



OFFICE OF INSPECTOR GENERAL
EXPORT-IMPORT BANK
OF THE UNITED STATES

EXPLICIT COMPUTER USAGE

Special Report
August 26, 2010
OIG-SR-10-02



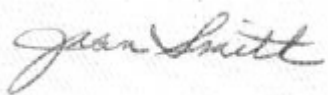
OFFICE OF INSPECTOR GENERAL

**Export-Import Bank
of the United States**

August 26, 2010

MEMORANDUM

TO: Fernanda Young, Chief Information Officer
Bill Smith, Director, IT Infrastructure and Security

FROM: Jean Smith
Assistant Inspector General for Audit 

SUBJECT: Explicit Computer Usage

This memorandum transmits Special Report OIG-SR-10-02, Explicit Computer Usage. The review was initiated by the Office of Inspector General of the Export-Import Bank of the United States (Bank) to determine whether the Bank has (1) policies on information technology use and disciplinary guidance and (2) controls to prevent and identify Ex-Im Bank employees accessing sexually explicit material on government computers.

The report contains one suggestion. We suggested that the Chief Information Officer alert the Inspector General (IG) of computer misuse involving incidents referred to management for disciplinary actions. The Chief Information Officer stated that incident reports will be provided to the IG after the Office of General Counsel reviews the reports. Appendix C of this report is the Chief Information Officer's formal response to our review.

We appreciate the courtesies and cooperation provided to the auditors during the review. If you have any questions, please call me at (202) 565-3944.

cc: Audit Committee
Alice Albright, Senior Vice President, Chief Operations Officer
Michael Cushing, Senior Vice President, Resource Management
John Simonson, Chief Financial Officer and Audit Liaison

EXECUTIVE SUMMARY

The Office of Inspector General (OIG) performed a limited review to address an inquiry from Senator Charles E. Grassley on the viewing, downloading, and possible distribution of pornography at the Export-Import Bank of the United States (Ex-Im Bank). Our specific objectives were to determine whether Ex-Im Bank has (1) policies on information technology use and disciplinary guidance and (2) controls to prevent and identify Ex-Im Bank employees accessing sexually explicit material on government computers.

Ex-Im Bank has policies and annual employee training on the proper use of government computers. Additionally, Ex-Im Bank's Policy 752 – *Employee Conduct and Discipline* provides the basic rules of discipline for Ex-Im Bank.

Controls are in place to block employees' computer from accessing sexually explicit material, monitor computer activity, and take appropriate action to prevent further illicit access and report incidents. The Office of the Chief Information Officer (OCIO) maintains Internet and e-mail blockers to prevent access to prohibited sources, reviews activity logs daily, and takes necessary appropriate action. When employee misuse is identified, the Chief Information Officer submits a Security Incident Report for further processing by General Counsel. However, the OIG is not alerted of the incident.

General practice by government agencies is to report misconduct to the Inspector General (IG). We suggest that the Chief Information Officer includes the IG in the distribution of Security Incident Reports on computer misuse involving incidents referred to management for disciplinary actions.

The Chief Information Officer stated that incident reports will be provided to the IG after the Office of General Counsel reviews the reports. Appendix C of this report is the Chief Information Officer's formal response to our review.

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

I. BACKGROUND 1

II. OBJECTIVES 1

III. SCOPE AND METHODOLOGY 1

IV. FINDINGS AND SUGGESTION 2

 A. ADEQUATE POLICIES ON INFORMATION TECHNOLOGY USE AND
 DISCIPLINARY GUIDANCE EXIST..... 2

 B. ADEQUATE CONTROLS ARE IN PLACE TO MANAGE ACCESS OF
 SEXUALLY EXPLICIT MATERIAL 4

 Suggestion 1 6

 Management Response 6

APPENDIX A – STANDARDS OF ETHICAL CONDUCT 7

APPENDIX B – DOUGLAS FACTORS 9

APPENDIX C – MANAGEMENT RESPONSE 10

I. BACKGROUND

Use of government property, 5 Code of Federal Regulations, part 2635.704 (a) states:

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.

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.

II. OBJECTIVES

The objectives of this review were to determine whether Ex-Im Bank has (1) policies on information technology use and disciplinary guidance and (2) controls to prevent and identify Ex-Im Bank employees accessing sexually explicit material on government computers.

