



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Nuclear Regulatory Commission (NRC) Inspector General (OIG) investigations closed 2013

Request date: 2014

Released date: 04-August-2014  
Released date: 25-September-2014

Posted date: 08-December-2014

Note: Material released 25-September begins on PDF page 59

Source of document: US Nuclear Regulatory Commission  
Mail Stop T-5 F09  
Washington, DC 20555-0001  
Fax: 301-415-5130  
E-mail: [FOIA.resource@nrc.gov](mailto:FOIA.resource@nrc.gov)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

**RESPONSE TO FREEDOM OF  
INFORMATION ACT (FOIA) / PRIVACY  
ACT (PA) REQUEST**

2014-0329

1

RESPONSE  
TYPE

☐ FINAL

☒ PARTIAL

REQUESTER

DATE

AUG 06 2014

**PART I. -- INFORMATION RELEASED**

- ☐ No additional agency records subject to the request have been located.
- ☐ Requested records are available through another public distribution program. See Comments section.
- ☐  Agency records subject to the request that are identified in the specified group are already available for public inspection and copying at the NRC Public Document Room.
- ☐  Agency records subject to the request that are contained in the specified group are being made available for public inspection and copying at the NRC Public Document Room.
- ☒  Agency records subject to the request are enclosed.
- ☐ Records subject to the request that contain information originated by or of interest to another Federal agency have been referred to that agency (see comments section) for a disclosure determination and direct response to you.
- ☒ We are continuing to process your request.
- ☐ See Comments.

**PART I.A -- FEES**

AMOUNT\*

\$

\* See comments  
for details

☐ You will be billed by NRC for the amount listed.

☐ None. Minimum fee threshold not met.

☐ You will receive a refund for the amount listed.

☐ Fees waived.

**PART I.B -- INFORMATION NOT LOCATED OR WITHHELD FROM DISCLOSURE**

- ☐ No agency records subject to the request have been located. For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.
- ☒ Certain information in the requested records is being withheld from disclosure pursuant to the exemptions described in and for the reasons stated in Part II.
- ☒ This determination may be appealed within 30 days by writing to the FOIA/PA Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001. Clearly state on the envelope and in the letter that it is a "FOIA/PA Appeal."

**PART I.C COMMENTS ( Use attached Comments continuation page if required)**

SIGNATURE ASSISTANT INSPECTOR GENERAL

Joseph McMillan

**RESPONSE TO FREEDOM OF INFORMATION  
ACT (FOIA) / PRIVACY ACT (PA) REQUEST**

DATE

AUG 06 2014

**PART II.A -- APPLICABLE EXEMPTIONS**

GROUP

A

Records subject to the request that are contained in the specified group are being withheld in their entirety or in part under the Exemption No.(s) of the PA and/or the FOIA as indicated below (5 U.S.C. 552a and/or 5 U.S.C. 552(b)).

- ☐ Exemption 1: The withheld information is properly classified pursuant to Executive Order 12958.
- ☐ Exemption 2: The withheld information relates solely to the internal personnel rules and practices of NRC.
- ☐ Exemption 3: The withheld information is specifically exempted from public disclosure by statute indicated.
- ☐ Sections 141-145 of the Atomic Energy Act, which prohibits the disclosure of Restricted Data or Formerly Restricted Data (42 U.S.C. 2161-2165).
- ☐ Section 147 of the Atomic Energy Act, which prohibits the disclosure of Unclassified Safeguards Information (42 U.S.C. 2167).
- ☐ 41 U.S.C., Section 4702(b), prohibits the disclosure of contractor proposals in the possession and control of an executive agency to any person under section 552 of Title 5, U.S.C. (the FOIA), except when incorporated into the contract between the agency and the submitter of the proposal.
- ☐ Exemption 4: The withheld information is a trade secret or commercial or financial information that is being withheld for the reason(s) indicated.
- ☐ The information is considered to be confidential business (proprietary) information.
- ☐ The information is considered to be proprietary because it concerns a licensee's or applicant's physical protection or material control and accounting program for special nuclear material pursuant to 10 CFR 2.390(d)(1).
- ☐ The information was submitted by a foreign source and received in confidence pursuant to 10 CFR 2.390(d)(2).
- ☐ Disclosure will harm an identifiable private or governmental interest.
- ☐ Exemption 5: The withheld information consists of interagency or intraagency records that are not available through discovery during litigation. Applicable privileges:
- ☐ Deliberative process: Disclosure of predecisional information would tend to inhibit the open and frank exchange of ideas essential to the deliberative process. Where records are withheld in their entirety, the facts are inextricably intertwined with the predecisional information. There also are no reasonably segregable factual portions because the release of the facts would permit an indirect inquiry into the predecisional process of the agency.
- ☐ Attorney work-product privilege. (Documents prepared by an attorney in contemplation of litigation)
- ☐ Attorney-client privilege. (Confidential communications between an attorney and his/her client)
- ☐ Exemption 6: The withheld information is exempted from public disclosure because its disclosure would result in a clearly unwarranted invasion of personal privacy.
- ☒ Exemption 7: The withheld information consists of records compiled for law enforcement purposes and is being withheld for the reason(s) indicated.
- ☐ (A) Disclosure could reasonably be expected to interfere with an enforcement proceeding (e.g., it would reveal the scope, direction, and focus of enforcement efforts, and thus could possibly allow recipients to take action to shield potential wrong doing or a violation of NRC requirements from investigators).
- ☒ (C) Disclosure could constitute an unwarranted invasion of personal privacy.
- ☐ (D) The information consists of names of individuals and other information the disclosure of which could reasonably be expected to reveal identities of confidential sources.
- ☒ (E) Disclosure would reveal techniques and procedures for law enforcement investigations or prosecutions, or guidelines that could reasonably be expected to risk circumvention of the law.
- ☒ (F) Disclosure could reasonably be expected to endanger the life or physical safety of an individual.
- ☐ OTHER (Specify)

**PART II.B -- DENYING OFFICIALS**

Pursuant to 10 CFR 9.25(g), 9.25(h), and/or 9.65(b) of the U.S. Nuclear Regulatory Commission regulations, it has been determined that the information withheld is exempt from production or disclosure, and that its production or disclosure is contrary to the public interest. The person responsible for the denial are those officials identified below as denying officials and the FOIA/PA Officer for any denials that may be appealed to the Executive Director for Operations (EDO).

| DENYING OFFICIAL   | TITLE/OFFICE                     | RECORDS DENIED | APPELLATE OFFICIAL       |                          |                                     |
|--------------------|----------------------------------|----------------|--------------------------|--------------------------|-------------------------------------|
|                    |                                  |                | EDO                      | SECY                     | IG                                  |
| Joseph A. McMillan | Assistant Inspector General, OIG |                | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
|                    |                                  |                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            |
|                    |                                  |                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            |

Appeal must be made in writing within 30 days of receipt of this response. Appeals should be mailed to the FOIA/Privacy Act Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, for action by the appropriate appellate official(s). You should clearly state on the envelope and letter that it is a "FOIA/PA Appeal."

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

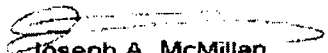


UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

OFFICE OF THE  
INSPECTOR GENERAL

April 17, 2013

MEMORANDUM TO: R. William Borchardt  
Executive Director for Operations

FROM:   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

SUBJECT: LOGON CREDENTIAL HARVESTING USING GOOGLE  
SPREADSHEETS (OIG CASE NO. 11-48)

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), recently completed an investigation regarding a notification that unknown individual(s) sent a phishing e-mail to more than 200 NRC employee's NRC e-mail accounts for the purpose of harvesting NRC network user ID and password (credentials). At least 12 NRC employees clicked on the link in the e-mail. While conducting the investigation, OIG identified 55 people from National Institutes of Health (NIH) who also received the e-mail, clicked on the link and provided their credentials. OIG coordinated this investigation with the Department of Justice (DOJ). This memorandum conveys relevant details from this investigation. There is no need to respond to this office.

**Allegation**

OIG initiated this investigation after being notified by the NRC Computer Security Office (CSO) on June 24, 2011, that an unknown individual(s) sent a phishing e-mail to approximately 215 NRC employees' NRC e-mail accounts for the purpose of harvesting NRC network credentials. The link in the e-mail went to a legitimate Web site,

(b)(7)(F) where a form was set up for users to "validate" their network credentials by entering their username and password, which allows the unknown individual(s) to steal their credentials. At least 12 NRC users were identified as having clicked on the link to the Google Spreadsheet page.

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/1

requested users to click on a link to update their user account information. This included the subject's name, e-mail address, logon ID, and password.

In January 2012, OIG received the search warrant return from Google, Inc. The search warrant return included a spreadsheet that contained 97 entries from people who replied to the e-mail. Of the 97 entries, 55 were identified as belonging to the NIH and 1 to the Department of Agriculture. OIG notified the Department of Health and Human Services (HHS) OIG of the potential compromise of their users' accounts.

In March 2012, DOJ CCIPS organized a conference call among several Government agencies working on similar cases. OIG participated in a conference call with OIG staff from the National Aeronautics and Space Administration (NASA), HHS, Department of Education, and Army Criminal Investigation Division. The conference call was in relation to an (b)(7)(F)

(b)(7)(F)

In August 2012, (b)(7)(E)

(b)(7)(E)

The subjects identified lived in (b)(7)(C) No subjects or co-conspirators were identified in the United States.

NASA OIG contacted the (b)(7)(C) regarding the identified target located within their jurisdiction.

NASA OIG also contacted the (b)(7)(C) who were in the planning stages of an operation to arrest the 10 identified targets in that country. Those subjects were located (b)(7)(C) however, did not provide any date as to when these arrests would occur.

NASA OIG also provided information on two targets located in (b)(7)(C) to a representative of the (b)(7)(C) and was told a criminal case had been initiated there.

(b)(7)(C)

Information on a target in (b)(7)(C) was transmitted through the Justice Department Legal Attaché office in (b)(7)(C) This target is believed to have victimized a number of individuals based in (b)(7)(C) as well as in the United States.

Between December 2012 and January 2013, OIG contacted other members of the joint investigation to determine if progress had been made with foreign law enforcement in working on the actionable targets provided to them as a result of this investigation. OIG

learned that progress with the foreign law enforcement authorities had stalled and that currently no progress has been made in getting them to take action on the targets provided to them.

Distribution  
File location (b)(7)(E)

Case File No. 11-48

Historical File

Magnum

| OIG/AIGI | OIG       | OIG/AIGI | OIG/AIGI    | OIG     | OIG     |
|----------|-----------|----------|-------------|---------|---------|
|          | (b)(7)(C) |          | J. McMillan | D. Lee  | H. Bell |
| 4/12/13  | 5/12/13   | 5/1/13   | 4/17/13     | 4/10/13 | 4/18/13 |

Official File Copy

5

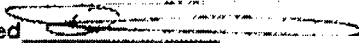
THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.



OFFICE OF THE  
INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~  
UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

April 17, 2013

MEMORANDUM TO: Concur: Case Closed   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

FROM:

(b)(7)(C)

SUBJECT: LOGON CREDENTIAL HARVESTING USING GOOGLE  
SPREADSHEETS (OIG CASE NO. 11-48)

**Allegation**

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), initiated this investigation after being notified by the NRC Computer Security Office (CSO) on June 24, 2011, that an unknown individual(s) sent a phishing e-mail to approximately 215 NRC employees' NRC e-mail accounts for the purpose of harvesting NRC network user ID and password (credentials). The link in the e-mail went to a legitimate Web site, (b)(7)(F) where a form was set up for users to "validate" their network credentials by entering their username and password, which allows the unknown individual(s) to steal their credentials. At least 12 NRC users were identified as having clicked on the link to the Google Spreadsheet page.

THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

APR  
2

## Findings

OIG was unable to conclusively identify the person(s) engaging in the spear phishing activities against the NRC. The investigation identified several suspects located in different foreign countries who may be participants in a scheme to fraudulently obtain network logon credentials from a variety of sources, including the U.S. Government, to send SPAM e-mail messages. Investigative leads sent to these other countries resulted in no law enforcement action being taken against the targets. As a result, the OIG was unable to identify domestic targets who may be involved in the operation.

## Basis for Findings

In June 2011, the OIG Cyber Crime Unit (CCU) was contacted by CSO regarding an attempt to harvest network logon credentials from NRC users via a link in an e-mail. The link sent the users to a Google Spreadsheets page that requested they enter their computer account information to verify their account. At least 12 NRC users were identified as having clicked on the link to the Google Spreadsheets page. Approximately 215 NRC employees received this e-mail. As a result of this activity, the NRC spent numerous man-hours identifying, cleaning, and changing NRC user profiles. As a result, access to the Google Spreadsheets was also blocked from the NRC network. Shortly after this time, the NRC received two similar e-mails requesting the same type of information using Google Spreadsheets.

NRC OIG coordinated this investigation with the Department of Justice (DOJ), Cyber Crimes and Intellectual Property Section (CCIPS), for possible prosecution and investigative assistance.

OIG sent a subpoena to Google for information relating to the account subscribers connected to the Google Spreadsheets identified in the e-mails sent to NRC users in June 2011. Google representatives contacted OIG and provided information from Google relating to two Google accounts associated with Google Spreadsheet links in the e-mails sent to the NRC on June 30, 2011, and July, 4, 2011. A review of the Google accounts identified that one of the accounts was set up for the sole purpose of sending the spear phishing e-mails and was set up from (b)(7)(C) and the other was a compromised account of a Google user from (b)(7)(C).

(b)(7)(E) in relation to these accounts and another phishing e-mail containing a link to Google Spreadsheet that was sent to the NRC in December 2011. The phishing e-mail requested users to click on a link to update their user account information. This included the subject's name, e-mail address, logon ID, and password.



In January 2012, OIG (b)(7)(E) (b)(7)(E) included a spreadsheet that contained 97 entries from people who replied to the e-mail. Of the 97 entries, 55 were identified as belonging to the National Institutes of Health and 1 to the Department of Agriculture. OIG notified the Department of Health and Human Services (HHS) OIG of the potential compromise of their users' accounts.

In March 2012, DOJ CCIPS organized a conference call among several Government agencies working on similar cases. OIG participated in a conference call with OIG staff from the National Aeronautics and Space Administration (NASA), HHS, Department of Education, and Army Criminal Investigation Division. The conference call was in relation to an (b)(7)(F)

(b)(7)(F)

In August 2012, several subjects were identified through an analysis of records obtained through subpoenas and search warrants in this investigation. The subjects identified lived in (b)(7)(C). No subjects or co-conspirators were identified in the United States.

NASA OIG contacted the (b)(7)(C) regarding the identified target located within their jurisdiction.

NASA OIG also contacted the (b)(7)(C) who were in the planning stages of an operation to arrest the 10 identified targets in that country. Those subjects were located in the (b)(7)(C) however, did not provide any date as to when these arrests would occur.

NASA OIG also provided information on two targets located in (b)(7)(C) to a representative of the (b)(7)(C) and was told a criminal case had been initiated there.

Information on a target in (b)(7)(C) was transmitted through the Justice Department Legal Attaché office in (b)(7)(C). This target is believed to have victimized a number of individuals based in (b)(7)(C) as well as in the United States.

Between December 2012 and January 2013, OIG contacted other members of the joint investigation to determine if progress had been made with foreign law enforcement in working on the actionable targets provided to them as a result of this investigation. OIG learned that progress with the foreign law enforcement authorities had stalled and that currently no progress has been made in getting them to take action on the targets provided to them.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

Because the information regarding the foreign individuals has been referred to DOJ for action, and no subjects or co-conspirators were identified in the United States, it is recommended that this case be closed to file.

