U.S. Department of Energy
Office of Inspector General
Office of Investigations

Investigative Report to Management

I12TC001

January 24, 2012

U.S. Department of Energy
Office of Inspector General
Office of Investigations

January 24, 2012

MEMORANDUM FOR THE CHIEF INFORMATION OFFICER,
NATIONAL NUCLEAR SECURITY ADMINISTRATION

FROM: (b)(6)(b)(7)(C)
Technology Crimes Section

SUBJECT: Investigation of Unauthorized Disclosure of Information by an Employee of the National Nuclear Security Administration (OIG Case No. I12TC001)

This report serves to inform you of the results of an investigation by the U.S. Department of Energy (DOE), Office of Inspector General (OIG), Office of Investigations (Investigations). The investigation involved allegations of unauthorized release of sensitive cyber security information by (b)(6)(b)(7)(C) Incident Assurance Response Center (IARC), National Nuclear Security Administration (NNSA), Las Vegas, NV. Specifically, it was alleged that (b)(6)(b)(7)(C) publicly posted sensitive computer network security information to the Internet from August 3-8, 2011. This information included approximately 4,838 "proprietary intrusion detection signatures" which allow NNSA cyber security to detect known security threats to the Department's unclassified network.

In summary, prior to OIG involvement, an IARC internal investigation (b)(6)(b)(7)(C) found that (b)(6)(b)(7)(C) did publicly post the identified sensitive information, and that conduct was in violation of DOE policy regarding the handling of information classified as "Official Use Only." As a result, (b)(6)(b)(7)(C) the IARC contract by (b)(6)(b)(7)(C) The Assistant United States Attorney for District of Nevada, Las Vegas, NV declined to prosecute (b)(6)(b)(7)(C)

The OIG's subsequent investigation found that the NNSA was in violation of DOE policy regarding proper reporting of cyber incidents of this type. Specifically, DOE Order 205.1B, Department of Energy Cyber Security Program, states that this category of cyber security incident shall be reported to the Department's Joint Cybersecurity Coordination Center (JC3) within 4 hours after learning of an incident.

The NNSA never reported the above cited incident through official channels to the JC3. The JC3 independently learned of the incident through an anonymous source and published an incident report regarding the matter on October 17, 2011, 69 days after the incident was originally identified by the IARC (August 8, 2011).

Additionally and for your information, the OIG is conducting an audit of the Department's incident response management program. The audit report, when completed, will be forwarded to the Department for review.

This report makes 3 recommendations for corrective action related to potential control deficiencies.

For questions or further information regarding this report please contact Special Agent (b)(6)(b)(7)(C) at 202-586-(b)(6)(b)(7)(C)

INVESTIGATIVE REPORT TO MANAGEMENT

I. ALLEGATION

On October 6, 2011 the U.S. Department of Energy (Department), Office of Inspector General (OIG), received an allegation from the DOE Chief Information Security Office, that (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Incident Assurance Response Center (IARC), National Nuclear Security Administration (NNSA) posted approximately 4,838 sensitive computer intrusion detection signatures to a publicly accessible Internet website for a period of six days. According to a report provided by the complainant, this information was discovered by the DOE Computer Security Incident Response Team (CSIRT), Los Alamos National Labs (Los Alamos) on August 8, 2011. The CSIRT reported the incident to the IARC on August 8, 2011.

Additionally, the OIG is conducting an audit of the Department's incident response management program, titled "The Department's Cyber Security Incident Management Program". The audit's purpose is to determine whether the Department has developed and deployed an effective enterprise-wide cyber security incident management program. The audit report, when completed, will be forwarded to the Department for review.

II. POTENTIAL STATUTORY OR REGULATORY VIOLATIONS

The OIG investigation focused on potential violations of reporting and notification procedures regarding cyber security incidents in accordance with DOE Order 205.1B, Department of Energy Cyber Security Program, which states under section 4.(c)(13) that:

> A defined process for incident reporting that requires all cyber security incidents involving information or information systems, including privacy breaches, under DOE or DOE contractor control must be identified, mitigated, categorized, and reported to the DOE Cyber Incident Response Capability (DOE-CIRC and now known as JC3) in accordance with DOE-CIRC procedures and guidance. This document outlines the referenced DOE-CIRC reporting procedures and guidance to facilitate your reporting and CIRC's response activity. CIRC should be informed of all reportable cyber security incidents as specified below. CIRC will work with your site management to determine the severity or significance of any cyber security incident.

Further guidance contained in the order states that:

> Information Compromise is a type 1 low security incident which is defined as: Any unauthorized disclosure of information that is released from control to entities that do not require the information to accomplish an official Government function such as may occur due to inadequate clearing, purging, or destruction of media and related equipment or transmitting information to an unauthorized entity.

The incident in question falls under the category of a type 1 incident. JC3 requires type 1 incidents to be reported to them within 4 hours.

III. INVESTIGATIVE FINDINGS

Summary

The OIG investigation found the NNSA did not follow proper procedure, in accordance with DOE Order 205.1B, requiring the reporting of cyber security incidents to appropriate authorities within a specified timeframe.

Details

Unauthorized Posting of Sensitive Cyber Security Information to a Public Website

(b)(6)(b)(7)(C)
OIG review of an internal NNSA IARC report of investigation regarding the incident in question revealed that sensitive cyber security information in the possession of (b)(6)(b)(7)(C) Incident Assurance Response Center (IARC), National Nuclear Security Administration (NNSA), Las Vegas, NV was uploaded by [redacted] to a commercial Internet cloud storage service known as box[.]net, for a period of approximately 41 days. The sensitive information was in the form of "proprietary intrusion detection signatures" which allow NNSA cyber security to detect known security threats to the Department's unclassified network.