III. SCOPE AND METHODOLOGY

We interviewed Ex-Im Bank's Director, Information Technology (IT) Infrastructure and Security in the Office of the Chief Information Officer, and we reviewed computer activity logs. We also reviewed applicable procedures and information available on the Ex-Im Bank's internal website.

Over a two day period during our fieldwork, we conducted an unannounced test on Ex-Im Bank's controls of preventing and identifying pornography access on government computers. The test consisted of attempting to access and retrieve pornographic material on the Internet and e-mails. Subsequent to this test, we reviewed how promptly Ex-Im Bank responded to our test activities.

We conducted our fieldwork from August 2, 2010 to August 10, 2010.

We performed a limited review to address an inquiry from Senator Charles E. Grassley regarding employees' use of Ex-Im Bank computers to obtain pornography.

IV. FINDINGS AND SUGGESTION

A. ADEQUATE POLICIES ON INFORMATION TECHNOLOGY USE AND DISCIPLINARY GUIDANCE EXIST

Ex-Im Bank issued adequate policies to inform users of the proper use of its computers and potential disciplinary actions for misuse. Additionally, as part of the annual IT security training, computer users are reminded that use of Ex-Im Bank computers prohibit accessing sexually explicit or sexually orientated material. Annual IT security training requires the participants to review and accept Ex-Im Bank's *Rules of Behavior*.

Ex-Im Bank established policies titled *Rules of Behavior* and "*Limited Personal Use*" of *Government Office Equipment Including Information Technology* to advise users that use of computers, e-mail, the Internet, and electronic information, must be in a professional, appropriate, ethical, and lawful manner.

The *Rules of Behavior* states that employees and contractors must:

- Adhere to the "*Limited Personal Use*" of *Government Office Equipment Including Information Technology*.
- Adhere to the established standards of conduct as defined in Ex-Im Bank Policy 752 – *Employee Conduct and Discipline* and *Standards of Ethical Conduct for Employees of the Executive Branch*.

The *Rules of Behavior* further states:

Failure to conform one's conduct to these rules may lead to adverse action, including but not limited to, suspension of access privileges, reprimand, suspension, or termination from the federal service, and/or civil and/or criminal penalties. All users have no right to or expectation of privacy while using any Ex-Im Bank IT system at any time, including accessing the Internet, using e-mail, or limited personal use.

"*Limited Personal Use*" of *Government Office Equipment Including Information Technology* provides a list of inappropriate personal uses. "The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials" is included in the policy's Inappropriate Personal Uses list.

For disciplinary guidance, Ex-Im Bank established Policy 752 – *Employee Conduct and Discipline*. This Policy contains Standards of Ethical Conduct for Employees (Appendix

Special Report

A), Douglas Factors¹ (Appendix B), and a Table of Offenses and Suggested Disciplinary Penalties. Disciplinary penalties listed in Policy 752 are provided as guidance. In each case of formal discipline, the supervisor must coordinate with the Office of Human Resources before proposing and deciding the appropriate action. All proposed suspensions and removals must be coordinated with the Assistant General Counsel for Administration in the Office of the General Counsel (OGC). Present below is the suggested penalty for conducting explicit computer use.

<i>Nature of Offense</i>	<i>First Offense</i>	<i>Second Offense</i>	<i>Third Offense</i>
Misuse of the Bank’s computer systems, Internet, or electronic mail	Written Reprimand to Removal	14-Day Suspension to Removal	Removal

Although Ex-Im Bank alerted employees of prohibited computer use, over the last two years the Director, IT Infrastructure and Security Office, identified two employees who accessed pornography on Ex-Im Bank computers and alerted the OGC. While the OGC was processing the cases, these employees voluntarily left the federal government.

¹ In *Douglas v. Veterans Administration* (1981), the Merit Systems Protection Board identified 12 relevant factors that agency management needs to consider and weigh in deciding an appropriate disciplinary penalty.