File Location's (b)(7)(E)  
Distribution:  
11-48 Historical file Magnum

| OIG/AIGI  | OIG/AIGI | OIG/AIGI | OIG/AIGI    | OIG     | OIG     |
|-----------|----------|----------|-------------|---------|---------|
| (b)(7)(C) |          |          | J. McMillan | D. Lee  | H. Bell |
| 7/16/13   | 6/13/13  | 5/1/13   | 4/17/13     | 4/15/13 | 4/15/13 |

Official File Copy

4

THIS DOCUMENT IS THE PROPERTY OF THE RMC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

April 4, 2014

MEMORANDUM TO: Joseph A. McMillan, Assistant Inspector General  
for Investigations  
Office of the Inspector General

FROM: Miriam L. Cohen  
Chief Human Capital Officer

SUBJECT: CLOSURE OF OFFICE OF THE INSPECTOR GENERAL  
CASE NO. 12-09

This responds to your December 9, 2013, memorandum to R. W. Borchardt forwarding the Report of Investigation for OIG Case No. 12-09. This report, which was sent to management for appropriate action, pertained to the alleged misuse of Government time and equipment by an employee in the Office of Public Affairs (OPA).

(b)(7)(C)

To address the findings in this report, OPA management issued a written reprimand to the employee for [redacted] misconduct. This action was coordinated with this office and the Office of the General Counsel.

This completes our action on the investigation report findings and this case should be closed. Your time and attention to this matter is appreciated.

CONTACT: (b)(7)(C) [redacted] ELRB/OCHCO



CHAIRMAN

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~  
UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

April 10, 2014

MEMORANDUM TO: Hubert T. Bell, Inspector General  
FROM: Chairman Allison M. Macfarlane *AM Macfarlane*  
SUBJECT: Closure of Office of the Inspector General Case No. 12-09

Thank you for providing me with a copy of your report in the above-described case, which pertained to the alleged misuse of government time and equipment by an employee in the Office of Public Affairs (OPA).

I have reviewed the report, including your findings and conclusions. Additionally, I asked the Chief Human Capital Officer to work with the Office of the General Counsel and my (b)(7)(C) to review the report and assist me in developing an appropriate response. A copy of the Office of the Chief Human Capital Officer's April 4, 2014 memorandum responding to your report is enclosed.

(b)(7)(C) To address the findings in this report, the (b)(7)(C) issued a written reprimand to the employee for misconduct. This action was coordinated with my office, the Office of the Chief Human Capital Officer, and the Office of the General Counsel.

As this investigation is now closed, and our action in response to your findings is now complete, enclosed please also find my copy of your report, which I am returning to you for proper storage and disposition.

Enclosures:  
As stated

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/4



OFFICE OF THE  
INSPECTOR GENERAL

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

December 18, 2013

MEMORANDUM TO: Chairman Macfarlane

FROM:

*Hubert T. Bell*  
Hubert T. Bell  
Inspector General

SUBJECT:

MISUSE OF GOVERNMENT TIME BY AN OFFICE OF PUBLIC  
AFFAIRS EMPLOYEE (OIG CASE NO. 12-09)

Attached is an Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), Report of Investigation pertaining to alleged misuse of Government time and equipment by an Office of Public Affairs employee to (b)(7)(C).  
(b)(7)(C) Copies have been provided to the Office of the Chief Human Capital Officer and Office of the General Counsel to facilitate an NRC management response. A copy has also been provided to the Division of Facilities and Security/Office of Administration.

This report is furnished for whatever action you deem appropriate. Please notify this office within 120 days of what action you take based on the results of this investigation. Contact this office if further assistance is required.

The distribution of this report should be limited to those NRC managers required for evaluation of this matter. Neither the Report of Investigation nor its exhibits may be placed in ADAMS without OIG's written permission.

Attachments: Report of Investigation w/ exhibits

cc: Mark Satorius, EDO

(b)(7)(C) OCHCO

(b)(7)(C) OGC

(b)(7)(C) ADM/DFS

CONTACT: (b)(7)(C) OIG

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

MEMORANDUM TO: Chairman Macfarlane

FROM: Hubert T. Bell  
Inspector General

SUBJECT: MISUSE OF GOVERNMENT TIME BY AN OFFICE OF PUBLIC  
AFFAIRS EMPLOYEE (OIG CASE NO. 12-09)

Attached is an Office of the Inspector General (OIG), U.S. Nuclear Regulatory  
Commission (NRC), Report of Investigation pertaining to alleged misuse of Government  
time and equipment by an Office of Public Affairs employee to (b)(7)(C)

(b)(7)(C) Copies have been provided to the Office of the Chief  
Human Capital Officer and Office of the General Counsel to facilitate an NRC  
management response. A copy has also been provided to the Division of Facilities and  
Security/Office of Administration.

This report is furnished for whatever action you deem appropriate. Please notify this  
office within 120 days of what action you take based on the results of this investigation.  
Contact this office if further assistance is required.

The distribution of this report should be limited to those NRC managers required for  
evaluation of this matter. Neither the Report of Investigation nor its exhibits may be  
placed in ADAMS without OIG's written permission.

Attachments: Report of Investigation w/ exhibits

cc: Mark Satorius, EDO  
(b)(7)(C) OCHCO  
(b)(7)(C) OGC  
(b)(7)(C) ADM/DFS

CONTACT: (b)(7)(C) OIG

Distribution: (b)(7)(E)

Case File 12-09 Historical File MAGNUM

|          |           |          |             |          |          |          |
|----------|-----------|----------|-------------|----------|----------|----------|
| OIG      | OIG       | OIG      | OIG         | OIG      | OIG      | OIG      |
|          | (b)(7)(C) |          | J. McMillan | D. Lee   | H. Bell  |          |
| 12/19/13 | 12/18/13  | 12/12/13 | 12/18/13    | 12/19/13 | 12/18/13 | 12/18/13 |

Official Record Copy

OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION



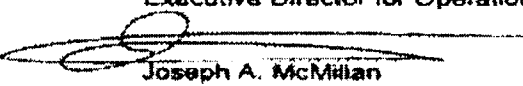
OFFICE OF THE  
INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

December 18, 2013

MEMORANDUM TO: Mark A. Satorius  
Executive Director for Operations

FROM:   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

SUBJECT: UPDATE: MISUSE OF GOVERNMENT TIME BY AN OFFICE  
OF PUBLIC AFFAIRS EMPLOYEE (CASE NO. 12-09)

Recently, you received the subject report pertaining to an Office of Public Affairs (OPA) employee. Because OPA reports to the Chairman, we are reissuing the report directly to the Chairman. My staff will work with your staff, if needed, to coordinate retrieval of this material.

cc: (b)(7)(C) OGC  
(b)(7)(C) OCHCO  
(b)(7)(C) ADM/DFS

CONTACT: (b)(7)(C) OIG

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/6

MEMORANDUM TO: Mark A. Satorius  
Executive Director for Operations

FROM: Joseph A. McMillan  
Assistant Inspector General  
for Investigations

SUBJECT: UPDATE: MISUSE OF GOVERNMENT TIME BY AN OFFICE  
OF PUBLIC AFFAIRS EMPLOYEE (CASE NO. 12-09)

Recently, you received the subject report pertaining to an Office of Public Affairs (OPA) employee. Because OPA reports to the Chairman, we are reissuing the report directly to the Chairman. My staff will work with your staff, if needed, to coordinate retrieval of this material.

cc: (b)(7)(C) OGC  
(b)(7)(C) OCHCO  
(b)(7)(C) ADM/DFS

CONTACT: (b)(7)(C) OIG

Distribution:

File Location: (b)(7)(E)

Case File 12-28 Historical File MAGNUM

| OIG/AIGI | OIG/AIGI  | Editor   | OIG/AIGI    | OIG      | OIG      |
|----------|-----------|----------|-------------|----------|----------|
|          | (b)(7)(C) |          | J. McMillan | D. Lee   | H. Bell  |
| 12/15/13 | 12/18/13  | 12/17/13 | 12/18/13    | 12/18/13 | 12/18/13 |

Official File Copy

THIS DOCUMENT IS THE PROPERTY OF THE WPC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE WPC OIG.

~~OFFICIAL USE ONLY~~ ~~OIG INVESTIGATION INFORMATION~~



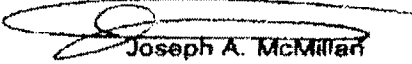


OFFICE OF THE  
INSPECTOR GENERAL

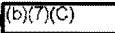

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

December 9, 2013

MEMORANDUM TO: Mark A. Satorius  
Executive Director for Operations

FROM:   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

SUBJECT: MISUSE OF GOVERNMENT TIME BY AN OFFICE OF PUBLIC  
AFFAIRS EMPLOYEE (OIG CASE NO. 12-09)


Attached is an Office of the Inspector General (OIG), U.S. Nuclear Regulatory  
Commission (NRC), Report of Investigation (ROI) pertaining to alleged misuse of  
Government time and equipment by an Office of Public Affairs (OPA) employee to   
 A copy of the ROI with exhibits is also  
attached for you to provide to the Office of the Chief Human Capital Officer.

This report is furnished for whatever action you deem appropriate. Please notify this  
office within 120 days of what action you take based on the results of this investigation.  
Contact this office if further assistance is required.

The distribution of this report should be limited to those NRC managers required for  
evaluation of this matter. Neither the Report of Investigation nor its exhibits may be  
placed in ADAMS without OIG's written permission.

Attachments: Report of Investigation w/ exhibits (plus one copy)

cc:  OGC w/ exhibits  
 ADM/DFS w/ exhibits

CONTACT:  OIG

THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED  
OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.

OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION

A/7

**OFFICE OF THE INSPECTOR GENERAL**

**Report of Investigation**



**MISUSE OF GOVERNMENT TIME BY AN  
OFFICE OF PUBLIC AFFAIRS EMPLOYEE**

|   |                |              |
|---|----------------|--------------|
| (b)(7)(C)   | Case No. 12-08 | (b)(7)(C)    |
| (b)(7)(C)   | Special Agent  | Team Leader  |
| Joseph A. McMillan, Assistant Inspector General<br>for Investigations |                | Date 12/8/13 |

**THIS REPORT IS RELEASABLE ONLY BY THE U.S. NUCLEAR REGULATORY  
COMMISSION, OFFICE OF THE INSPECTOR GENERAL.**

**THIS REPORT OR ITS EXHIBITS MAY NOT BE PLACED IN ADAMS WITHOUT  
WRITTEN PERMISSION OF THE NRC OIG.**

**EXEMPT FROM RELEASE UNDER FREEDOM OF INFORMATION ACT  
EXEMPTIONS (5), (6) OR (7) AND PRIVACY ACT EXEMPTIONS (j)(2) OR (k)(1)**

THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED  
OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.

## STATUTES, REGULATIONS, AND POLICY

### NRC Management Directive (MD) 7.8, "Outside Employment":

#### I. Policy

It is the policy of the U.S. Nuclear Regulatory Commission that NRC employees receive written approval before engaging in certain outside employment, in accordance with ethics regulation 5 CFR 5801.103. Employees may engage in outside employment not covered by this directive without obtaining NRC approval.

### NRC Handbook MD 7.8(I), "Outside Employment":

#### B. Requirements for Outside Employment

1. NRC regulations require that employees, except special Government employees, obtain prior written approval before engaging in outside employment with entities regulated by or having business with the Commission. These entities are the following:

- (a) A Commission licensee;
- (b) An applicant for a Commission license;
- (c) An organization directly engaged in activities in the commercial nuclear field;
- (d) A Commission contractor;
- (e) A Commission supplier;
- (f) An applicant for or holder of a license issued by a State pursuant to an agreement between the Commission and the State;
- (g) A trade association that represents clients concerning nuclear matters;
- (h) A law firm or other organization that is participating in an NRC proceeding or that regularly represents itself or clients before the NRC.

### NRC Management Directive (MD) 2.7- "Personal Use of Information Technology"

#### Policy (2.7-01)

It is the policy of the U.S. Nuclear Regulatory Commission to permit employees limited use of agency information technology for personal needs if the use does not interfere with official business and involves minimal or no additional expense to the NRC.

#### **Handbook MD 2.7, Section D, "Inappropriate Personal Uses"**

Employees are expected to conduct themselves professionally in the workplace and to refrain from using agency information technology for activities that are inappropriate. Misuse or inappropriate personal use of agency information technology includes— (1)

Any personal use that could cause congestion, delay, or disruption of service to any agency system or equipment. Examples of possible misuse include:

- ... Use of information technology for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services)...

- ... Any other activity that interferes with official duties.

#### **NRC Agency-wide Rules of Behavior for Authorized Computer Use**

##### **3. Rules of Behavior for Non-public Users**

The following rules apply to all NRC non-public users of NRC computing resources. These rules are based on and are consistent with policy and procedures in NRC MD 2.7, "Personal Use of Information Technology," and MD 12.5, "NRC Cyber Security Program."

##### **3.1 System Access and Use**

Preventing unauthorized access to NRC IT systems and information requires the full cooperation of all users for effective and successful security. Users must be aware of their responsibilities for maintaining effective access controls, particularly regarding the use of identification and authentication information and strict adherence with the permissions granted to them. The following rules of behavior are relevant to NRC system access and use.

Users shall:

- Use Government-owned or Government-leased computing resources for work related purposes only except as allowed by MD 2.3, "Telecommunications"; MD 2.7; and MD 12.5. No other unofficial use is authorized.

Users shall not:

- Use NRC computing resources to conduct or support a personal business.

**SUBJECT**

(b)(7)(C)

Office of Public Affairs (OPA)  
U.S. Nuclear Regulatory Commission (NRC)

**ALLEGATION**

The Office of the Inspector General (OIG), NRC, received an anonymous allegation that (b)(7)(C) on official Government time. The (b)(7)(C) alleged(s) asserted that during several visits to OPA, they observed that (b)(7)(C) "spent all of (b)(7)(C) time talking on the phones to (b)(7)(C)"

**FINDINGS**

OIG found that, inconsistent with MD 2.7 (b)(7)(C) engaged in activity on (b)(7)(C) Government computer that was related to (b)(7)(C) secondary employment as the regular (b)(7)(C) MD 2.7 prohibits using agency information technology in support of outside employment or business activity. (b)(7)(C) activities of this kind included the downloading of document files of some (b)(7)(C) on (b)(7)(C) as well as numerous visits to (b)(7)(C) related Web sites, including (b)(7)(C) own blog and other similar sites, on (b)(7)(C) Government computer. (b)(7)(C) in addition (b)(7)(C) on occasion used the Government computer to write (b)(7)(C) (b)(7)(C) and process travel and administrative documents (b)(7)(C) related to paid activities where (b)(7)(C) acted as a speaker at (b)(7)(C) events or a judge at (b)(7)(C) competitions.

OIG found no evidence that (b)(7)(C) posted articles to the (b)(7)(C) for pay directly from the Government computer. OIG also found that (b)(7)(C) government email account reflected a high volume of traffic related to NRC work and a comparatively minor proportion of traffic related in any way to the topic of (b)(7)(C)

**BASIS OF FINDINGS**

(b)(7)(E)

OIG conducted a (b)(7)(E) of (b)(7)(C) Government computer in November 2011, including (b)(7)(E)

(b)(7)(C)

(b)(7)(E) From this, OIG learned that (b)(7)(C) frequently browsed (b)(7)(C) related web sites, including — own blog, from — Government computer. An OIG check of (b)(7)(C) browsing history over an 11-day period from October 28, 2011, to November 7, 2011, showed that (b)(7)(C) had connected to (b)(7)(C) on 6 of 7 workdays during the period. An OIG check of (b)(7)(C) browsing history covering a longer overlapping period from July 25, 2011, to November 28, 2011, showed connections to (b)(7)(C) related sites on 55 of the 88 workdays during the period. A separate OIG check of the browsing history covering the period from December 9, 2012, to February 7, 2013 revealed connections with (b)(7)(C) (b)(7)(C) blog on 23 of the 41 workdays during the period. Time stamp data disclosed in these reviews showed that such connections occurred throughout the day on multiple working days, with visits as early as 8:26 a.m. and as late as 5:17 p.m. OIG also found a number of files on (b)(7)(C) Government computer that included adobe documents and Word files of articles (b)(7)(C) had written for the (b)(7)(C) and document files of bills for expenses to — industry entities.

