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

BREACH OF REGION[redacted] SERVER
OCI-AR-2012-CAC-0147

TABLE OF CONTENTS

Distribution:
File

Submitted By:

[redacted]
Special Agent
Electronic Crimes Division
Office of Investigations

Approved By:

[redacted]
Special Agent in Charge
Electronic Crimes Division
Office of Investigations

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2012-CAC-0147	**DATE OPENED:**	07/25/2012
CASE TITLE:	BREACH OF REGION [redacted] SERVER	**LAST UPDATED:**	
CASE CATEGORY:	COMPUTER INTRUSION	**CASE AGENT:**	[redacted]
JOINT AGENCIES:	None	**OFFICE:**	ECD

JURISDICTION: [redacted]

SECTION A - NARRATIVE

Predication

An investigation was opened on July 25, 2012, based on information received from the Environmental Protection Agency, Computer Security Incident Response Center, Research Triangle Park, North Carolina. The investigation was initiated as a result of an EPA Information Security Officer reporting a breach of security resulting in unauthorized changes being made to a Region [redacted] server.

Possible violations:

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

Impact/Dollar Loss

No Dollar loss was sustained by the Government.

There were no significant impacts to EPA systems, programs, or processes.

Synopsis

On March 6, 2012, [redacted], CSIRC, Office of Environmental Information, EPA, Research Triangle Park, North Carolina, notified [redacted], EPA, Office of Inspector General, Office of Investigations, Electronic Crimes Division, of the possible breach of an EPA Region [redacted] server by an unidentified person. Specifically, the breach consisted of unauthorized changes being made to the Region [redacted] server.

This investigation disclosed the allegations were proven. Investigative activities found there were, in fact, changes made to the server's desktop background. However, the investigation found no criminal activity or malicious intent related to this incident.

Details

Allegation: Violation of TITLE 18 United States Code Section 1030(a)(5), Fraud and related activity in connection with computers.

On March 9, 2012, [redacted] and [redacted], EPA, OIG, OI, Denver Field Office, interviewed [redacted] EPA, Region [redacted] Technical Services Unit, [redacted] verified the details of the allegation regarding the suspected breach of the server in question. They confirmed unauthorized changes were made to a virtual server image which was used to image employee computers in the Region. [redacted] stated [redacted] the last known good deployment of the image from this server sometime around noon on March 5, 2012. Based on this, [redacted] believed the compromise occurred sometime after 1 p.m. on March 5, 2012.

[redacted] stated [redacted] discovered that when attempting to load an image from the virtual server to a local computer, a background image was displayed during the boot loader process. This image depicted a cartoon [redacted] Normally, the Microsoft logo would be displayed during this process.

[redacted] opined, after considering the totality of the circumstances involved, it would be a "virtual impossibility" that the server image was compromised from outside of EPA. [redacted] conducted a review of the server's access authorities and discovered [redacted] contractors, [redacted] Silver Spring, Maryland, had user rights to the database. A review of the server's internal logs by [redacted] disclosed that [redacted] along with [redacted] contractors, [redacted] were active on the system during the time of the incident. Based on this review, [redacted] stated [redacted] specifically suspected [redacted] was responsible for the change made to the server. [redacted] was unable to say definitively from [redacted] examination of the logs that [redacted] was involved with the incident; only that [redacted] had a "gut-feeling." [redacted] offered no other support for this conclusion. (EXHIBIT 1)

On January, 29, 2013, [redacted], EPA, OIG, OI, ECD, conducted an interview of [redacted], contractor, [redacted] stated [redacted] is the [redacted] for the contract responsible for supporting the Region [redacted] Technical Services Unit. During February or March 2012, [redacted] and [redacted] of contractors were tasked with creating a Microsoft Deployment Toolkit (MDT) server which was to be used to deploy Windows 7 operating systems to customers located in Region [redacted] team, responsible for building and testing the server, consisted of [redacted], [redacted]. [redacted] stated the individuals on [redacted] team were the only persons with initial access to the server. However, during March 2012, [redacted] and [redacted]

provided their EPA government employee counterparts with a demonstration of the server's capabilities. Shortly after the demonstration (NFI), the following EPA government employees requested and were granted access to the server: [redacted] Information Technology Specialists, EPA, Region [redacted], and [redacted] stated, to the best of [redacted] recollection, a "day or two" after the EPA government employees were granted access to the server, a change was made to the servers background. [redacted] could not recall what changes were made to the server; however, [redacted] did recall there were no significant impacts to operations and opined no one [redacted] was responsible. (EXHIBIT 2)

On January 29, 2013, [redacted] conducted an interview of [redacted] recalled [redacted] being tasked to create a MDT server which would be used in deploying Windows 7 operating system images to Region [redacted] customers. [redacted] stated [redacted] did not have the same level of involvement during this project as others on [redacted] did. [redacted] relayed [redacted] and [redacted] were the main team members to develop and use the MDT server. [redacted] further stated two government employees, [redacted] and [redacted] also had access to the server. [redacted] opined the [redacted] individuals most likely to make the changes to the server were [redacted] due to their sense of humor. However, [redacted] could not definitively say who had made the changes to the server. (EXHIBIT 3)

On January 29, 2013, [redacted] conducted an interview of [redacted] recalled that sometime in March 2012 [redacted] tasked the contracting team with developing a new MDT server. [redacted] stated [redacted] discussed this project with [redacted] who then set up access to the server. Initially, the contractors were the only individuals with access to the server. [redacted] stated during this time, [redacted] had changed the background on the server to depict a cartoon image [redacted] Shortly after this change was made, the government requested access to the server. Because government employees requested access, [redacted] removed the cartoon image on the server and restored the original background.