B. ADEQUATE CONTROLS ARE IN PLACE TO MANAGE ACCESS OF SEXUALLY EXPLICIT MATERIAL

Ex-Im Bank has adequate controls in place to block employees' computer from accessing sexually explicit material, monitor computer activity, and take appropriate action to prevent further illicit access and report incidents. However, the Inspector General (IG) has not been traditionally alerted of these incidents. General practice by government agencies is to report misconduct to the IG. While Ex-Im Bank's Charter directs General Counsel to ensure appropriate legal counsel for advice on, and oversight of, issues relating to personnel matters, alerting the IG of computer misuse will assist the IG in preventing and detecting fraud and abuse in programs and operations as required under the Inspector General Act of 1978, as amended.

To test the effectiveness of Ex-Im Bank's controls, we attempted to browse the Internet and download pornographic material using Ex-Im Bank computers. We randomly used web addresses associated with pornography and search engines – using words and phrases normally associated with pornography – for links and addresses to connect to pornography sites. For the most part, all attempts were blocked.

On the third day that the above controls testing began, the Office of the Chief Information Officer (OCIO) IT Infrastructure and Security Office Director met with the OIG's Assistant Inspector General for Audit (AIGA) to report logged activity by OIG staff to access pornography. This Director presented the AIGA with a Security Incident Report and supporting documentation. The AIGA advised the Director that the OIG staff activity was a test of Ex-Im Bank controls. Also, because the test resulted in reaching three pornography sites, the AIGA provided the three accessed sites to the Director who immediately blocked them for future access on Ex-Im Bank computers.

Recognizing that it is impossible to totally block pornography because new sites are constantly created and some sites contain a combination of pornography and non-pornography, our test confirmed that Ex-Im Bank has adequate controls in place to manage access to sexually explicit material.

Our discussion of Ex-Im Bank's controls is presented below.

Blockers

Ex-Im Bank significantly strengthened its IT capabilities to block inappropriate Internet sites and e-mails since 2006. Although it took an extensive amount of time to implement the current systems, in July 2009 the Software/Hardware Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) were fully implemented.

Special Report

Full implementation of this hardware/software took several years primarily due to the need to upgrade IT infrastructure and enhance the power system. Because installation was conducted one floor at a time, some Ex-Im Bank computer users had blocking software installed as far back as three years ago, while others were not blocked until approximately one year ago.

Ex-Im Bank's OCIO identified sites, words, and numerous categories for its IDS and IPS to either monitor or block. Prohibited categories which are either monitored by OCIO or automatically blocked altogether are sites that include materials which are: sexually explicit, violent, hate, gambling and approximately 48 other categories.

The site blocking hardware/software is updated every five minutes via subscription-based services. It is also manually updated by the IT Infrastructure and Security Office when a prohibited site is identified outside of the subscribed service.

Monitoring

Security Engineers in the IT Infrastructure and Security Office review Internet browsing logs daily. The logs are analyzed to see if Ex-Im Bank users are excessively using computer bandwidth or attempting to visit blocked, malware², or questionable sites.

E-mail attachments are also monitored via IDS software. This filtering software works by comparing known sexually explicit key words and other known spamware/virus names to the e-mail attachment(s).

When questionable activity is identified by Security Engineers and others, such as Ex-Im Bank's Helpdesk staff, the IT Infrastructure and Security Office Director will research the activity to determine the appropriate action.

Action

Research revealing prohibited activity and/or potential harm to Ex-Im Bank's IT systems is summarized and discussed at the daily IT Infrastructure and Security Office meeting. For a newly identified site which may be harmful or prohibited, the OCIO will add the site to the IPS systems. For prohibited activity conducted by an employee or contractor, the IT Infrastructure and Security Office Director will issue a report and supporting evidence of the behavior to the Chief Information Officer (CIO). The CIO will then forward the report and evidence to the OGC for a determination of the behavior and appropriate disciplinary action.

² Malware is short for malicious software. It is software designed to infiltrate a computer system without the owner's informed consent.

To improve the reporting of computer misuse, the IT Infrastructure and Security Office Director recently created a standardized form – Security Incident Report – based on lessons learned from reporting previous incidents.

Over the past two years, the IT Infrastructure and Security Office Director reported incidents on five employees.

- Three involved malware.
- Two involved accessing pornography.