(b)(7)(C)

(b)(7)(C)

(For further details, see Exhibits 1, 2, and 3.)

An OIG review of the publicly available archive for (b)(7)(C) columns between November 2011 and May 2013 on the (b)(7)(C) Web site showed that the (b)(7)(C) published such articles between 6 and 7 times per month on average, with a low of 3 and a high of 13 for any given month during that period.

(For further details, see Exhibit 4.)

OIG conducted a detailed forensic examination of (b)(7)(C) Government email for a 6-month period from June 2011 through December 2011. This examination disclosed no emails to (b)(7)(C) which is the email address used to submit material to the (b)(7)(C) consistent with (b)(7)(C) claims that (b)(7)(C) only during non-duty hours and from a non-Government computer. This examination disclosed only 10 instances out of over 2,500 sent emails from (b)(7)(C) using — Government email that appeared in any way — related. This included one communication from (b)(7)(C) industry recipient, indicating that the recipient should never use the Government email address for any — related communication. Most of the other

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

OFFICIAL USE ONLY – OIG INVESTIGATION INFORMATION

(b)(7)(C) related sent emails on the Government account for the period were brief personal communications to other NRC employees who had apparently solicited (b)(7)(C) advice about (b)(7)(C)

(For further details, see Exhibits 5 and 6.)

(b)(7)(C) Training Records

OIG learned that (b)(7)(C) was familiar with the NRC Agency-Wide Rules of Behavior for Authorized Computer Use, based upon (b)(7)(C) completion of the NRC annually required computer security training, whose third section specifically includes the Rules of Behavior and requires the participant to make a specific acknowledgement of those rules. (b)(7)(C) provided a certificate indicating that (b)(7)(C) had completed such training on August 14, 2012. (b)(7)(C)

(For further details, see Exhibit 7.)

Review of (b)(7)(C)

An OIG (b)(7)(C) including NRC performance appraisals for the years 2009, 2010, and 2011, and several performance based awards documented on Standard Form (SF) 50, indicated that (b)(7)(C) had been consistently rated overall "Outstanding" for the period 2009-2011 inclusive, and had consistently received performance rating based bonuses in all fiscal years dating from 2007 to 2012, and additional unspecified bonuses in all prior years between 2003 and 2006

(For further details, see Exhibit 8.)

Interview of (b)(7)(C)

(b)(7)(C) told OIG (b)(7)(C) had been working at NRC since February 2003, and recalled that (b)(7)(C) had been (b)(7)(C) stated that (b)(7)(C) had held the regular (b)(7)(C) This position required the regular submission of (b)(7)(C) (b)(7)(C) stated that (b)(7)(C) submission of (b)(7)(C) was done outside Government working hours, by email from (b)(7)(C) personal home computer to the email address, (b)(7)(C) with copies to the (b)(7)(C) email addresses of two editors for (b)(7)(C)

(b)(7)(C) told OIG that, in addition to the regular (b)(7)(C) (b)(7)(C) writes a blog on (b)(7)(C) to social media outlets (b)(7)(C) described

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

these as occasional activities, and stated that they did not earn income. (b)(7)(C)

(b)(7)(C) stated that all posting of entries on such Web sites or applications is done outside Government working hours, from personal home computer or from a personal tablet. However, (b)(7)(C) admitted that, on occasion, (b)(7)(C) may have given a "quick answer" to a comment on (b)(7)(C) blog using his Government computer. (b)(7)(C)

(b)(7)(C) also stated that (b)(7)(C) occasionally earned money for attending (b)(7)(C) related events such as (b)(7)(C) where (b)(7)(C) served as a judge, and for participating in or leading panel discussions on (b)(7)(C) (b)(7)(C) stated that this was always done while on leave status, on weekends, or regular days off. (b)(7)(C) explained that (b)(7)(C) works a compressed work schedule with alternate Fridays off. (b)(7)(C) also stated that on occasion (b)(7)(C) used a Government scanner connected to (b)(7)(C) work computer to upload documents related to (b)(7)(C) travel for such (b)(7)(C) related events, for the purpose of emailing them to (b)(7)(C) at a personal email address in order to facilitate applying for reimbursement of expenses from the sponsors of these (b)(7)(C) related events. (b)(7)(C) stated that this was a rare occurrence and that the (b)(7)(C) did not typically reimburse any expenses relating to (b)(7)(C) work for them, although (b)(7)(C) had discussed this possibility with (b)(7)(C). (b)(7)(C)

When questioned about the results of the OIG forensic analysis of his Government computer, which revealed extensive browsing history on (b)(7)(C) related Web sites, as well as files that appeared to be draft versions of (b)(7)(C) and other (b)(7)(C) related documents, (b)(7)(C) admitted to viewing (b)(7)(C) related Web sites, including (b)(7)(C) own blog and those of other (b)(7)(C) and to occasionally working on files related to (b)(7)(C) on the computer. (b)(7)(C) stated that this was on non-work time. "When I stayed late after work, to finish up a column, when... I was on deadline" and would not have consumed much work time even on the occasions when it occurred during working hours, as (b)(7)(C) NRC workload was significant. (b)(7)(C)

(b)(7)(C) told OIG (b)(7)(C) occasionally conducted interviews or other telephone calls related to (b)(7)(C) from (b)(7)(C) NRC work location. (b)(7)(C) estimated that this may have occurred "four to five" times, and stated that this was always done in a closed-door OPA conference room during lunch period or otherwise outside official work time, and that this was always done using his personal cellular telephone. (b)(7)(C) told OIG that a visitor to the OPA office might hear (b)(7)(C) talking on his Government desk telephone about (b)(7)(C) on occasion, but (b)(7)(C) explained that this would generally be during the course of conversations with (b)(7)(C) spouse, who made a practice of calling (b)(7)(C) a (b)(7)(C) desk rather than on the personal cellular telephone and frequently discussed (b)(7)(C) and/or the general topic of (b)(7)(C). (b)(7)(C)

(For further details, see Exhibit 5.)



~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

Interview of (b)(7)(C)

(b)(7)(C) supervisor, (b)(7)(C) told OIG that (b)(7)(C) was aware of (b)(7)(C) and had no concerns over the effect of this activity on (b)(7)(C) NRC job performance. (b)(7)(C) stated that (b)(7)(C) did not believe (b)(7)(C) had reason to cause (b)(7)(C) (b)(7)(C) described (b)(7)(C) job performance in highly positive terms, and stated that (b)(7)(C) frequently designated (b)(7)(C) to act as (b)(7)(C) OPA in (b)(7)(C) absence. (b)(7)(C) recounted that (b)(7)(C) had frequent daily interaction with (b)(7)(C) and that in the course of such interaction (b)(7)(C) typically observed (b)(7)(C) to be actively engaged in NRC OPA work projects and not in (b)(7)(C) or conversation.

(For further details, see Exhibit 9.)

MEMORANDUM TO: Mark A. Satorius  
Executive Director for Operations

FROM: Joseph A. McMillan  
Assistant Inspector General  
for Investigations

SUBJECT: MISUSE OF GOVERNMENT TIME BY AN OFFICE OF PUBLIC  
AFFAIRS EMPLOYEE (OIG CASE NO. 12-09)

Attached is an Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), Report of Investigation (ROI) pertaining to alleged misuse of Government time and equipment by an Office of Public Affairs (OPA) employee to write a column about wine for a local newspaper. A copy of the ROI with exhibits is also attached for you to provide to the Office of the Chief Human Capital Officer.

This report is furnished for whatever action you deem appropriate. Please notify this office within 120 days of what action you take based on the results of this investigation. Contact this office if further assistance is required.

The distribution of this report should be limited to those NRC managers required for evaluation of this matter. Neither the Report of Investigation nor its exhibits may be placed in ADAMS without OIG's written permission.

Attachments: Report of Investigation w/ exhibits (plus one copy)

cc: (b)(7)(C) OGC w/ exhibits  
(b)(7)(C) ADM/DFS w/ exhibits

CONTACT: (b)(7)(C) OIG

Distribution: (b)(7)(E)

Case File 12-09 Historical File MAGNUM

| OIG       | OIG      | OIG      | OIG      | OIG         | OIG      | OIG     |
|-----------|----------|----------|----------|-------------|----------|---------|
| (b)(7)(C) |          |          |          | J. McMillan | D. Lee   | H. Bell |
| 11/15/13  | 11/15/13 | 11/15/13 | 11/22/13 | 12/8/13     | 11/29/13 | 12/9/13 |

Official Record Copy

**EXHIBITS**

1. Memorandum to File, Computer Forensic Report, dated February 7, 2013 (with Attachments).
2. Memorandum to File, Review of (b)(7)(C) Internet Use, dated January 9, 2012.
3. Memorandum to File, Additional Review of Log Logic Search, dated November 20, 2013, with attachments.
4. Memorandum to File, Review of (b)(7)(C) Archive, dated November 20, 2013, with attachment.
5. Transcript, Interview of (b)(7)(C) dated April 30, 2013.
6. Memorandum to File, Review of (b)(7)(C) Email, dated January 20, 2013.
7. Training Certificate (b)(7)(C) NRC Computer Security Awareness Training, dated August 14, 2012.
8. Memorandum to File, Review of (b)(7)(C) dated May 31, 2013.
9. Transcript, Interview of (b)(7)(C) dated May 8, 2013.



OFFICE OF THE  
INSPECTOR GENERAL

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555-0001

May 15, 2013

MEMORANDUM TO:

Concur: Case Closed  
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

(b)(7)(C)

FROM:

(b)(7)(C)

SUBJECT:

MISUSE OF GOVERNMENT COMPUTER BY OFFICE OF  
ADMINISTRATION EMPLOYEE (OIG CASE NO. 12-24)

**Allegation**

This Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), investigation was initiated based on a proactive project to identify instances of computer misuse on the NRC computer network. OIG identified an NRC computer assigned to the (b)(7)(C) Personnel Security Branch (PSB), Division of Facilities and Security (DFS), Office of Administration (ADM), which was used to obtain sexually explicit or sexually oriented images using Google searches.

**Findings**

OIG found the user account (b)(7)(C) belonging to (b)(7)(C) ADM, NRC, accessed various pornographic images by utilizing various search terms on Google Images. OIG also found that an unauthorized application (Google Chrome) was installed on the NRC computer. OIG notes that (b)(7)(C) was terminated by (b)(7)(C) company for time and attendance issues prior to the completion of this investigation and no longer works for NRC; therefore, this report is issued as a close-to-file memorandum.

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.

7/8

### Basis of Findings

On February 7, 2012, a person using the user account (b)(7)(C) on NRC Asset Tag (b)(7)(C) accessed the Web page [www.mobypicture.com/group/pussy](http://www.mobypicture.com/group/pussy) via a link from Google Images. This page displays numerous pictures of female genitalia in pornographic fashion. A check of the user account revealed the account belonged to (b)(7)(C).

This user also entered the keywords "wet pussy" and "cojiendo rico" (which translates to "Rich Fucking") within Google Images to view other pornographic images, to include images of sexual acts as well as nudity.

The OIG Cyber Crime Unit's (CCU) analysis identified that the (b)(7)(C) profile user viewed more than 300 images that were either pornographic in nature, sexually oriented, or related to sexually related keywords searched through Google of various photo hosting Web sites. The images include close-ups of genitalia and persons engaging in sexual activities. All of the images identified appear in several folders located under the Google Chrome Internet Browser (Chrome) application folder.

There were also signs that unauthorized software was installed on the computer by the user (b)(7)(C). The application Google Chrome, an Internet browser similar to Internet Explorer, was installed under the profile (b)(7)(C) under (b)(7)(C).

(b)(7)(C) A review of the application permissions revealed that the user (b)(7)(C) installed the application under (b)(7)(C) profile.

OIG briefed (b)(7)(C) PSB, on this investigation (b)(7)(C) informed OIG that (b)(7)(C) was terminated by (b)(7)(C) company because of time and attendance issues. (b)(7)(C) stated that (b)(7)(C) submitted false timecards and failed to make up hours when (b)(7)(C) arrived late to work.

CCU notified the NRC Computer Security Office (CSO) of the Google Chrome application installed on (b)(7)(C) computer. CCU also informed CSO of NRC users' ability to install the Google Chrome application without the approval of NRC's Office of Information Services.

Because (b)(7)(C) is no longer employed as a (b)(7)(C) by the NRC and no additional personnel action can be taken against (b)(7)(C) it is recommended that this case be closed to the files of this office.

**Basis of Findings**

On February 7, 2012, a person using the user account (b)(7)(C) on NRC Asset Tag (b)(7)(C) accessed the Web page [www.mobypicture.com/group/pussy](http://www.mobypicture.com/group/pussy) via a link from Google Images. This page displays numerous pictures of female genitalia in pornographic fashion. A check of the user account revealed the account belonged to (b)(7)(C).

This user also entered the keywords "wet pussy" and "cojiendo rico" (which translates to "Rich Fucking") within Google Images to view other pornographic images, to include images of sexual acts as well as nudity.

The OIG Cyber Crime Unit's (CCU) analysis identified that the (b)(7)(C) profile user viewed more than 300 images that were either pornographic in nature, sexually oriented, or related to sexually related keywords searched through Google of various photo hosting Web sites. The images include close-ups of genitalia and persons engaging in sexual activities. All of the images identified appear in several folders located under the Google Chrome Internet Browser (Chrome) application folder.

There were also signs that unauthorized software was installed on the computer by the user (b)(7)(C). The application Google Chrome, an Internet browser similar to Internet Explorer, was installed under the profile (b)(7)(C) under (b)(7)(C).

A review of the application permissions revealed that the user (b)(7)(C) installed the application under (b)(7)(C) profile.

OIG briefed (b)(7)(C) PSB on this investigation. (b)(7)(C) informed OIG that (b)(7)(C) was terminated by (b)(7)(C) company because of time and attendance issues. (b)(7)(C) stated that (b)(7)(C) submitted false timecards and failed to make up hours when (b)(7)(C) arrived late to work.

CCU notified the NRC Computer Security Office (CSO) of the Google Chrome application installed on (b)(7)(C) computer. CCU also informed CSO of NRC users' ability to install the Google Chrome application without the approval of NRC's Office of Information Services.

Because (b)(7)(C) is no longer employed as a (b)(7)(C) by the NRC and no additional personnel action can be taken against (b)(7)(C), it is recommended that this case be closed to the files of this office.

