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: INTRUSIONINTO MULTIPLE WORKSTATIONS [redacted] AND [redacted]

OCI-RTP-2012-CAC-0062

TABLE OF CONTENTS

Distribution:
[redacted]
SAC
File

Approvals:

_____
Special Agent

_____
Special Agent in Charge

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2012-CAC-0062	**DATE OPENED:**	02/24/2012
CASE TITLE:	UNKNOWN SUBJECT: INTRUSIONINTO MULTIPLE WORKSTATIONS [redacted]	**CASE AGENT:**	[redacted]
CASE CATEGORY:	COMPUTER INTRUSION	**OFFICE:**	OFFICE OF CYBER INVESTIGATIONS AND HOMELAND SECURITY - IMMEDIATE OFFICE
JOINT AGENCIES:	Federal Bureau of Investigation		
JURISDICTION:	N/A		

SECTION A - NARRATIVE

Predication

On February 16, 2012, Special Agent [redacted], United States Environment Protection Agency, Office of Inspector General, Office of Investigations, Region 4, Research Triangle Park field office, received a complaint from [redacted] Office of Technology Operations and Planning, and Technology Information Security Staff, [redacted], pertaining to an intrusion of the Office of the Administrator, [redacted] computer, and the Office of Air and Radiation, [redacted] computer.

Possible violations:

1. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices
2. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

Impact/Dollar Loss

This incident impacted the security and stability of the EPA local area network and EPA Senior Level administration operations.

Synopsis

On February 16, 2012, Special Agent [redacted] United States Environment Protection Agency, Office of Inspector General, Office of Investigations, Region [redacted] field office, received a complaint from [redacted] Office of Technology Operations and Planning, and Technology Information Security Staff, [redacted], pertaining to an intrusion of the Office of the Administrator, [redacted] computer, and the Office of Air and Radiation, [redacted] computer. (Exhibit 1)

On February 20, 2012 [redacted], OCI coordinated with the Cyber division of the Federal Bureau of Investigation who offered to assist with any information they had related to the intrusion but declined to join this investigation.

On February 22, 2012 analysis was completed [redacted] malware recovered from the intrusion incident by the CSIRC. Analysis showed the malware was fairly common and targeted a wide audience of recipients. (Exhibit 2)

On January 30, 2013 [redacted], OCI, interviewed [redacted] and discussed [redacted] position and activities in OA. [redacted] was unsure how [redacted] system had been compromised or why [redacted] would have been targeted. (Exhibit 3)

Details

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

Findings: On February 16, 2012, TISS reported EPA systems [redacted] no damage was discovered to the EPA network. No additional information was available to identify the intruders.

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connectiou with computers.

Findings: On February 16, 2012, TISS reported [redacted] no damage was discovered to the EPA network. No additional information was available to identify the intruders.

Disposition

Investigation was not able to determine the identity of the intruders. A referral for prosecution was not 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
Case Initiation	1
MOA Malware Analysis	2
MOI Interview of [redacted]	3