Suggestion 1

The CIO should include the IG in the distribution of Security Incident Reports on computer misuse involving incidents referred to management for disciplinary actions.

Management Response

The CIO stated that management concurred with the intent of the recommendation. The current procedure already provides that OCIO forward these incident reports to the OGC for their review. After the OGC review, the CIO will distribute incident reports to the IG.

APPENDIX A – STANDARDS OF ETHICAL CONDUCT**PART 2635 - STANDARDS OF ETHICAL CONDUCT FOR EMPLOYEES OF THE EXECUTIVE BRANCH SUBPART A - GENERAL PROVISIONS**

§ 2635.101 Basic obligation of public service.

(a) Public service is a public trust. Each employee has a responsibility to the United States Government and its citizens to place loyalty to the Constitution, laws and ethical principles above private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in this section, as well as the implementing standards contained in this part and in supplemental agency regulations.

(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.

(1) Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws and ethical principles above private gain.

(2) Employees shall not hold financial interests that conflict with the conscientious performance of duty.

(3) Employees shall not engage in financial transactions using nonpublic Government information or allow the improper use of such information to further any private interest.

(4) An employee shall not, except as permitted by subpart B of this part, solicit or accept any gift or other item of monetary value from any person or entity seeking official action from, doing business with, or conducting activities regulated by the employee's agency, or whose interests may be substantially affected by the performance or nonperformance of the employee's duties.

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

(6) Employees shall not knowingly make unauthorized commitments or promises of any kind purporting to bind the Government.

(7) Employees shall not use public office for private gain.

(8) Employees shall act impartially and not give preferential treatment to any organization or individual.

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

(10) Employees shall not engage in outside employment or activities, including seeking or negotiating for employment, that conflict with official Government duties and responsibilities.

(11) Employees shall disclose waste, fraud, abuse, and corruption to appropriate authorities.

Special Report

(12) Employees shall satisfy in good faith their obligations as citizens, including all just financial obligations, especially those--such as Federal, State, or local taxes--that are imposed by law.

(13) Employees shall adhere to all laws and regulations that provide equal opportunity for all Americans regardless of race, color, religion, sex, national origin, age, or handicap.

(14) Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in this part. Whether particular circumstances create an appearance that the law or these standards have been violated shall be determined from the perspective of a reasonable person with knowledge of the relevant facts.

(c) Related statutes. In addition to the standards of ethical conduct set forth in this part, there are conflict of interest statutes that prohibit certain conduct. Criminal conflict of interest statutes of general applicability to all employees, 18 U.S.C. 201, 203, 205, 208, and 209, are summarized in the appropriate subparts of this part and must be taken into consideration in determining whether conduct is proper. Citations to other generally applicable statutes relating to employee conduct are set forth in subpart I and employees are further cautioned that there may be additional statutory and regulatory restrictions applicable to them generally or as employees of their specific agencies. Because an employee is considered to be on notice of the requirements of any statute, an employee should not rely upon any description or synopsis of a statutory restriction, but should refer to the statute itself and obtain the advice of an agency ethics official as needed.

APPENDIX B – DOUGLAS FACTORS

In *Douglas v. Veterans Administration* (1981), the Merit Systems Protection Board identified 12 relevant factors that agency management needs to consider and weigh in deciding an appropriate disciplinary penalty. The 12 Douglas Factors are:

1. The nature and seriousness of the offense and its relation to the employee's duties, position, and responsibilities, including whether the offense was intentional or technical or inadvertent, or was committed maliciously or for gain, or was frequently repeated;
2. The employee's job level and type of employment, including supervisory or fiduciary role, contacts with the public, and prominence of the position;
3. The employee's past disciplinary record;
4. The employee's past work record, including length of service, performance on the job, ability to get along with fellow workers, and dependability;
5. The effect of the offense upon the employee's ability to perform at a satisfactory level and its effect upon supervisors' confidence in the employee's ability to perform assigned duties;
6. Consistency of the penalty with those imposed upon other employees for the same or similar offenses;
7. Consistency of the penalty with the applicable agency table of penalties (which are not to be applied mechanically so that other factors are ignored);
8. The notoriety of the offense or its impact upon the reputation of the agency;
9. The clarity with which the employee was on notice of any rules that were violated in committing the offense, or had been warned about the conduct in question;
10. The potential for employee's rehabilitation;
11. Mitigating circumstances surrounding the offense, such as unusual job tensions, personality problems, mental impairment, harassment, or bad faith, malice or provocation on the part of others involved in the matter; and
12. The adequacy and effectiveness of alternative sanctions to deter such conduct in the future by the employee or others.