A couple of weeks after the government employees received access to the MDT server, [redacted] noticed the background on the server was changed to a cartoon image [redacted] Upon noticing the change, [redacted] called [redacted] and asked if [redacted] had made a change to the server; [redacted] replied "no."

[redacted] stated multiple government employees had access to the server and they utilized the same username, [redacted] and password so there was no way to determine exactly which government employees had access to the server.

In addition, [redacted] stated [redacted] believed [redacted] may have made the changes to the server and is now trying to place the blame on [redacted] [redacted] stated [redacted] has "a problem" with [redacted] doesn't do things the way [redacted] wants. (EXHIBIT 4)

On January 29, 2013, [redacted] conducted an interview of [redacted] stated, during February or March of 2012, a team of contractors with [redacted] Inc., set up a MDT server in order to push images to Region [redacted] customers. [redacted] stated

[redacted] and [redacted] other contractors (NFI) knew how to use the MDT server and were very familiar with the system. [redacted] stated [redacted] built the system and would likely have known how to make changes to the server. [redacted] believed the change made to the server background was nothing more than a joke which had been blown out of proportion. Additionally, [redacted] stated the server in question is not in use anymore because it was only used to deploy Windows XP images, which is no longer used by Region [redacted] Furthermore, [redacted] stated that at the time of the incident [redacted]. contractors were the only individuals with access to the server; however, at some point, government employees were give access to the server. [redacted] believes if anyone would have made the changes to the server it would have been [redacted] (EXHIBIT 5)

On January 30, 2013, [redacted] conducted an interview of [redacted] [redacted] could not recall when [redacted] was made aware of the incident; however, [redacted] stated it was shortly after the incident occurred. [redacted] stated [redacted] did not believe the changes to the server were made intentionally or maliciously. [redacted] believed [redacted] [redacted] contractor, [redacted] [redacted]., would have been the individual most likely to make the changes due to [redacted] humorous nature. Additionally, [redacted] opined the incident was "no big deal" as there was no damage done to the server. (EXHIBIT 6)

On January 30, 2013, [redacted] conducted an interview of [redacted] During February or March 2012, [redacted] was made aware of an incident involving a MDT server. [redacted] stated someone had changed the background of the server. When an IT Specialist would begin imaging machines remotely, an image would pop up in the background. [redacted] stated when this incident occurred the affected server was in a "testing" phase and was not used in live operations. [redacted] stated [redacted] believed there were some configuration changes making the server unable to deploy software.

[redacted] opined the [redacted] contractors most likely made the changes to the server. [redacted] believes this because the contractors initially configured the server and possessed the most knowledge of the server's operational capabilities. Furthermore, [redacted] staff of government employees took over the development and use of the MDT server which may have caused the contractors to feel threatened. (EXHIBIT 7)

On January 30, 2013, [redacted] conducted an interview of [redacted] During February or March 2012, [redacted] was made aware of an incident involving a MDT server. [redacted] recalled receiving a phone call from [redacted] asking if [redacted] made any changes to the MDT server. [redacted] told [redacted] he had not made any changes to the MDT server. [redacted] described the image to [redacted] stated [redacted] believed [redacted] knew what image [redacted] was referring to. [redacted] has changed the background view on the MDT client only [redacted] sees on [redacted] computer; however, it shouldn't have been seen by anyoue else. [redacted] provided [redacted] with a printed image that matched the description of the posting made to the server. [redacted] stated [redacted] remembered using this image as [redacted] background at some point but stated [redacted] never intentionally used this image as a background other users would see. [redacted] stated it is possible [redacted] was logged into the MDT server on [redacted] government issued computer and mistakenly changed the background on the MDT server while intending to make the change to [redacted] personal background view.

[redacted] explained that during the course of [redacted] work [redacted] has multiple processes running on [redacted] government issued computer. [redacted] stated if [redacted] was conducting work on the MDT through the MDT application on [redacted] government issued computer [redacted] could have accidentally changed the background on the MDT application rather than [redacted] desktop. [redacted] maintained this was not intentional. (EXHIBIT 8)

Disposition

This investigation disclosed the allegation was proven; however, no criminal or malicious activities were found to have occurred to intrude upon, breach security within, or compromise EPA systems.

SECTION B – ENTITIES AND INDIVIDUALS

Name: [redacted]
Role: Subject
EPA Employee: N
Business Address: [redacted]
Business Phone: [redacted]

SECTION C – PROSECUTION STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): As there was no criminal activity discovered during this investigation this case was not referred for action.

EXHIBITS

DESCRIPTION	EXHIBIT
MOI-03/09/2012 – [redacted]	1
MOI-01/29/2013 – [redacted]	2
MOI-01/29/2013 – [redacted]	3
MOI-01/29/2013 – [redacted]	4
MOI-01/29/2013 – [redacted]	5
MOI-01/30/2013 – [redacted]	6
MOI-01/30/2013 – [redacted]	7
MOI-01/30/2013 – [redacted]	8