



**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(S) – UNAUTHORIZED EPA LAN ACCESS
OCI-AR-2012-CAC-0014**

TABLE OF CONTENTS

Narrative	Section A
Entities and Individuals	Section B
Prosecutive Status	Section C
Exhibits	

Distribution:


File

Approvals:

Special Agent

Special Agent in Charge

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.: OCI-AR-2012-CAC-0014 **DATE OPENED:** 11/01/2011

CASE TITLE: UNKNOWN SUBJECT(S) **CASE AGENT:** [REDACTED]
 – UNAUTHORIZED EPA
 LAN ACCESS

CASE CATEGORY: COMPUTER INTRUSION **OFFICE:** OFFICE OF INVESTIGATIONS

JOINT AGENCIES: None

JURISDICTION: DISTRICT OF COLUMBIA

SECTION A - NARRATIVE

Predication

This investigation was opened on November 1, 2011, based on the notification by [REDACTED] Security Management Division, EPA, Washington, DC, of a security violation concerning EPA’s Local Area Network committed by unknown person(s). According to [REDACTED] SMD was notified that unknown individual(s) were accessing EPA’s LAN allegedly with a personal computer. The access was occurring in the EPA East and Ariel Rios North Buildings, Washington, DC [REDACTED] related there have been at least six times the EPA LAN had been accessed so far.

Possible violations:

1. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

Impact/Dollar Loss

The impact of this incident represents a compromise of the command and control of EPA systems and the EPA network.

Synopsis

On November 1, 2011, [REDACTED], Security Management Division, EPA, Washington, DC reported a security violation concerning EPA’s Local Area Network (LAN) committed by unknown person(s). According to [REDACTED], SMD was notified that unknown individual(s) were accessing EPA’s LAN allegedly with a personal computer. The

access was occurring in the EPA East and Ariel Rios North Buildings, Washington, DC. [REDACTED] related there have been at least six times the EPA LAN had been accessed so far.

Although the allegations were substantiated as unauthorized access was documented in EPA's LAN records, the investigation was unable to positively identify the individual(s) who gained access to the EPA data networks through physical means to steal/maintain access to EPA internet resources.

[REDACTED]

Details

Allegation 1: 18 USC 1029 Fraud and related activity in connection with access devices.

Findings: Unknown individual(s), without proper authorization, gained access to the EPA physical LAN closets networks and utilized network resources.

Disposition

Investigation failed to identify the individual(s) who gained access to the EPA's network. No referral for prosecution 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

<u>DESCRIPTION</u>	<u>EXHIBIT</u>
MOI Interview of [REDACTED], August 24, 2011	1
MOI Interview of [REDACTED], September 6, 2011	2
MOI Interview of [REDACTED], October 28, 2011	3
MOA Review of Security Logs, February 9, 2012	4
MOA Attempt to contact [REDACTED], May, 30 2013	5