APPENDIX C – MANAGEMENT RESPONSE

SEE NEXT PAGE



EXPORT-IMPORT BANK
of the UNITED STATES

August 26, 2009

Jean Smith
Assistant Inspector General for Audit
Office of Inspector General
Export-Import Bank of the United States

Ref: Explicit Computer Usage - August 19, 2010, OIG-SR-10-xx.

Dear Jean:

Thank you for the opportunity to review and comment on the IG special report "Explicit Computer Usage" dated August 19, 2010, number OIG-SR-10-xx.

We agree with both findings and concur with the suggestion (with a minor revision proposed below)

Finding A: Adequate policies on information technology use and disciplinary guidance exist. We are in agreement with your finding that the Ex-Im Bank has adequate controls in place to manage access to pornographic/sexually explicit web sites.

Ex-Im Bank has policies, procedures and controls in place to ensure staff and contractors have a safe computing environment at work.

Ex-Im Bank has policies covering "Rules of Behavior for Users of Export Import Bank Information Systems" clearly delineating responsibilities and expected behavior of all individuals with access to the systems; and "Limited Personal Use of Government Office Equipment Policy," establishing privileges and responsibilities of Ex-Im Bank employees and contractors with regard to acceptable personal use of Government office equipment that does not interfere with Ex-Im Bank's mission or operations and does not violate the Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635. These policies follow NIST and the CIO Council Government-wide guidelines.

The Ex-Im Bank performs mandatory annual IT Security and Privacy Awareness Training. This training reinforces policy defined by the Limited Use Policy, Rules of Behavior, Sensitive Information Policy, and the Remote Access Policy and other policies as appropriate. The Office of the Chief Information Officer (OCIO) also conducts an occasional IT security expo in order to reinforce awareness of the IT security, rules of behavior and privacy policies of Ex-Im Bank.

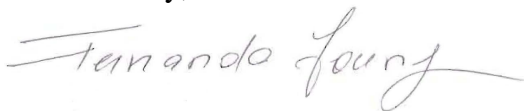
Finding B: Adequate controls are in place to manage access of sexually explicit material The OCIO has also implemented comprehensive Internet and e-mail blocking solutions to web sites and email with: 1) inappropriate content, 2) content that is likely to present IT security issues, and 3) content that presents network capacity issues.

Currently, no explicit regulation mandates federal agencies to actively implement IT solutions for blocking access to inappropriate web sites in the workplace. The Bank has proactively implemented industry best practice capabilities in that area – solutions provided by vendors such as CISCO. The site blocking hardware and software is updated every five minutes via subscription-based services. It is also manually updated internally to handle exceptions (adding or deleting sites that are not properly categorized or blocking sites with known security issues).

Logs are monitored daily and incidents are evaluated and are generally disseminated using our incident reporting procedure. The procedure states that the CIO will forward the incident report and accompanying evidence to the Office of General Counsel (OGC) for a determination of the behavior and appropriate disciplinary action.

Suggestion 1: The CIO should include the IG in the distribution of Security Incident Reports on computer misuse involving incidents referred to management for disciplinary actions. We concur with the intent of the recommendation. The current procedure already provides that OCIO forward these incident reports to the Office of General Counsel (OGC) for their review. After the OGC review, the CIO will distribute incident reports to the IG.

Sincerely,



Fernanda Young
Chief Information Officer

Cc:

Michael Cushing, Senior Vice President, Resource management


Jonathan Cordone, Senior Vice President and General Council

John Simonson, Senior Vice President and Chief Financial Officer

Alice Albright, Executive Vice president and Chief Operating Officer

Diane Farrell, Member of the Board of Directors

Bijan R. Kian, Member of the Board of Directors



**Office of Inspector General
Export-Import Bank of the United States
811 Vermont Avenue, NW
Washington, DC 20571
202-565-3908
www.exim.gov/oig**