Distribution (b)(7)(E)

Case No. 12-24

| OIG/AIGI  | OIG/AIGI  | Editor    | OIG/AIGI  | OIG/AIGI    | OIG      | OIG     |
|-----------|-----------|-----------|-----------|-------------|----------|---------|
| (b)(7)(C) | (b)(7)(C) | (b)(7)(C) | (b)(7)(C) | J. McMillan | D. Leach | H. Bell |
| 5/5/13    | 5/13/13   | 5/14/13   | 5/15/13   | 5/15/13     | 5/16/13  | 5/16/13 |

Official File Copy

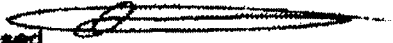


OFFICE OF THE  
INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20545-5601

February 20, 2013

MEMORANDUM TO: Concur; Case Closed   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

(b)(7)(C)

FROM:

(b)(7)(C)

SUBJECT: MISUSE OF GOVERNMENT EQUIPMENT AND RESOURCES  
BY AN OFFICE OF ADMINISTRATION EMPLOYEE (OIG CASE  
NO. 12-49)

**Allegation**

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), initiated this investigation based on an anonymous allegation received via the OIG Hotline Website regarding misuse of Government equipment and resources by (b)(7)(C)

(b)(7)(C) Office of Administration (ADM), NRC. Specifically, the (b)(7)(C) alleged reported that (b)(7)(C) was sending personal e-mails from work and mailing packages to (b)(7)(C) regarding medical insurance of two minor children not related to (b)(7)(C)

**Findings**

OIG did not substantiate any violation of policy regarding the use of Government resources or equipment.

THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/9

OFFICIAL USE ONLY – OIG INVESTIGATION INFORMATION

Basis for Findings

OIG reviewed commercial records for law enforcement which identified that a (b)(7)(C) (b)(7)(C) resided at (b)(7)(C) (b)(7)(C) also reviewed (b)(7)(C) e-mail account and identified no personal e-mails.

Mail Room Services staff told OIG that a package sent from the NRC Mail Room would have to have a tracking number in order to verify mailing. Also records are not kept for a prolonged period. Mail Services staff also noted that only Fed-Ex and UPS package receipts were kept on file. Employees are allowed to mail personal letters as long as postage is paid by the sender. OIG was unable to determine if (b)(7)(C) in fact, ever mailed a package from the NRC facility.

(b)(7)(C) (b)(7)(C) told OIG that (b)(7)(C) has never mailed a package from the NRC building for official business or for which (b)(7)(C) did not personally pay for the postage. (b)(7)(C) stated (b)(7)(C) has mailed packages to (b)(7)(C) in the past from the U.S. Post Office located on Twinbrook Parkway in Rockville, Maryland. (b)(7)(C) stated (b)(7)(C) paid for the mailings with (b)(7)(C) personal credit card.

(b)(7)(C) (b)(7)(C) admitted to sending some personal e-mails from work to (b)(7)(C) (b)(7)(C) using (b)(7)(C) personal e-mail account. The e-mails pertained to various issues concerning to (b)(7)(C) children (b)(7)(C) stated (b)(7)(C) would review e-mails for (b)(7)(C) before (b)(7)(C) would send them to (b)(7)(C) At no time (b)(7)(C) did (b)(7)(C) believe (b)(7)(C) e-mails were excessive or in violation of any NRC policy.

OIG interviewed (b)(7)(C) who stated (b)(7)(C) currently resides in (b)(7)(C) (b)(7)(C) (b)(7)(C) said (b)(7)(C) has never received a Government envelope from (b)(7)(C) All correspondence received has been by certified mail or other mailings.

Because OIG did not find any evidence to suggest that (b)(7)(C) was misusing Government equipment and resources, it is recommended that this case be closed to the files of OIG.



**Basis for Findings**

OIG reviewed commercial records for law enforcement which identified that a (b)(7)(C) resided at (b)(7)(C). (b)(7)(C) also reviewed (b)(7)(C) e-mail account and identified no personal e-mails.

Mail Room Services staff told OIG that a package sent from the NRC Mail Room would have to have a tracking number in order to verify mailing. Also records are not kept for a prolonged period. Mail Services staff also noted that only Fed-Ex and UPS package receipts were kept on file. Employees are allowed to mail personal letters as long as postage is paid by the sender. OIG was unable to determine if (b)(7)(C) in fact, ever mailed a package from the NRC facility.

(b)(7)(C) (b)(7)(C) told OIG that (b)(7)(C) has never mailed a package from the NRC building for official business or for which (b)(7)(C) did not personally pay for the postage. (b)(7)(C) stated (b)(7)(C) has mailed packages to (b)(7)(C) in the past from the U.S. Post Office located on Twinbrook Parkway in Rockville, Maryland. (b)(7)(C) stated (b)(7)(C) paid for the mailings with (b)(7)(C) personal credit card.

(b)(7)(C) (b)(7)(C) admitted to sending some personal e-mails from work to (b)(7)(C) using (b)(7)(C) personal e-mail account. The e-mails pertained to various issues concerning (b)(7)(C) children. (b)(7)(C) stated (b)(7)(C) would review e-mails for (b)(7)(C) before (b)(7)(C) would send them to (b)(7)(C). At no time (b)(7)(C) did (b)(7)(C) believe (b)(7)(C) e-mails were excessive or in violation of any NRC policy.

OIG interviewed (b)(7)(C) who stated (b)(7)(C) currently resides in (b)(7)(C). (b)(7)(C) (b)(7)(C) said (b)(7)(C) has never received a Government envelope from (b)(7)(C). All correspondence received has been by certified mail or other mailings.

Because OIG did not find any evidence to suggest that (b)(7)(C) was misusing Government equipment and resources, it is recommended that this case be closed to the files of OIG.

**Distribution:**  
File Location: (b)(7)(E)  
Historical I/F: Magnum OIG Case File No. 12-49

| OIG/AIGI  | OIG/AIGI  | OIG/AIGI  | OIG         | OIG     | OIG     |
|-----------|-----------|-----------|-------------|---------|---------|
| (b)(7)(C) | (b)(7)(C) | (b)(7)(C) | J. McMillan | D. Lee  | H. Bell |
| 2/14/13   | 2/14/13   | 2/20/13   | 2/20/13     | 2/20/13 | 2/22/13 |

Official File Copy

3

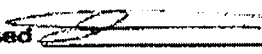
THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.



OFFICE OF THE  
INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~  
UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

February 14, 2013

MEMORANDUM TO FILE: Concur: Case Closed   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

(b)(7)(C)

FROM:

(b)(7)(C)

SUBJECT: CONCERNS REGARDING THE NRC'S "OPEN DOOR"  
POLICY AND DIFFERING PROFESSIONAL OPINION  
PROCESS (OIG CASE NO. 12-052)

**Allegation**

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), initiated this investigation based on an anonymous allegation submitted to the OIG Hotline. According to the allegor, NRC's Open and Collaborative Work Environment (OCWE) and Differing Professional Opinion (DPO) process sound fair, "but when the rubber meets the road, the programs fall apart. . . ." As examples, the allegor wrote that (1) OCWE does not mean management has to listen, but just provides a mechanism for subordinates to say something, (2) the allegor has been retaliated against for raising concerns, (3) people do not raise concerns due to fear of retribution, and (4) the DPO "program owner" told the allegor the program has "nearly fatal flaws that rendered the system useless." The allegor did not provide any specific examples to support these allegations due to concern that specifics would identify the allegor's identity.

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE NRC OIG.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/10

### Findings

OIG found NRC staff have differing perceptions of the effectiveness of the DPO program and whether use of the program leads to retaliation; however, interviewees did not identify any specific examples that demonstrated retaliation against DPO program users. OIG found the DPO program manager is aware of staff's negative perceptions and seeks to improve the program and employee perceptions of the program.

### Basis of Findings

OCWE is an agency objective that is explained in Management Directive (MD) 10.161, *Civil Rights Program and Affirmative Employment and Diversity Management Program*. One of its objectives is to promote NRC's organizational values of integrity, service, openness, commitment, cooperation, excellence, and respect, and expectations for an open, collaborative work environment, as the guiding forces in reaching affirmative employment and diversity management goals and promoting a discrimination-free work environment. Furthermore, the Office of Enforcement's (OE) internal Web site defines OCWE as a work environment that encourages all employees and contractors to promptly raise concerns and differing views without fear of reprisal.

The DPO program is described and explained in MD 10.159, *The NRC's Differing Professional Opinions Program*. This program has three objectives (1) to foster informal discussions with peers and supervisors on issues involving professional judgments that may differ from a currently held view or practice, (2) to establish a formal process for expressing DPOs concerning issues directly related to the mission of NRC, and (3) to ensure the full consideration and prompt disposition of DPOs by affording an independent, impartial review by knowledgeable personnel.

OE's internal Web site describes the DPO program as a formal process that allows all employees and contractors to have their differing views on established, mission-related issues considered by the highest level managers in their organizations, i.e., office directors and regional administrators. The process also provides managers with an independent, three-person review of the issue (one person chosen by the employee). After a decision is issued to an employee, he or she may appeal the decision to the Executive Director for Operations (EDO) (or the Chairman for those offices reporting to the Commission).

A listing and summary of all 21 DPOs that have been received, processed, and completed since the DPO Program was revised in May 2004 is posted on the internal DPO Web site (<http://www.internal.nrc.gov/OE/dpo/closed-dpo-cases.html>). The Web site reflected the agency has closed nine cases that were submitted in 2005, six submitted in 2006, two submitted in 2008, one submitted in 2009, one submitted in 2010, and two submitted in 2011. OIG reviewed the summaries for the three most

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

recent DPO closures (filed in 2010 and 2011), and noted that in all three cases, the review panel agreed with at least some of the issues raised in the DPOs and made recommendations intended to address these matters. In addition, the cognizant office director agreed with the panel's conclusions and recommendations.

Due to lack of specific examples in the anonymous allegation, OIG interviewed (b)(7)(C) (b)(7)(C) as to their perceptions of the program. OIG also asked the (b)(7)(C) for any specific examples that might demonstrate issues raised by the allegor. The (b)(7)(C) were interviewed because they would have knowledge of NRC staff that filed DPOs and felt they were being or were retaliated for using the DPO program.

OIG interviewed four NTEU members and determined that there was a consensus among the members that NRC staff felt that if they submitted a DPO, it would be career suicide or that they would be retaliated against by management. However, only one member (who had filed six DPOs) relayed a personal experience of perceived retaliation. This individual said that after submitting two DPOs, (b)(7)(C) annual performance appraisal was lower than the previous year and, on another occasion, (b)(7)(C) was removed from the project and given other duties. (b)(7)(C) could not provide additional information regarding the alleged retaliation. This individual said (b)(7)(C) was aware that management has the prerogative to assign different duties to staff, but (b)(7)(C) found it odd that (b)(7)(C) would be removed from the project after filing (b)(7)(C) DPO. None of the NTEU members interviewed could provide other specific examples of retaliation by management against a DPO submitter but they agreed that because there is a perception by NRC staff that filing a DPO leads to retaliation, many staff are unwilling to use the program.

(b)(7)(C) OE, stated that (b)(7)(C) has never said that the DPO process has fatal flaws that render it useless to any concerned individual seeking (b)(7)(C) advice on addressing a differing view. (b)(7)(C) also stated that though (b)(7)(C) believes that many of the retaliation complaints are probably more of a perception than reality, the reality is that the perception in the minds of the staff seems real. (b)(7)(C) further stated that it is difficult for (b)(7)(C) to track any retaliation complaints regarding the filing of DPOs because most of those allegations go to OIG, and (b)(7)(C) is not provided with that information by OIG. (b)(7)(C) also said that (b)(7)(C) thought (b)(7)(C) knew who made the allegation because of the small number of DPO submittals (b)(7)(C) receives. In this case, (b)(7)(C) explained that (b)(7)(C) returned a DPO submittal to an individual because the issue was still in process and advised the individual to use the Non-Concurrence Process to address (b)(7)(C) concern. (b)(7)(C) does not believe that the DPO program has fatal flaws, but believes that there is room for improvement and that OE is taking steps towards that end.

(b)(7) was aware of the negative perceptions of the DPO program from employees (including staff and management) who have used the process, from employees who have participated in focus groups on internal safety culture and the Safety Culture Climate Survey (SCCS), and from the 2009 SCCS (e.g., only 54 percent thought it was effective).

(b)(7)(C) These sources have identified multiple issues that could result in negative perceptions, including fear of retaliation. (b)(7)(C) stated that OE is aware of these issues and is taking actions to address these issues as part of their efforts to revise the DPO MD.

(b)(7)(C) (b)(7)(C) also speculated that some employees may, in fact, have been retaliated against for using the DPO Program, but (b)(7)(C) was not aware of specific data to support any substantiated claims of retaliation. Based on anecdotal comments from employees,

(b)(7)(C) (b)(7)(C) thinks that several employees who believed that they have been retaliated against have made the choice not to pursue their retaliation concern.

(b)(7)(C) (b)(7)(C) stated that some of the measures that make the program fair and useful are having an independent panel of NRC employees review the issues (one panel member selected by the employee), having the option of appealing the decision to the EDO, and allowing the employee to ask for the discretionary release of the DPO records. Furthermore, (b)(7)(C) stated that "success" for the DPO process should not be limited to a simple matter of whether or not the DPO panel or the DPO decision maker (i.e., office director or regional administrator) agrees or disagrees with a DPO submitter. Success means having a process that ensures that employees can raise differing views, have the issues fairly evaluated, and have the outcome articulated openly and honestly.

(b)(7)(C) (b)(7)(C) said that there was insufficient data to draw a specific conclusion about the frequency with which the DPO Program is used. The fact that the program is not frequently used could be interpreted as a positive, in that employees may be in alignment on issues or that they are using informal dialog or the Non-Concurrence Process to address differing views instead of using the DPO Program. Alternatively, the lack of use could also be interpreted as a lack of confidence in the process.

Because OIG identified no specific examples of retaliation for using the DPO process and OE is actively addressing the perception issues with the DPO program, recommend that this investigation be closed to files of this office.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

(b)(7)(C) was aware of the negative perceptions of the DPO program from employees (including staff and management) who have used the process, from employees who have participated in focus groups on internal safety culture and the Safety Culture Climate Survey (SCCS), and from the 2009 SCCS (e.g., only 54 percent thought it was effective).

(b)(7)(C) These sources have identified multiple issues that could result in negative perceptions, including fear of retaliation. (b)(7)(C) stated that OE is aware of these issues and is taking actions to address these issues as part of their efforts to revise the DPO MD.

(b)(7)(C) (b)(7)(C) also speculated that some employees may, in fact, have been retaliated against for using the DPO Program, but (b)(7)(C) was not aware of specific data to support any substantiated claims of retaliation. Based on anecdotal comments from employees, (b)(7)(C) thinks that several employees who believed that they have been retaliated against have made the choice not to pursue their retaliation concern.

(b)(7)(C) (b)(7)(C) stated that some of the measures that make the program fair and useful are having an independent panel of NRC employees review the issues (one panel member selected by the employee), having the option of appealing the decision to the EDO, and allowing the employee to ask for the discretionary release of the DPO records. Furthermore, (b)(7)(C) stated that "success" for the DPO process should not be limited to a simple matter of whether or not the DPO panel or the DPO decision maker (i.e., office director or regional administrator) agrees or disagrees with a DPO submitter. Success means having a process that ensures that employees can raise differing views, have the issues fairly evaluated, and have the outcome articulated openly and honestly.

(b)(7)(C) (b)(7)(C) said that there was insufficient data to draw a specific conclusion about the frequency with which the DPO Program is used. The fact that the program is not frequently used could be interpreted as a positive, in that employees may be in alignment on issues or that they are using informal dialog or the Non-Concurrence Process to address differing views instead of using the DPO Program. Alternatively, the lack of use could also be interpreted as a lack of confidence in the process.

Because OIG identified no specific examples of retaliation for using the DPO process and OE is actively addressing the perception issues with the DPO program, recommend that this investigation be closed to files of this office.