(b)(6)(b)(7)(C)
After uploading these detection signatures to box[.]net, (b)(6)(b)(7)(C) then linked the information to [redacted] publicly available Internet blog for a period of six days. The unauthorized posting of this information to [redacted] personal Internet blog was discovered by the DOE Computer Security Incident Response Team (CSIRT), Los Alamos National Labs (Los Alamos) on August 8, 2011, and subsequently reported by CSIRT to the IARC on the same day.

(b)(6)(b)(7)(C)
Additionally, as part of its internal investigation, IARC assessed (b)(6)(b)(7)(C) box[.]net account and found it to be a personal account accessible only to (b)(6)(b)(7)(C) and protected by a password known only to (b)(6)(b)(7)(C)

Failure to Properly Report a Cyber Security Incident

NNSA never reported the incident in question to the Department's Joint Cybersecurity Coordination Center (JC3). Instead, when the IARC learned of the incident from the CSIRT it reported the matter to NNSA and then conducted its own internal investigation from August 8, 2011 to August 10, 2011. At the end of its internal investigation IARC concluded no compromise, based on public disclosure of the cited information, occurred. It reached this conclusion despite specific regulatory language to the contrary as found in DOE Order 205.1B and as cited earlier in this report. The IARC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) decided not to report the incident to JC3. They briefed (b)(6)(b)(7)(C)

(b)(6)(b)(7)(C) NNSA and (b)(6)(b)(7)(C) concurred with this decision. This position is contrary to the plain language of DOE Order 205.1B.

IV. COORDINATION

The OIG coordinated this matter with Michael Chu, Assistant United States Attorney (AUSA), District of Nevada, Las Vegas, NV. AUSA Chu declined criminal prosecution of (b)(6)(b)(7)(C) in this case.

V. RECOMMENDATIONS

Based on the information in this report, and other information that may be available to you, the OIG recommends that the Office of Chief Information Officer, NNSA:

1. Determine if the IARC has adequate controls in place to ensure compliance with DOE Order 205.1B, Department of Energy Cyber Security Program.

2. Determine if training is necessary regarding proper reporting procedures for incidents involving DOE Order 205.1B, Department of Energy Cyber Security Program.

3. Determine if periodic assessments should be conducted in the future to determine if events are being properly reported.

VI. FOLLOW-UP REQUIREMENTS

Please provide the Office of Inspector General with a written response within 30 days concerning any action(s) taken or anticipated in response to this report.

VII. PRIVACY ACT AND FREEDOM OF INFORMATION ACT NOTICE

This report, including any attachments and information contained therein, is the property of the Office of Inspector General (OIG) and is for ~~OFFICIAL USE ONLY.~~ The original and any copies of the report must be appropriately controlled and maintained. Disclosure to unauthorized persons without prior OIG written approval is strictly prohibited and may subject the disclosing party to liability. Unauthorized persons may include, but are not limited to, individuals referenced in the report, contractors, and individuals outside the Department of Energy. Public disclosure is determined by the Freedom of Information Act (Title 5, U.S.C., Section 552) and the Privacy Act (Title 5, U.S.C., Section 552a).

DOE F 1325.8
(08-93)
United States Government **Department of Energy**

Memorandum

DATE: August 9, 2012

REPLY TO ATTN OF: IG-24 (b)(6)(b)(7)(C) Special Agent)

SUBJECT: Case Closing Recommendation (OIG Case No. I12TC001)

TO: (b)(6)(b)(7)(C) Technology Crimes Section

The purpose of this memorandum is to recommend the closing of OIG Case Number I12TC001.

ALLEGATION

On October 7, 2011, Special Agent (SA (b)(6)(b)(7)(C) Technology Crimes Section (TCS), Office of Inspector General (OIG) Department of Energy (DOE), was notified by (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) National Nuclear Security Administration (NNSA) of the alleged unauthorized disclosure of sensitive network security information by a contractor at the Information Assurance Response Center, NNSA, Las Vegas, NV.

POTENTIAL STATUTORY VIOLATIONS

The investigation focused on a potential criminal violation of Title 18 U.S.C. § 1030; (Fraud and related activity in connection with computers).

INVESTIGATIVE FINDINGS

The investigation did not substantiate allegations of a criminal nature. However, based on investigative findings a DOE OIG Incident Report to Management (IRM) was submitted to Robert Osborn, Chief Information Officer (OCIO), NNSA on January 24, 2012. The IRM made the following three recommendations: 1) Determine if the IARC has adequate controls in place to ensure compliance with DOE order 205.1b, Department of Energy Cyber Security Program; 2) Determine if training is necessary regarding proper reporting procedures for incidents involving DOE order 205.1b, Department of Energy Cyber Security Program; and 3) Determine if periodic assessments should be conducted in the future to determine if events are being properly reported.

On April 9, 2012, a written response was received from the OICO of NNSA. According to the written response, NNSA management concurs with all OIG recommendations. NNSA has requested regular assessments by DOE Office of Health, Safety and Security (HSSs) of the IARC to determine if events are being properly reported and the staff is adhering to Department policies, national standards, accepted practices and procedures. NNSA will request that HSS place special emphasis on OIG findings for the foreseeable future to insure no systematic issues remain.

RECOMMENDATION

This case is being recommended for closure as all prudent investigative measures were taken, the allegation was substantiated and no further investigative activities remain.

Please contact me on 202-586 (b)(6) (b)(7)(C) should you have questions or require further information.

(b)(6)(b)(7)(C)

Special Agent
Technology Crimes Section
Office of Inspector General

Concur:

(b)(6)(b)(7)(C)

Technology Crimes Section
Office of Inspector General

20 Nov 12
Date