	4
Memorandum of Interview for [redacted] Dated September 21, 2011	5