Distribution:

File Location: (b)(7)(E)

Case No. 12-78

Historical File

Magnum

| OIG/AIGI  | OIG/AIGI  | OIG     | OIG/AIGI  | OIG            | OIG            |
|-----------|-----------|---------|-----------|----------------|----------------|
| (b)(7)(C) | (b)(7)(C) |         | J. McCann | D. L. G. G. G. | H. B. H. H. H. |
| 2/14/13   | 2/14/13   | 2/14/13 | 2/14/13   | 2/14/13        | 2/14/13        |

Official File Copy

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE NRC OIG.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~



OFFICE OF THE  
INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~  
UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0081

February 19, 2013

MEMORANDUM TO:

Concur. Case Closed  
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

(b)(7)(C)

FROM:

(b)(7)(C)

SUBJECT:

MISHANDLING OF NRC REGION II ALLEGATION  
RII-2010-A-0258 (OIG CASE NO: 12-54)

**Allegation:**

This office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), investigation was based on an allegation from (b)(7)(C) previously employed at Plant Hatch (Hatch), that NRC Region II allegation (b)(7)(E) was not properly investigated and that the NRC inspectors involved in reviewing (b)(7) concerns were ordered to conduct their investigation in a manner that would not result in findings against the licensee.

**Finding:**

(b)(7)(E) (b)(7)(E) NRC did not substantiate the first issue pertaining to retrievability of tool room calibration data. NRC did substantiate the second complaint of a chilled work environment as a result of employees identifying problems with the licensee.

**Basis for Findings:**

OIG learned that (b)(7)(C) raised two concerns in allegation (b)(7)(E). The first pertained to the method in which Hatch (b)(7)(C) ordered (b)(7)(C) to input supply (b)(7)(C).

THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC. OIG.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/11

(b)(7)(C) chain tool room information into the plant's data system. (b)(7)(C) alleged that there was no logic in how management ordered (b)(7)(C) to number the data, which made it difficult to retrieve the information from the system. (b)(7)(C) also alleged that raising concerns such as (b)(7)(C) complaint about the data system led to a chilled work environment at Hatch.

OIG reviewed NRC allegation management system records for (b)(7)(E) and learned that NRC responded to both allegations. With regard to (b)(7)(C) first allegation, NRC inspectors were able to randomly select listings and retrieve the data. NRC inspectors agreed with (b)(7)(C) that the way in which the tools were identified was arbitrary and could lead to confusion; however, because they were still able to retrieve the data, they did not substantiate this part of (b)(7)(C) complaint. NRC inspectors reviewed the potential for a chilling effect at the site as well as safety conscious work environment (SCWE) issues. NRC inspectors substantiated that a potential chilling effect may have occurred. Inspectors did not identify any SCWE issues but stated they would continue to monitor the licensee.

OIG interviewed (b)(7)(C) Hatch electrician. (b)(7)(C) said there was a high intimidation factor from upper Hatch management. (b)(7)(C) sent a complaint to NRC Region II regarding the intimidation, and the NRC addressed (b)(7)(C) complaint; however, (b)(7)(C) did not notice a change in the work environment. (b)(7)(C) did not believe the current NRC resident inspectors socialized with licensee employees or management and saw no signs of collusion between plant management and NRC inspectors. According to (b)(7)(C) there is still a chilled work environment at Hatch, but the NRC was not the cause of the plant's problems.

OIG interviewed the inspector who conducted the onsite inspection into (b)(7)(C) concerns. (b)(7)(C) Plant Hatch, Region II, NRC, as well as (b)(7)(C) Division of Reactor Projects, Project Branch 2, Region II, NRC. Both confirmed that (b)(7)(C) was able to retrieve tool calibration data. Both (b)(7)(C) and (b)(7)(C) confirmed that there was never pressure from plant management to not have a finding regarding (b)(7)(C) allegation.

Because OIG did not substantiate that the NRC did not properly review (b)(7)(C) concerns, it is recommended this case be closed to the files of this office.



(b)(7)(C) was no logic in how management ordered [redacted] to number the data, which made it difficult to retrieve the information from the system. (b)(7)(C) also alleged that raising concerns such as [redacted] complaint about the data system led to a chilled work environment at Hatch.

OIG reviewed NRC allegation management system records for (b)(7)(E) and learned that NRC responded to both allegations. With regard to (b)(7)(C) first allegation, NRC inspectors were able to randomly select listings and retrieve the data. NRC inspectors agreed with (b)(7)(C) that the way in which the tools were identified was arbitrary and could lead to confusion; however, because they were still able to retrieve the data, they did not substantiate this part of (b)(7)(C) complaint. NRC inspectors reviewed the potential for a chilling effect at the site as well as safety conscious work environment (SCWE) issues. NRC inspectors substantiated that a potential chilling effect may have occurred. Inspectors did not identify any SCWE issues but stated they would continue to monitor the licensee.

OIG interviewed (b)(7)(C) Hatch electrician [redacted] said there was a high intimidation factor from upper Hatch management [redacted] sent a complaint to NRC Region II regarding the intimidation, and the NRC addressed [redacted] complaint; however, (b)(7)(C) did not notice a change in the work environment [redacted] did not believe the current NRC resident inspectors socialized with licensee employees or management and saw no signs of collusion between plant management and NRC inspectors. According to (b)(7)(C) there is still a chilled work environment at Hatch, but the NRC was not the cause of the plant's problems.

OIG interviewed the inspector who conducted the onsite inspection into (b)(7)(C) concerns. (b)(7)(C) Plant Hatch, Region II, NRC, as well as (b)(7)(C) Division of Reactor Projects, Project Branch 2, Region II, NRC. Both confirmed that (b)(7)(C) was able to retrieve tool calibration data. Both (b)(7)(C) and (b)(7)(C) confirmed that there was never pressure from plant management to not have a finding regarding (b)(7)(C) allegation.

Because OIG did not substantiate that the NRC did not properly review (b)(7)(C) concerns, it is recommended this case be closed to the files of this office.

Distribution

Document location: (b)(7)(E) [redacted]  
MAGIUM Case File: 12-54 Historical File

| OIG        | OIG       | OIG       | OIG       | OIG       | OIG       |
|------------|-----------|-----------|-----------|-----------|-----------|
| (b)(7)(C)  | (b)(7)(C) | (b)(7)(C) | (b)(7)(C) | (b)(7)(C) | (b)(7)(C) |
| J. McGowan | D. Lee    | H. Bell   |           |           |           |
| 2/11/13    | 5/1/91    | 2-19-113  | 2-12-117  | 2-12-117  | 2-12-117  |

Official File Copy



OFFICE OF THE  
INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~  
UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

February 20, 2013

MEMORANDUM TO:

Concur: Case Closed *Joseph A. McMillan*  
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

(b)(7)(C)

FROM:

(b)(7)(C)

SUBJECT:

REGION IV MISHANDLING OF CONCERNS REGARDING  
SAN ONOFRE NUCLEAR GENERATING STATION (OIG  
CASE NO. 012-55)

**Allegation**

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission, conducted this investigation in response to an allegation from (b)(7)(C) a former employee of San Onofre Nuclear Generating Station (SONGS), that NRC's Office of Investigations (OI) did not properly handle a discrimination claim against SONGS. According to (b)(7)(C) a licensee manager provided inaccurate and incomplete statements to OI during its investigation and OI took the testimony at face value without reviewing any evidence to show that the manager lied to OI. (b)(7)(C)

**Findings**

OIG did not substantiate (b)(7)(C) allegation that OI mishandled a discrimination claim. (b)(7)(C) OIG found that following OI's first investigation into the matter, which did not substantiate the discrimination claim, and in response to a second allegation from (b)(7)(C) concerning the matter, OI undertook a second review of the matter. OIG found that OI's second review specifically examined whether the licensee manager had provided inaccurate information during the first OI investigation and that OI took the additional measure of having a third party within OI review the testimony of the SONGS manager to assess if there was any willful intent to provide OI investigators with (b)(7)(C)

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE NRC OIG.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/12

inaccurate and incomplete statements. Neither of the follow-up OI reviews substantiated (b)(7)(C) claim nor did (b)(7)(C) provide any additional evidence to support his allegation against OI.

#### Basis of Findings

(b)(7)(C) former electrical engineer at SONGS, filed an allegation with Region IV in 2006 concerning electrical issues regarding breakers, cable ampacity, supervisors rubber stamping electrical calculations, and a claim of discrimination for raising these concerns. Region IV found the licensee in minor violation of (b)(7)(C) first concern. Because a prima facie case was established on the claim of discrimination, OI, Region IV, conducted an investigation but did not substantiate that employment discrimination occurred.

(b)(7)(C) OI opened another investigation concerning (b)(7)(C) in 2009 after (b)(7)(C) claimed that (b)(7)(C) supervisor had provided inaccurate and incomplete statements to OI investigators during their initial discrimination investigation in 2007. This allegation was also not substantiated by OI. According to OI's investigative report (b)(7)(C) was unable to present clear and convincing evidence that (b)(7)(C) supervisor had intentionally provided false statements. OIG's review of the relevant interview transcript in OI's second investigation indicated that the OI investigator covered the issues of concern as presented by (b)(7)(C)

In March 2011, after receiving additional emails from (b)(7)(C) claiming that OI investigators were taking testimony provided by (b)(7)(C) at face value, OI conducted a review of the testimonies that were provided to OI during the 2007 and 2009 investigations and determined that there was no evidence to suggest that a SONGS supervisor intentionally provided conflicting or inaccurate testimony.

OIG learned that (b)(7)(C) filed a discrimination complaint with the Department of Labor (DOL) on July 13, 2007, and on January 16, 2008, DOL ruled against (b)(7)(C)

OIG also learned that the licensee agreed to a settlement with (b)(7)(C) to avoid the cost associated with further pursuit of the matter. As a result of the settlement, (b)(7)(C) was no longer employed by SONGS.

(b)(7)(C) (b)(7)(C) stated that when (b)(7)(C) first contacted this office and claimed discrimination by NRC (b)(7)(C) had been mistaken and had intended to say that (b)(7)(C) was discriminated against by OI because (b)(7)(C) felt that they did not do an adequate job on (b)(7)(C) allegation of discrimination. After (b)(7)(C) discussed (b)(7)(C) issue with the Office of Small Business and Civil Rights, (b)(7)(C) realized that (b)(7)(C) was in error in claiming discrimination by OI.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

(b)(7)(C) (b)(7)(C) also stated that (b)(7)(C) was unaware that OI had conducted another investigation into (b)(7)(C) allegation that (b)(7)(C) had provided incomplete and inaccurate statements to OI.

Because OIG did not identify evidence to indicate that OI did not do an adequate job in investigating (b)(7)(C) allegation, it is recommended that this case be closed to the office files.

Distribution

File location (b)(7)(E)

Case File No. 12-55

Historical File

Magnum

| OIG/AIGI  | OIG/AIGI | OIG/AIGI | OIG/AIGI                 | OIG                  | OIG                 |
|-----------|----------|----------|--------------------------|----------------------|---------------------|
| (b)(7)(C) |          |          | <i>RE</i><br>J. McMillan | <i>del</i><br>D. Lee | H. Bell <i>H.B.</i> |
| 2-11/13   | 1 1      | 2-20/13  | 2-20/13                  | 2-21/13              | 2-25/13             |

Official File Copy

3

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE NRC OIG

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

## Referral, Actions & Follow-Up

Prepared by: (b)(7)(C)

Case Title: Misuse of Government Computer System To Engage in Sexually Explicit Chat Conversations Case Number: C 12 057

Program Office: (b)(7)(C) Classification: (b)(7)(E)

Origination Doclink: :  
Subject's Last Name / Company Name: (b)(7)(C)  
Subject's First Name: (b)(7)(C)

### Agency Referral & Follow-up

PFCRA Referral: Yes ☒ No  
Referred to Agency: ☒ Yes No Date: 04/24/2013

Action:  
Referred to (Office): Office of the Executive Director for Operations  
Contact Person: William Borchardt  
Follow-Up Assigned To: (b)(7)(C) NRC

Expected Completion Date: (b)(7)(C)  
Revised Completion Date:  
Actual Completion Date:  
Completion Status: Open ☒ Closed

Comments: ROI submitted and response requested. On August 15, 2013, EDO requested an extension to 10/31/13, which was provided. EDO requested another extension to 12/31/13, which was approved.

### Administrative Action

PFCRA: Accepted Declined Date:  
Agency Action: Resignation Date: 12/13/2013  
Comments: The employee elected to resign from Federal Service effective December 13, 2013, when informed that [redacted] was facing a possible removal action and a possible suspension of [redacted] security clearance. (b)(7)(C)

(b)(7)(C)

Agency Action Letter.pdf

### Prosecution Referral

A/13

~~OFFICIAL USE ONLY~~

Federal Referral Date:

Prosecution Status:

Pending  
Accepted  
Declined

Date:

AUSA Office:

State/Local Referral

Date:

Prosecution Status:

Pending  
Accepted  
Declined

Date:

Office:

Comments:

**LE/Judicial Action**

Actions:

Arrest  
Arraignment  
Charges Dropped  
Indictment  
Information

Date:

Date:

Date:

Date:

Date:

Jurisdiction:

Level

Statute(s)/

Violation(s):

Court Action:

Date:

Sentence:

Details:

Comments:

**Recoveries**

Amount Recovered:

Type:

Recovery Date:

Comments:

**Potential Losses**

Amount:

Description:

Comment:

Status: Open

Allow Other Editors:

Edit Authorization:  
(Management), (Inv Analyst),

~~OFFICIAL USE ONLY~~

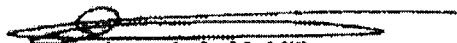


OFFICE OF THE  
INSPECTOR GENERAL

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~  
UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

April 24, 2013

MEMORANDUM TO: R. William Borchardt  
Executive Director for Operations

FROM:   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

SUBJECT: MISUSE OF GOVERNMENT COMPUTER TO ENAGAGE IN  
SEXUALLY EXPLICIT CHAT BY AN OFFICE OF  
ADMINISTRATION EMPLOYEE (OIG CASE NO. 12-57)

Attached is an Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), Report of Investigation pertaining to misuse of a Government computer to engage in sexually explicit chat by an Office of Administration employee.

This report is furnished for whatever action you deem appropriate. Please notify this office within 120 days of what action you take based on the results of this investigation. Contact this office if further assistance is required.

The distribution of this report should be limited to those NRC managers required for evaluation of this matter. Neither the Report of Investigation nor its exhibits may be placed in ADAMS without OIG's written permission.

Attachment: Report of Investigation w/ exhibits

cc: (b)(7)(C) ADM/DFS/PSB w/o exhibits

CONTACT: (b)(7)(C) OIG

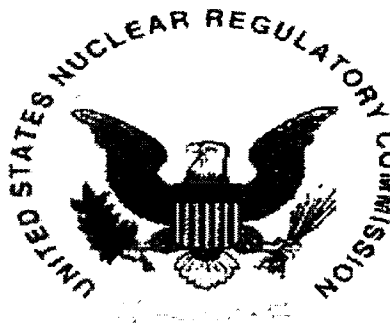
THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

A/14

OFFICE OF THE INSPECTOR GENERAL

Report of Investigation



Misuse of Government Computer to  
Engage in Sexually Explicit Chat by an  
Office of Administration Employee

(b)(7)(C)

Case No. 12-57

(b)(7)(C)

  
Joseph A. McMillan, Assistant Inspector General  
for Investigations

4/22/13  
Date

THIS REPORT IS RELEASABLE ONLY BY THE U.S. NUCLEAR REGULATORY  
COMMISSION, OFFICE OF THE INSPECTOR GENERAL.

THIS REPORT OR ITS EXHIBITS MAY NOT BE PLACED IN ADAMS WITHOUT  
WRITTEN PERMISSION OF THE NRC OIG.  
EXEMPT FROM RELEASE UNDER FREEDOM OF INFORMATION ACT  
EXEMPTIONS (5), (6) OR (7) AND PRIVACY ACT EXEMPTIONS (j)(2) OR (k)(1)

THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED  
OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.



~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

**Misuse of Government Computer to  
Engage in Sexually Explicit Chat by an  
Office of Administration Employee**

**Case No. 12-57**

**April 24, 2013**

---

THIS DOCUMENT IS THE PROPERTY OF THE NRC. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED  
OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE OFFICE OF THE INSPECTOR GENERAL.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

TABLE OF CONTENTS

|  | <u>PAGE</u> |
|--|-------------|
| STATUTES, REGULATIONS, AND POLICY..... | 1           |
| SUBJECT.....                           | 3           |
| ALLEGATION .....                       | 3           |
| FINDINGS.....                          | 3           |
| BASIS FOR FINDINGS.....                | 4           |
| EXHIBITS.....                          | 7           |

**STATUTES, REGULATIONS, AND POLICY**

**5 CFR Part 2635.101, Basic Obligation of Public Service**

(b) *General Principles.* The following general principles apply to every employee and may form the basis for the standards contained in this part. Where a situation is not covered by the standards set forth in this part, employees shall apply the principles set forth in this section in determining whether their conduct is proper.

(5) Employees shall put forth honest effort in the performance of their duties.

(9) Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.

**5 CFR, Sec. 2635.704 - Use of Government Property**

(a) An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes.

(b) Government property includes any form of real or personal property in which the Government has an ownership, leasehold, or other property interest as well as any right or other intangible interest that is purchased with Government funds, including the services of contractor personnel. The term includes office supplies, telephone and other telecommunications equipment and services, the Government mails, automated data processing capabilities, printing and reproduction facilities, Government records, and Government vehicles.

(c) Authorized purposes are those purposes for which Government property is made available to members of the public or those purposes authorized in accordance with law or regulation.

**NRC Management Directive and Handbook 12.5, "NRC Automated Information Security Program," Part 2**

**2.6.5 Use of the Internet**

NRC staff may use the NRC LAN/WAN to access the Internet. This access may be for official business or personal business in accordance with the NRC minimum personal use policy in MD 2.7. When using the Internet, users shall practice "safe surfing." Specifically, users shall—

- Avoid accessing pornographic or other sites that provide content that is incompatible with the NRC work environment. NRC uses software to block access to sites that provide content that is incompatible with the NRC work environment or that might present a security risk. These sites offer content relating to criminal skills, gambling,

hate speech, and pornography or other sexually oriented material. These sites are blocked on the basis of a characterization by the commercial provider of the blocking software, not an analysis of the site content. Thus, other sites may provide similar content but are not blocked. It is the user's responsibility to avoid such sites and to immediately terminate access to such sites that are reached unintentionally.

**NRC Management Directive 2.7, "Personal Use of Information Technology,"  
Handbook Section (D), "Inappropriate Personal Uses":**

Employees are expected to conduct themselves professionally in the workplace and to refrain from using agency information technology for activities that are inappropriate. Misuse or inappropriate personal use of agency information technology includes -

Use of agency information technology for activities that are illegal, inappropriate, or construed as justifiably offensive to fellow employees or the public.

Use of information technology, including telephone or facsimile service, to create, download, view, store, copy, transmit, or receive sexually explicit or sexually oriented materials...

**SUBJECT**

(b)(7)(C)

Division of Contracts (DC)  
Office of Administration (ADM)  
U.S. Nuclear Regulatory Commission (NRC)

**ALLEGATION**

The Office of the Inspector General (OIG), NRC, initiated this investigation based on a proactive effort to identify instances of misuse of NRC computer resources to view sexually explicit or sexually oriented materials. During this proactive effort, OIG identified a computer on the NRC network that was used to connect to the Web site ABFSingles.net on June 7, 2012. While on this Web site, the user of the computer was identified as engaging in sexually explicit conversations with other members of the Web site. The NRC computer was assigned to (b)(7)(C)

**FINDINGS**

OIG found that based on a review of Internet proxy logs for the periods of May 29, 2012 to June 19, 2012, September 24, 2012 to October 4, 2012, and December 6 to 17, 2012 (b)(7)(C) used NRC computer to engage in sexually explicit chat conversations on May 29 – 31, June 4, 6, 7, and 18, September 24 – 27, 2012, and December 8, 11, 12, 13, and 17, 2012, on the Web site ABFSingles.net.

(b)(7)(C) admitted to OIG that (b)(7)(C) visited the Web site ABFSingles.net and had been corresponding with (b)(7)(C) from (b)(7)(C) work computer in a manner that could be construed as sexual in nature for 6 or 7 months prior to (b)(7)(C) interview with OIG on December 18, 2012, and that (b)(7)(C) last visited the ABFSingles.net Web site from (b)(7)(C) Government computer on December 17, 2012.

**BASIS FOR FINDINGS**

Review of Information Identified on (b)(7)(E)

The OIG Cyber Crime Unit (CCU) conducted a proactive examination of the NRC (b)(7)(E) on June 20, 2012, for instances of misuse of NRC computer resources and identified an NRC computer that was used to connect to the Web site ABFSingles.net on June 7, 2012. The CCU identified that the computer user engaged in sexually explicit chat conversations with others on that Web site at approximately 8:42 a.m. and 12:06 p.m. This activity originated from an NRC computer with Internet Protocol address (b)(7)(C). A Domain Name Server lookup identified this computer's asset tag number as (b)(7)(C). OIG identified this computer as assigned to (b)(7)(C).

Based on a review of (b)(7)(E) for the periods of May 29, 2012, to June 19, 2012, September 24, 2012 to October 4, 2012, and December 6 to 17, 2012, OIG identified that (b)(7)(C) NRC computer was used to engage in sexually explicit chat conversations over the ABFSingles.net Web site during multiple daytime hours on May 29-31, 2012; June 4, 6, 7, and 16, 2012; September 24-27, 2012; and December 6, 11, 12, 13, and 17, 2012. OIG noted that in the May/June timeframe, the majority of the explicit chat conversations occurred on May 30 from 11:25 a.m. to 4 p.m.; June 4 from 11:30 a.m. to 4:11 p.m.; and June 6 from 8:36 a.m. to 3:50 p.m. In the September timeframe, the majority of explicit chat conversations occurred on September 24 from 10:37 a.m. to 4:58 p.m. and on September 25 from 10:44 a.m. to 5:29 p.m. In December, the majority of the chat communication occurred on December 13, 2012, from 8:57 a.m. to 6:30 p.m.

(For further details, see Exhibits 1, 2, 3, 4, and 5.)

Review of NRC Computer Assigned to (b)(7)(C)

OIG CCU forensically imaged the hard drive of the NRC computer bearing NRC Asset Tag (b)(7)(C) assigned to (b)(7)(C). CCU found no pertinent additional information residing on the computer related to this investigation.

(For further details, see Exhibit 6.)

Interview of (b)(7)(C)

(b)(7)(C) DC, ADM, stated that (b)(7)(C) noticed a decline in (b)(7)(C) work performance as (b)(7)(C) received an "Excellent" for (b)(7)(C) 2011 rating period, but received a "Fully Successful" for 2012 rating period. (b)(7)(C) related that (b)(7)(C) needs to make better use of (b)(7)(C) time. (b)(7)(C) said that (b)(7)(C) is slow to return telephone (b)(7)(C)

(b)(7)(C) calls and respond to e-mails, and (b)(7)(C) uses (b)(7)(C) personal phone frequently during the  
(b)(7)(C) workday. (b)(7)(C) said (b)(7)(C) has received negative feedback from customers concerning  
(b)(7)(C) and that (b)(7)(C) is the "weakest" performer in the office.

(For further details, see Exhibit 7.)

Interview of (b)(7)(C)

(b)(7)(C) (b)(7)(C) told OIG that (b)(7)(C) had been using (b)(7)(C) work computer to correspond with (b)(7)(C)  
(b)(7)(C) on an adult breast feeding Web site called ABFSingles.net for 6 or 7 months  
(b)(7)(C) prior to (b)(7)(C) OIG interview on December 18, 2012. (b)(7)(C) could not recall exactly when  
it began, but said, "It's been going on for a while. And it's not a daily...." (b)(7)(C) said (b)(7)(C) (b)(7)(C)  
would "talk and then nothing happens and a few weeks later or it could be a month later  
or two months later, we make contact again." (b)(7)(C) said (b)(7)(C) used the Web site to  
correspond by e-mail and chat conversations, and that (b)(7)(C) chat conversations could be  
"construed as sexual in nature." (b)(7)(C) stated that approximately a year ago while (b)(7)(C)  
(b)(7)(C) was on "TDY" travel, (b)(7)(C) met up with a woman that (b)(7)(C) chattered with on the  
(b)(7)(C) ABFSingles.net Web site. (b)(7)(C) said that (b)(7)(C) last visited the ABFSingles.net Web site  
(b)(7)(C) from (b)(7)(C) Government computer on December 17, 2012, a day prior to (b)(7)(C) interview with  
OIG.

(b)(7)(C) (b)(7)(C) said that going to ABFSingles.net website started while (b)(7)(C) was (b)(7)(C) (b)(7)(C)  
(b)(7)(C) and (b)(7)(C) believes it has become a problem. (b)(7)(C) related that (b)(7)(C) is an (b)(7)(C)  
(b)(7)(C) and (b)(7)(C) believes (b)(7)(C) behavior can possibly (b)(7)(C)  
(b)(7)(C) be a security risk. (b)(7)(C) said (b)(7)(C) is currently in counseling for this problem and  
consults with a therapist. Through counseling and therapy sessions, (b)(7)(C) stated  
(b)(7)(C) that (b)(7)(C) behavior could be an addiction. (b)(7)(C) said (b)(7)(C) used to believe (b)(7)(C) could stop at  
anytime, however, stopping has been a challenge for (b)(7)(C) (b)(7)(C)

(b)(7)(C) (b)(7)(C) acknowledged that (b)(7)(C) work has suffered" as a (b)(7)(C)  
(b)(7)(C) because of the time (b)(7)(C) spends on the ABFSingles.net Web site. In addition, (b)(7)(C)  
explained that at one point everything seemed to be derailing, and (b)(7)(C)  
because (b)(7)(C) was afraid of the consequences which could be life altering.

(b)(7)(C) requested to have the ABFSingles.net Web site blocked.<sup>2</sup>

(For further details, see Exhibit 8.)

<sup>1</sup> Following the interview with OIG, (b)(7)(C) provided OIG medical and therapy documentation.

<sup>2</sup> On December 18, 2012, OIG requested that CSO block the Web site ABFSingles.com. That same day, CSO confirmed that OIG blocked both URL and IP access to the Web site.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

Coordination with the

(b)(7)(C)

OIG coordinated this investigation with Special Agent  
Office of Special Investigations based on

(b)(7)(C)

(b)(7)(C)

indication that

was an

(b)(7)(C)

(b)(7)(C)

(b)(7)(C)



EXHIBITS

1. Memorandum to File, Misuse of Government Computer to Engage in Explicit Chat Conversations, dated July 3, 2012.
2. Memorandum to File, Review of Chat Conversations, dated October 19, 2012.
3. Memorandum to File, Misuse of Government Computer to Engage in Explicit Chat Conversations, dated October 19, 2012.
4. Memorandum to File, Review of Chat Conversations, dated December 4, 2012.
5. Memorandum to File, Review of Chat Conversations, dated January 7, 2013.
6. Memorandum to File, Forensic Preliminary Review of NRC Computer Asset Tag No. (b)(7)(C) dated January 8, 2013.
7. Memorandum of Interview, (b)(7)(C) dated December 20, 2012.
8. Transcript of Interview (b)(7)(C) dated December 18, 2012.

MEMORANDUM TO: R. William Borchardt  
Executive Director for Operations

FROM: Joseph A. McMillan /RA/  
Assistant Inspector General  
for Investigations

SUBJECT: MISUSE OF GOVERNMENT COMPUTER TO ENAGAGE IN  
SEXUALLY EXPLICIT CHAT BY AN OFFICE OF  
ADMINISTRATION EMPLOYEE (OIG CASE NO. 12-57)

Attached is an Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), Report of Investigation pertaining to misuse of a Government computer to engage in sexually explicit chat by an Office of Administration employee.

This report is furnished for whatever action you deem appropriate. Please notify this office within 120 days of what action you take based on the results of this investigation. Contact this office if further assistance is required.

The distribution of this report should be limited to those NRC managers required for evaluation of this matter. Neither the Report of Investigation nor its exhibits may be placed in ADAMS without OIG's written permission.

Attachment: Report of Investigation w/ exhibits

cc: (b)(7)(C) ADM/DFS/PSB w/o exhibits

CONTACT: (b)(7)(C) OIG

Case File 12-57 Historical File MAGNUM

| OIG       | OIG       | OIG       | OIG         | OIG     | OIG     |
|-----------|-----------|-----------|-------------|---------|---------|
| (b)(7)(C) | (b)(7)(C) | (b)(7)(C) | J. McMillan | D. Lee  | H. Bell |
| 2/12/13   | 2/12/13   | 2/12/13   | 2/22/13     | 3/24/13 | 3/24/13 |

Official File Copy

**RESPONSE TO FREEDOM OF  
INFORMATION ACT (FOIA) / PRIVACY  
ACT (PA) REQUEST**

2014-0329 - Revised

2

RESPONSE  
TYPE

FINAL



PARTIAL

REQUESTER

DATE

SEP 25 2014

**PART I. -- INFORMATION RELEASED**

- ☐ No additional agency records subject to the request have been located.
- ☐ Requested records are available through another public distribution program. See Comments section.
- ☐

|       |
|-------|
| GROUP |
|-------|

 Agency records subject to the request that are identified in the specified group are already available for public inspection and copying at the NRC Public Document Room.
- ☐

|       |
|-------|
| GROUP |
|-------|

 Agency records subject to the request that are contained in the specified group are being made available for public inspection and copying at the NRC Public Document Room.
- ☒

|       |
|-------|
| GROUP |
| C     |

 Agency records subject to the request are enclosed.
- ☐ Records subject to the request that contain information originated by or of interest to another Federal agency have been referred to that agency (see comments section) for a disclosure determination and direct response to you.
- ☐ We are continuing to process your request.
- ☐ See Comments.

**PART I.A -- FEES**

AMOUNT\*

\$

0



You will be billed by NRC for the amount listed.



None. Minimum fee threshold not met.



You will receive a refund for the amount listed.



Fees waived.

\* See comments  
for details**PART I.B -- INFORMATION NOT LOCATED OR WITHHELD FROM DISCLOSURE**

- ☐ No agency records subject to the request have been located. For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.
- ☒ Certain information in the requested records is being withheld from disclosure pursuant to the exemptions described in and for the reasons stated in Part II.
- ☒ This determination may be appealed within 30 days by writing to the FOIA/PA Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001. Clearly state on the envelope and in the letter that it is a "FOIA/PA Appeal."

**PART I.C COMMENTS ( Use attached Comments continuation page if required)**

it came to our attention that we provided you everything you had requested in our interim release number 1 and the final release number 2, except for the following, which are being provided with this revision.

C 10-012  
C 10-018  
C 11-038  
C 11-042

SIGNATURE - ASSISTANT INSPECTOR GENERAL

Joseph McMillan



# RESPONSE TO FREEDOM OF INFORMATION ACT (FOIA) / PRIVACY ACT (PA) REQUEST

DATE

SEP 25 2014

## PART II.A -- APPLICABLE EXEMPTIONS

GROUP

C

Records subject to the request that are contained in the specified group are being withheld in their entirety or in part under the Exemption No.(s) of the PA and/or the FOIA as indicated below (5 U.S.C. 552a and/or 5 U.S.C. 552(b)).

- ☐ Exemption 1: The withheld information is properly classified pursuant to Executive Order 12958.
- ☐ Exemption 2: The withheld information relates solely to the internal personnel rules and practices of NRC.
- ☐ Exemption 3: The withheld information is specifically exempted from public disclosure by statute indicated.
- ☐ Sections 141-145 of the Atomic Energy Act, which prohibits the disclosure of Restricted Data or Formerly Restricted Data (42 U.S.C. 2161-2165).
- ☐ Section 147 of the Atomic Energy Act, which prohibits the disclosure of Unclassified Safeguards Information (42 U.S.C. 2167).
- ☐ 41 U.S.C., Section 4702(b), prohibits the disclosure of contractor proposals in the possession and control of an executive agency to any person under section 552 of Title 5, U.S.C. (the FOIA), except when incorporated into the contract between the agency and the submitter of the proposal.
- ☐ Exemption 4: The withheld information is a trade secret or commercial or financial information that is being withheld for the reason(s) indicated.
- ☐ The information is considered to be confidential business (proprietary) information.
- ☐ The information is considered to be proprietary because it concerns a licensee's or applicant's physical protection or material control and accounting program for special nuclear material pursuant to 10 CFR 2.390(d)(1).
- ☐ The information was submitted by a foreign source and received in confidence pursuant to 10 CFR 2.390(d)(2).
- ☐ Disclosure will harm an identifiable private or governmental interest.
- ☐ Exemption 5: The withheld information consists of interagency or intraagency records that are not available through discovery during litigation. Applicable privileges:
- ☐ Deliberative process: Disclosure of predecisional information would tend to inhibit the open and frank exchange of ideas essential to the deliberative process. Where records are withheld in their entirety, the facts are inextricably intertwined with the predecisional information. There also are no reasonably segregable factual portions because the release of the facts would permit an indirect inquiry into the predecisional process of the agency.
- ☐ Attorney work-product privilege. (Documents prepared by an attorney in contemplation of litigation)
- ☐ Attorney-client privilege. (Confidential communications between an attorney and his/her client)
- ☐ Exemption 6: The withheld information is exempted from public disclosure because its disclosure would result in a clearly unwarranted invasion of personal privacy.
- ☒ Exemption 7: The withheld information consists of records compiled for law enforcement purposes and is being withheld for the reason(s) indicated.
- ☐ (A) Disclosure could reasonably be expected to interfere with an enforcement proceeding (e.g., it would reveal the scope, direction, and focus of enforcement efforts, and thus could possibly allow recipients to take action to shield potential wrong doing or a violation of NRC requirements from investigators).
- ☒ (C) Disclosure could constitute an unwarranted invasion of personal privacy.
- ☐ (D) The information consists of names of individuals and other information the disclosure of which could reasonably be expected to reveal identities of confidential sources.
- ☒ (E) Disclosure would reveal techniques and procedures for law enforcement investigations or prosecutions, or guidelines that could reasonably be expected to risk circumvention of the law.
- ☐ (F) Disclosure could reasonably be expected to endanger the life or physical safety of an individual.
- ☐ OTHER (Specify)

## PART II.B -- DENYING OFFICIALS

Pursuant to 10 CFR 9.25(g), 9.25(h), and/or 9.65(b) of the U.S. Nuclear Regulatory Commission regulations, it has been determined that the information withheld is exempt from production or disclosure, and that its production or disclosure is contrary to the public interest. The person responsible for the denial are those officials identified below as denying officials and the FOIA/PA Officer for any denials that may be appealed to the Executive Director for Operations (EDO).

| DENYING OFFICIAL   | TITLE/OFFICE                     | RECORDS DENIED | APPELLATE OFFICIAL       |                          |                                     |
|--------------------|----------------------------------|----------------|--------------------------|--------------------------|-------------------------------------|
|                    |                                  |                | EDO                      | SECY                     | IG                                  |
| Joseph A. McMillan | Assistant Inspector General, OIG |                | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
|                    |                                  |                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            |
|                    |                                  |                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            |

Appeal must be made in writing within 30 days of receipt of this response. Appeals should be mailed to the FOIA/Privacy Act Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, for action by the appropriate appellate official(s). You should clearly state on the envelope and letter that it is a "FOIA/PA Appeal."



OFFICE OF THE  
INSPECTOR GENERAL

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

September 25, 2013

MEMORANDUM TO: Concur: Case Closed [Signature]  
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

FROM:

(b)(7)(C)

SUBJECT: SPECIAL PROJECT: NRC REGULATORY OVERSIGHT  
(OIG CASE NO. 010-12)

**Recommendation**

This project is being closed and a new project with the same objectives has been reopened in fiscal year 2013.

**Project Conclusion**

This project was initiated in January 2010 as a mechanism to identify potential investigative matters associated with NRC technical and regulatory oversight where individual misconduct was not identified as a concern. Over the course of this project a number of technical issues were evaluated, to include the following issues:

- Inaccurate information provided to Congressional Representative pertaining to a condensate storage tank return pipe leak at the Indian Point Unit 2 (b)(7)(E)
- A 2.206 petition submitted by Pilgrim Watch pertaining to inaccessible cables and wiring at the Pilgrim nuclear power plant (b)(7)(E)
- A 2.206 petition pertaining to a tritium leak at the Vermont Yankee power plant (b)(7)(E)

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.

c/1

- Misleading information in the Fukushima Near-term Task Force Report pertaining to potassium iodide (b)(7)(E)
- Veracity of Region I public affairs officer statement pertaining to release of tritium at Oyster Creek Generating Station (b)(7)(E)
- Incorrect NRC Mid-cycle assessment letter pertaining to Fort Calhoun (b)(7)(E)
- A 2.206 petition regarding General Electric Mark I nuclear power plants and plants located on or near an earthquake fault line (b)(7)(E)

In addition, one investigation (b)(7)(E) was initiated into whether the NRC Office of Federal and State Materials and Environmental Programs (FSME) had, in official correspondence, mischaracterized positions taken by the Colorado Department of Public Health and the Environment (CDPHE), the State level nuclear regulator in the Agreement State of Colorado. The OIG found that while certain FSME correspondence incorrectly implied that NRC had drawn conclusions about the adequacy of CDPHE's compliance with its legal requirements, FSME subsequently provided clarifying correspondence to address the concerns of CDPHE.

Finally, during the course of this project a number of issues were monitored for potential development of allegations but did not necessarily cross the threshold for an allegation, investigation, or a project.

- Misleading information in the Fukushima Near-term Task Force Report pertaining to potassium iodide (b)(7)(E)
- Veracity of Region I public affairs officer statement pertaining to release of tritium at Oyster Creek Generating Station (b)(7)(E)
- Incorrect NRC Mid-cycle assessment letter pertaining to Fort Calhoun (b)(7)(E)
- A 2.206 petition regarding General Electric Mark nuclear power plants and plants located on or near an earthquake fault line (b)(7)(E)

In addition, one investigation (b)(7)(E) was initiated into whether the NRC Office of Federal and State Materials and Environmental Programs (FSME) had, in official correspondence, mischaracterized positions taken by the Colorado Department of Public Health and the Environment (CDPHE), the State level nuclear regulator in the Agreement State of Colorado. The OIG found that while certain FSME correspondence incorrectly implied that NRC had drawn conclusions about the adequacy of CDPHE's compliance with its legal requirements, FSME subsequently provided clarifying correspondence to address the concerns of CDPHE.

Finally, during the course of this project a number of issues were monitored for potential development of allegations but did not necessarily cross the threshold for an allegation, investigation, or a project.

Distribution:

File Location:

(b)(7)(E)

Case No. 10-12

Historical File

Magnum

|           |             |        |         |
|-----------|-------------|--------|---------|
| (b)(7)(C) | OIG/AIGI    | OIG    | OIG     |
|           | J. McMillan | D. Lee | H. Bell |
| 925113    | 925113      | 925113 | 74613   |

Official File Copy

2

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20565-0001

OFFICE OF THE  
INSPECTOR GENERAL

August 20, 2013

MEMORANDUM TO: Concur: Case Closed [Signature]  
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

(b)(7)(C)

Team Leader

(b)(7)(C)

FROM:

(b)(7)(C)  
Special Agent, (b)(7)(C)

SUBJECT: PROACTIVE INITIATIVE: TRANSIT SUBSIDY BENEFITS  
PROGRAM MISUSE (OIG CASE 11-38)

**Project**

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), initiated a proactive initiative in April 2011 to identify instances of Transit Subsidy Benefits Program (TSBP) misuse within NRC.

**Finding**

From April 2011 – December 2012, OIG conducted four investigations pertaining to potential misuse of the TSBP by four NRC employees. All four investigations substantiated misuse of the TSBP. As a result of each OIG investigation, the agency took administrative action against the employee.

**Basis for Findings:**

Over the course of the proactive project, OIG completed four investigations stemming from allegations of TSBP misuse. The following are summaries of the investigations.

- (b)(7)(E) This investigation involved an NRC employee who used the TSBP to pay for parking both at a Metro station when (b)(7)(C) took the train to and from work, and at the White Flint Metro station when (b)(7)(C) drove (b)(7)(C) privately owned vehicle (POV) to work and parked at the station. This investigation was referred for Program Fraud Civil Remedies Act (PFCRA) action. The subject received a 30 day-suspension and paid back \$2,409.50 of restitution.

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.



- (b)(7)(E) [redacted] This investigation involved an NRC employee who used the TSBP to pay for parking of (b)(7)(C) [redacted] POV at the White Flint Metro station. The subject received an alternate disciplinary agreement in lieu of a 3-day suspension.
- (b)(7)(E) [redacted] This investigation involved an NRC employee who used the TSBP to pay for parking both at a Metro station when (b)(7)(C) [redacted] took the train to and from work and at the White Flint Metro station when (b)(7)(C) [redacted] drove (b)(7)(C) [redacted] POV to work and parked at the station. This investigation was referred for PFCRA action. The subject received a 21-day suspension.
- (b)(7)(E) [redacted] This investigation involved an NRC employee who used the TSBP to pay for parking primarily at the White Flint Metro station when (b)(7)(C) [redacted] drove (b)(7)(C) [redacted] POV to work and parked at the station. This investigation was referred for PFCRA action. The subject was removed from the agency.

OIG learned that in October 2011, Metro's SmartBenefits program initiated steps to comply with the Internal Revenue Service's (IRS) requirement to separate parking and transit subsidy benefits to restrict comingled use. This change automatically separates transit subsidy funds from parking funds.

Based on the fact that this project met its objective of identifying TSBP misuse and that Metro complied with IRS requirements ensuring transit subsidy funds could no longer be comingled with parking funds, it is recommended this project be closed to the files of this office.

- (b)(7)(E) This investigation involved an NRC employee who used the TSBP to pay for parking of (b)(7)(C) POV at the White Flint Metro station. The subject received an alternate disciplinary agreement in lieu of a 3-day suspension.
- (b)(7)(E) This investigation involved an NRC employee who used the TSBP to pay for parking both at a Metro station when (b)(7)(C) took the train to and from work and at the White Flint Metro station when (b)(7)(C) drove (b)(7)(C) POV to work and parked at the station. This investigation was referred for PFCRA action. The subject received a 21-day suspension.
- (b)(7)(E) This investigation involved an NRC employee who used the TSBP to pay for parking primarily at the White Flint Metro station when (b)(7)(C) drove (b)(7)(C) POV to work and parked at the station. This investigation was referred for PFCRA action. The subject was removed from the agency.

OIG learned that in October 2011, Metro's SmartBenefits program initiated steps to comply with the Internal Revenue Service's (IRS) requirement to separate parking and transit subsidy benefits to restrict comingled use. This change automatically separates transit subsidy funds from parking funds.

Based on the fact that this project met its objective of identifying TSBP misuse and that Metro complied with IRS requirements ensuring transit subsidy funds could no longer be comingled with parking funds, it is recommended this project be closed to the files of this office.

File Location: (b)(7)(E)

Distribution

Case File 11-38

Historical File

Magnum

|           |         |         |     |                        |                           |                            |
|-----------|---------|---------|-----|------------------------|---------------------------|----------------------------|
| (b)(7)(C) |         |         |     | OIG <i>[Signature]</i> | OIG                       | OIG                        |
|           |         |         |     | J. McMillan            | D. Lee <i>[Signature]</i> | H. Bell <i>[Signature]</i> |
| For       | 8/20/13 | 8/20/13 | 1/1 | 8/20/13                | 8/20/13                   | 8/20/13                    |

Official File Copy



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

OFFICE OF THE  
INSPECTOR GENERAL

August 27, 2013

MEMORANDUM TO: Mark Satorius  
Executive Director for Operations

FROM:  (b)(7)(C)  
Joseph P. McMillan  
Assistant Inspector General  
for Investigations

SUBJECT: INVESTIGATION OF FOREIGN ASSIGNEE SECURITY  
PROCESS (OIG CASE NO. 11-042)

**Allegation**

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), initiated this investigation subsequent to learning, through activities conducted in support of OIG (b)(7)(E) that the NRC may not be coordinating with external agencies as required by agency guidance on the foreign assignee security process. OIG examined whether NRC was meeting requirements identified in relevant Management Directive 12.3, *NRC Personnel Security Program* and SECY-05-0142, "Update on the NRC Foreign Assignee Program," as amended or superseded by policy guidance.

**Findings**

OIG found that the Division of Facilities and Security (DFS), Office of Administration, is currently coordinating with the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and State Department as suggested in Management Directive (MD) 12.3, *NRC Personnel Security Program*, prior to approving foreign assignees for temporary assignments at NRC. However, under the direction of the prior DFS program manager, DFS was not coordinating with the State Department from approximately November 2010 through May 2012. OIG informed DFS and Office of International Programs managers responsible for foreign assignee security of several observations concerning enforceability of individual assignee security plan requirements and suggested a program enhancement to permit foreign assignees to store prohibited items such as cell phones at the agency entry point.

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.

### **Basis of Findings**

NRC accepts assignees from international regulatory authorities consistent with the U.S. policy and formal agreements, developed by the Office of International Programs (OIP), between NRC and the sponsoring country or the International Atomic Energy Agency. The primary purpose of each assignment is to transfer to the assignee the NRC office expertise in the chosen regulatory area. The second purpose involves the exchange of expertise that benefits NRC.

For the past 24 months, headquarters NRC has averaged 10 foreign assignees onsite, normally for terms of 3 to 12 months dependent on the subject matter of exchange. During FY 2011, the following countries participated in the headquarters NRC Foreign Assignee Program: China, France, Germany, Japan, Spain, Pakistan, and Republic of Korea. A majority of the FY 2011 exchanges were for 12-months; France was an anomaly with a 3-year assignee rotating in different program offices. The Office of Nuclear Reactor Regulation and Office of New Reactors hosted approximately 80 percent of the assignees; the remaining 20 percent were hosted nearly equally by the Office of Nuclear Regulatory Research, Office of Nuclear Material Safety and Safeguards, and Office of Federal and State Materials and Environmental Management Programs. The same headquarters NRC program offices, with nearly identical distributions, hosted 14 foreign assignees in FY 2012 from the following countries: China, Czech Republic, France, Germany, Indonesia, Pakistan, Republic of Korea, Spain, and the United Arab Emirates.

### **Overview of Significant Steps in the Security Process**

- OIP, in cooperation with the DFS Facilities Security Branch (FSB), serves as coordinator of the Foreign Assignee Program. Initial OIP screening establishes the applicant is fluent in English, technically competent, able to contribute to the work of the NRC, and is a regular employee of a government or quasi-government organization with a regulatory/safety role.
- OIP consults with the appropriate program office(s) to determine if (1) the proposed assignee's experience, training objectives, and language skills make him/her suitable for placement in one of the technical branches, and (2) the organizational unit can reasonably integrate the proposed assignee into its work activities.
- If the decision is made to proceed with an incoming application, OIP works with the proposed program office and DFS to facilitate the screening and placement of the foreign national pending a favorable indices check. (b)(7)(E)

(b)(7)(E)

~~—OFFICIAL USE ONLY—OIG INVESTIGATION INFORMATION—~~

(b)(7)(E)

THIS DOCUMENT IS THE PROPERTY OF THE NRC OIG. IF LOANED TO ANOTHER AGENCY IT AND ITS CONTENTS ARE NOT TO BE REPRODUCED OR  
DISTRIBUTED OUTSIDE THE RECEIVING AGENCY WITHOUT THE PERMISSION OF THE NRC OIG.

~~—OFFICIAL USE ONLY—OIG INVESTIGATION INFORMATION—~~

(b)(7)(E)

Interview of (b)(7)(C)

OIG learned in June 2012 the current (b)(7)(C) formalized procedures for security processing of foreign visitors by creating an office instruction that provides sequential processing steps for FSB and OIP personnel coordinating a foreign assignee training request. This DFS Office Instruction, titled, *Unclassified Visits for Foreign Trainees*, incorporated the NRC headquarters broader Management Directive (MD) guidance for headquarters foreign assignee visits. MD 12.3, *NRC Personnel Security Program*, did not specify all visits with regard to indices vetting of visitors to regions or licensed facilities. The (b)(7)(C) said that without more detailed instructions, it could not be determined whether every foreign visitor to an NRC licensed facility was properly vetted previously. This office instruction provides processing guidance for all foreign visitors, including foreign assignees to headquarters or the regions, or licensed facility, to ensure foreign visitors are vetted with indices checks prior to approval of travel. The (b)(7)(C) confirmed a training folder is created and maintained by the FSB on each foreign assignee documenting compliance with the indices checks and security plan requirements.

OIG learned the (b)(7)(C) did not coordinate indices checks with the State Department from approximately November 2010 to May 2012 but was coordinating with the FBI and CIA. The (b)(7)(C) explained a (b)(7)(C) recommended to forego the State Department indices check because it excessively delayed the screening process of foreign assignees. The (b)(7)(C) acknowledged the management directive suggests a State Department check should be accomplished. The (b)(7)(C) could not produce a written recommendation from the review team.

[Investigative Note: OIG learned from the (b)(7)(C) Office of the Executive Director for Operations, that no (b)(7)(C) effort addressed specifically the foreign assignee security process. Efforts started a couple of times to address contractor access to the NRC complex and the (b)(7)(C) started to look at what requirements and indices checks were required for contractor unescorted access in late 2010. During this period foreign assignee requirements were discussed, but neither a full review nor written product was accomplished.]

OIG reviewed DFS documentation for nine current assignees and noted responses for (b)(7)(E) were maintained and security plans were on file for each assignee.

7E

Interview of (b)(7)(C)

The (b)(7)(C) told OIG that the NRC security process for foreign assignees has not changed much in the last 15 years that (b)(7)(C) has managed the program. In fact, no foreign assignee has been assigned without completed background checks during (b)(7)(C) tenure. Key aspects of the program are designed to ensure the assignees have no LAN access to NRC systems. (b)(7)(E)

(b)(7)(E)

The (b)(7)(C) highlighted if assignees need information from the NRC Technical Library, information is collected for the assignee on a per use basis limited to the specific topic of the task the assignee is working on.

Interviews of (b)(7)(C)

OIG interviewed (b)(7)(C) and neither reported any concerns with the assignees violating their security plans. If the assignee needs documents or information not available to them through public access channels, they will request the information from the supervisor. (b)(7)(C) requires all information requests be in writing.

(b)(7)(C) said that personnel working in close proximity to foreign assignees are briefed by the supervisors of the assignees of the security plan requirements and to be sensitive to the assignees' presence regarding security of sensitive information through the use of locked storage cabinets/safes and to use a designated room when using Safeguards or classified information.

(b)(7)(C) related the security plan restricts the assignees from bringing any electronic device onto the property, including cell phones. (b)(7)(C) believed this presents a personal safety concern, especially with the (b)(7)(C). The assignees travel by bus and the metro transit system to get to work.

#### Review of Security Access Card Data

OIG reviewed security access badge data for nine current and/or recently departed foreign assignees and did not identify entry times or locations that were not in accordance with their security plans. The data reviewed contained all recorded building access - dates, times, and locations - from the assignee's start date to their end date/or through October 18, 2011, when the reports were run. No inappropriate after-hours or weekend access was identified.

**Observations About Enforceability and Cell Phones**

OIG noted that the agency's enforcement of the no cell phone/recording device rule and escorted access outside of assignee office space relies primarily on the assignee to follow these rules. This is because an assignee would not necessarily need to badge into other unrestricted office space in order to gain access and because the agency does not screen assignees as they arrive at the NRC to ensure they are not carrying any electronic devices.

OIG communicated these observations to (b)(7)(C) OIP, and (b)(7)(C) FSB, DFS, along with a suggestion for the guard station to offer an option to lock up assignee cell phones for the work day, or to provide lockers for visitors and assignees to secure electronics so that the assignees can have these devices while commuting to and from work.

**Review of Office of Information Services Access for Foreign Assignees**

(b)(7)(E)

Because this investigation did not identify any current areas of noncompliance with MD 12.3, *NRC Personnel Security Program*, as it relates to processing foreign assignee requests, this information is provided to you for informational purposes.



**Observations About Enforceability and Cell Phones**

OIG noted that the agency's enforcement of the no cell phone/recording device rule and escorted access outside of assignee office space relies primarily on the assignee to follow these rules. This is because an assignee would not necessarily need to badge into other unrestricted office space in order to gain access and because the agency does not screen assignees as they arrive at the NRC to ensure they are not carrying any electronic devices.

OIG communicated these observations to (b)(7)(C) OIP, and (b)(7)(C) FSB, DFS, along with a suggestion for the guard station to offer an option to lock up assignee cell phones for the work day, or to provide lockers for visitors and assignees to secure electronics so that the assignees can have these devices while commuting to and from work.

**Review of Office of Information Services Access for Foreign Assignees**

(b)(7)(E)

Because this investigation did not identify any current areas of noncompliance with MD 12.3, *NRC Personnel Security Program*, as it relates to processing foreign assignee requests, this information is provided to you for informational purposes.

**Distribution:**

**File Location:**

(b)(7)(E)

Case No. 11-42

Historical File

Magnum

\*See previous concurrence

| DIS/IGF   | DIS/IGF | DIS/IGF | DIS/IGF | DIS/IGF     | DIS/IGF   | DIS/IGF |
|-----------|---------|---------|---------|-------------|-----------|---------|
| (b)(7)(C) |         |         |         | J. McMillan | (b)(7)(C) |         |
| 8/18/13   | 8/18/13 | 8/18/13 | 8/18/13 | 8/14/13     | 8/24/13   | 8/27/13 |
| 21        | 21      |         |         |             |           |         |

Official File Copy

**Observations About Enforceability and Cell Phones**

OIG noted that the agency's enforcement of the no cell phone/recording device rule and escorted access outside of assignee office space relies primarily on the assignee to follow these rules. This is because an assignee would not necessarily need to badge into other unrestricted office space in order to gain access and because the agency does not screen assignees as they arrive at the NRC to ensure they are not carrying any electronic devices.

OIG communicated these observations to (b)(7)(C) OIP, and (b)(7)(C) FSB, DFS, along with a suggestion for the guard station to offer an option to lock up assignee cell phones for the work day, or to provide lockers for visitors and assignees to secure electronics so that the assignees can have these devices while commuting to and from work.

**Review of Office of Information Services Access for Foreign Assignees**

(b)(7)(E)

Because this investigation did not identify any current areas of noncompliance with MD 12.3, *NRC Personnel Security Program*, as it relates to processing foreign assignee requests, this information is provided to you for informational purposes.

Distribution:

File Location: (b)(7)(E)

(b)(7)(E)

Case No. 11-42

Historical File

Magnum

|         |         |           |         |             |         |             |
|---------|---------|-----------|---------|-------------|---------|-------------|
| OIG/ALJ | OIG/ALJ | Editor    | OIG/ALJ | OIG/ALJ     | OIG     | OIG         |
|         |         | (b)(7)(C) |         | J. McMillan | D. Lee  | H. B. H. 11 |
| 8/8/13  | 8/18/13 | 8/14/13   | 8/18/13 | 8/14/13     | 8/14/13 | 8/21/13     |


Official File Copy



OFFICE OF THE  
INSPECTOR GENERAL

**UNITED STATES**  
**NUCLEAR REGULATORY COMMISSION**  
WASHINGTON, D.C. 20555-0001

December 30, 2013

MEMORANDUM TO: Concur: Case Closed   
Joseph A. McMillan  
Assistant Inspector General  
for Investigations

THRU:

(b)(7)(C)  
Team Leader (b)(7)(C)

FROM:

(b)(7)(C)  
Special Agent (b)(7)(C)

SUBJECT: PROACTIVE INITIATIVE: NETWORK INTRUSION PROJECT  
(OIG CASE NO. 10-018)

**Project**

The Office of the Inspector General (OIG), U.S. Nuclear Regulatory Commission (NRC), initiated a proactive initiative in March 2010 to identify possible proactive cases involving network intrusions dealing with unknown network traffic and e-mails from internal and external sources as well as remediates compromised NRC exchange accounts.

**Findings**

From March 2010 to November 2013, OIG special agents assigned to the Cyber Crimes Unit (CCU) initiated and/or assisted OIG special agents in conducting approximately 17 investigations dealing with the compromise or attempted compromise of NRC computer resources by known and unknown sources. In addition, CCU special agents participated in various meetings held by various Federal cyber task forces.

### Basis for Finding

Over the course of this proactive project, the following are examples of investigations undertaken by the CCU:

- Case No. (b)(7)(E) This investigation involved several incidents of targeted spear phishing e-mails sent to NRC employees. These e-mails contained compromised word documents which contained a Trojan backdoor malicious software (malware) used to gain unauthorized access to the computer. The document was intercepted at the firewall. No compromise occurred and investigation was able to track the sender to a foreign country.
- Case No. (b)(7)(E) This investigation involved several incidents of targeted spear phishing e-mails sent to NRC employees. These e-mails contained compromised rich text format (RTF) and Portable Document Format (PDF) documents which contained a Trojan backdoor malicious software (malware) used to gain unauthorized access to the computer. The RTF was intercepted by the firewall but the PDF was not. One NRC employee interacted with the unknown sender and the unknown sender sent the same document and attempted to use social engineering to convince the employee to open the file. No compromise occurred and investigation was able to track the sender to a foreign country.
- Case No. (b)(7)(E) This investigation involved an unknown person impersonating an NRC employee who e-mailed a compromised Excel spreadsheet containing an Adobe Flash exploit. The unknown person utilized a Google e-mail address but impersonated an NRC employee in their signature block. The investigation traced the unknown user back to a compromised U.S. local government computer which was part of an ongoing investigation by another federal law enforcement agency.
- Case No. (b)(7)(E) This investigation involved several hundred incidents of phishing e-mails sent to NRC employees in a logon credential harvesting attempt. These e-mails contained a link to a cloud based Google spreadsheet document asking users to verify their account by logging in. A dozen NRC employees clicked on the link. In the course of the investigations, other U.S. Federal agency users were identified as having provided logon information and CCU was able to track the person who set up the spreadsheet to a foreign country.
- Case No. (b)(7)(E) This investigation involved a harassing e-mail sent to the NRC Chairman. The e-mail contained language that rose to the level of character

defamation. The investigation uncovered the sender as an unemployed homeless man with known mental health issues from Washington State.

- Case No. (b)(7)(E) This investigation involved several incidents of targeted spear phishing e-mails sent to NRC employees. These e-mails contained a link to a cloud based Microsoft Skydrive storage site which contained the malicious file. There was one incident of compromise and the investigation tracked the sender to a foreign country.
- Case No. (b)(7)(E) This investigation involved the personal e-mail account of an NRC employee that was compromised and which sent a malware to other NRC employees in the contact list. These e-mails contained a PDF file with a known JavaScript vulnerability. One computer was infected and CCU was unable to track the person who compromised the personal e-mail account due to the lack of logs.
- Case No. (b)(7)(E) This investigation involved an unknown person who sent a threat to an NRC employee via a personal Web site. The NRC employee received a forwarded e-mail from their personal web site containing threats to the employee based on their role as a government representative. The investigation was unable to identify the individual that sent the e-mail as the person used an Internet Service Provider located in a foreign country.
- Case No. (b)(7)(E) This investigation involved a stakeholder who received an e-mail containing a malware from an e-mail name of nrc.nrc. This e-mail contained a compressed file which was identified as containing malware. The stakeholder's computer was compromised and the investigation was unable to trace the e-mail sender beyond a compromised computer in California.

During the course of this project, CCU special agents participated in meetings held by Federal cybercrime task forces and professional organizations to combat malicious intrusions into the NRC network. These groups included:

- Federal Bureau of Investigations Baltimore Cyber Task Force
- U.S. Secret Service Electronic Crimes Task Force
- Department of Justice Computer Crime and Intellectual Property Section

Within the NRC, the CCU continues the relationships with the Computer Security Office as well as continues to foster the relationship with the Office of Information Systems, Security Operations Branch.

Recommend closure of this project and a similar project will be initiated for fiscal year 2014.

~~OFFICIAL USE ONLY - OIG INVESTIGATION INFORMATION~~

- Case No. (b)(7)(E) This investigation involved several incidents of targeted spear phishing e-mails sent to NRC employees. These e-mails contained a link to a cloud based Microsoft Skydrive storage site which contained the malicious file. There was one incident of compromise and the investigation tracked the sender to a foreign country.
- Case No. (b)(7)(E) This investigation involved the personal e-mail account of an NRC employee that was compromised and which sent a malware to other NRC employees in the contact list. These e-mails contained a PDF file with a known JavaScript vulnerability. One computer was infected and CCU was unable to track the person who compromised the personal e-mail account due to the lack of logs.
- Case No. (b)(7)(E) This investigation involved an unknown person who sent a threat to an NRC employee via a personal Web site. The NRC employee received a forwarded e-mail from their personal web site containing threats to the employee based on their role as a government representative. The investigation was unable to identify the individual that sent the e-mail as the person used an Internet Service Provider located in a foreign country.
- Case No. (b)(7)(E) This investigation involved a stakeholder who received an e-mail containing a malware from an e-mail name of nrc.nrc. This e-mail contained a compressed file which was identified as containing malware. The stakeholder's computer was compromised and the investigation was unable to trace the e-mail sender beyond a compromised computer in California.

During the course of this project, CCU special agents participated in meetings held by Federal cybercrime task forces and professional organizations to combat malicious intrusions into the NRC network. These groups included:

- Federal Bureau of Investigations Baltimore Cyber Task Force
- U.S. Secret Service Electronic Crimes Task Force
- Department of Justice Computer Crime and Intellectual Property Section

Within the NRC, the CCU continues the relationships with the Computer Security Office as well as continues to foster the relationship with the Office of Information Systems, Security Operations Branch.

Recommend closure of this project and a similar project will be initiated for fiscal year 2014.

File Location: (b)(7)(E)

Distribution:

Case File 10-18

Historical File Magnum

| OIG        | OIG      | Editor | OIG | OIG         | OIG      | OIG      |
|------------|----------|--------|-----|-------------|----------|----------|
| (b)(7)(C)  |          |        |     | J. McMillan | D. Lee   | H. Bell  |
| 12/17/2013 | 12/17/13 | 111    | 111 | 12/18/13    | 12/24/13 | 12/24/13 |

Official File Copy