Office of Inspector General Corporation for National and Community Service

Corporation Internet Use & Information Privacy Study Report

OIG Report Number 09-03

Corporation for
NATIONAL & COMMUNITY SERVICE

March 25, 2009

Prepared by:
Richard S. Carson and Associates, Inc.
4720 Montgomery Lane
Suite 800
Bethesda, MD 20814

This report was issued to Corporation management on March 25, 2009. Under the laws and regulations governing audit follow-up, the Corporation is to make final management decisions on the report's findings and recommendations no later than September 25, 2009 and complete its corrective actions by March 25, 2010. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

Corporation for
NATIONAL & COMMUNITY SERVICE

OFFICE OF INSPECTOR GENERAL

March 25, 2009

TO: Mikel Herrington
Acting Director of AmeriCorps*NCCC

Margaret Rosenberry
Director, Office of Grants Management

FROM: Kenneth C. Bach /s/
Assistant Inspector General for Support

SUBJECT: Report 09-03, *Corporation Internet Use & Information Privacy Study Report*

We contracted with the independent firm of Richard S. Carson and Associates, Inc. (Carson) to perform a review of the Corporation's Internet Use & Information Privacy.

Carson is responsible for the attached report, dated March 25, 2009, and the conclusions expressed therein. We do not express opinions on the report and conclusions.

Under the Corporation's audit resolution policy, a final management decision on the findings in this report is due by September 25, 2009. Notice of final action is due by March 25, 2010.

If you have questions pertaining to this report, please call me at (202) 606-9377.

Attachment

cc: Richard Friend, Acting Chief Information Officer
Juliette Sheppard, Director of Information Assurance
William Anderson, Acting Chief Financial Officer
Sherry Blue, Audit Resolution Coordinator
Diane C. Reily, Vice President, Richard S. Carson and Associates, Inc.

Table of Contents

Executive Summary

In 2006, Richard S. Carson and Associates, Inc. (Carson Associates) conducted a review of AmeriCorps's level of compliance with the Corporation for National and Community Service's (Corporation) Internet use policy, on behalf of the Office of the Inspector General (OIG). In 2008, the OIG elected to re-evaluate the AmeriCorps*National Civilian Community Corps (NCCC) compliance with the Corporation's Internet Acceptable Use and privacy policies. The objectives of the evaluation were to:

- Determine if Internet usage is consistent with Corporation policy.
- Identify files and/or programs not authorized by Corporation policy.
- Verify compliance with Corporation policy regarding the storage of Personally Identifiable Information (PII).

Results in Brief

We found that the Corporation's policies on acceptable use of information resources and privacy are in line with the latest Federal guidelines and mandates. Officials of both NCCC campuses were aware of the policies and distributed this knowledge throughout their organizations.

Our evaluation once again revealed instances of inappropriate use of Corporation information systems involving pornography. During visits to NCCC campuses at Perry Point, MD, and Sacramento, CA, we determined that two laptops out of 21 evaluated, and six desktops out of 14 evaluated, contained inappropriate pornographic images that are expressly prohibited by the Corporation's acceptable use policy. In addition, it was noted that at the Perry Point campus, management wasn't protecting Corporation information resources in accordance with the acceptable use policy. We found that the front and rear doors of the campus computer lab are not kept locked at all times.

With regard to NCCC's compliance with the Corporation's information privacy policy, we noted that there was no PII being stored on any of the evaluated computers. Furthermore, each campus displayed a document in its lab that stated that PII was not to be stored on the Corporation's computers. At the Perry Point location, the uploading of personal privacy information is expressly forbidden by the rules of behavior that each person is required to sign before being given access to the Corporation's information resources.

The NCCC's responses to the OIG's are included in this report as Appendix A.

Acronyms and Abbreviations

CIO	Chief Information Officer
IM	Instant Messaging
ICQ	I Seek You
IT	Information Technology
N/A	Not Applicable
NCCC	AmeriCorps*National Civilian Community Corps
OIG	Office of Inspector General
OIT	Office of Information Technology
RoB	Rules of Behavior

Purpose

The objectives of this independent evaluation were as follows:

- Assess the Corporation's degree of compliance with ISP-P-13-0808, Acceptable Use of Information Resources, ISP-P-12-0808, Information Privacy policies, and CNCS CIO 2008-001, Information Privacy Policy.
- Determine whether prohibited practices and instances of abuse took place on Internet use on non-networked and a limited number of networked Corporation owned equipment.

Methodology

We conducted this evaluation during the period of November 15, 2008, through December 31, 2008, at NCCC campuses in Sacramento, CA, Perry Point, MD. Our methodology consisted of inquiries, observation, and testing designed to determine compliance with the Corporation policies ISP-P-13-8080: *CNCS Acceptable Use of Information Resources,* ISP-P-12-8080: *Information Privacy,* and CIO-2008-001: *Information Privacy Policies.*

Acceptable Use

The Corporation's *Acceptable Use of Information Resources Policy* requires that Corporation personnel act responsibly when using its information resources. They must not share passwords or use someone else's password; avoid introducing malicious or harmful programs; or use resources in such a manner as to delay or impede others from performing their duties. They must also refrain from accessing expressly prohibited materials.

Managers are responsible for detecting instances of abuse and taking actions to correct those abuses. They are also responsible for ensuring that the information resources under their charge are protected from unauthorized access and other forms of abuse.

Observations

The Corporation has taken steps, including policy revisions, to remediate issues noted during our prior assessment. In addition, it has developed security awareness training presentations that cover acceptable/unacceptable use of government resources, and has established a requirement for users to sign a Rules of Behavior form.

However, our assessment revealed that these policies and procedures are not being effectively implemented at the Sacramento and Perry Point NCCC campuses. As a result, we found instances of inappropriate Internet use on Corporation-owned computers.

AmeriCorps NCCC - Sacramento, California

The NCCC Pacific Regional Center is located in the McClellan Business Park in Sacramento, CA. During our assessment, it was noted that the Regional Director had distributed a memorandum communicating the intent of CNCS ISP-P-13-8080 and that personnel were aware of its existence and content. The policy and the memorandum are located in a binder in each of the computer labs, thus ensuring that personnel have access to the information.

A card reader, which ensures that only authorized personnel gain access to information resources, protects the physical access of each lab.

For the laptop computers NCCC leaders and member use in the field, NCCC , management has elected to re-image the hard drives once the computers are returned from deployments. This method is used to identify and eliminate any software problems that may have been introduced. This re-imaging also checks for instances of inappropriate material which might embarrass the Corporation or offend new team members.

Observation #1
There were no technologies or manual methodologies being used to detect, assign responsibility for, or limit unacceptable use of information resources at the NCCC campus in Sacramento.

According to CNCS Policy ISP-P-13-8080, *Acceptable Use of Information Resources,* dated August 15, 2008, users are responsible for using Corporation information resources responsibly and in compliance with all information security policies and guidelines. Supervisors must ensure that their personnel are informed of the acceptable use policy, and must monitor usage so they can take action to correct abuses when they occur.

It does not appear that supervisors are currently monitoring how their personnel are using the information resources under their charge, as evidenced by the pornographic materials discovered on the desktop computers (see the table below).

Computer Host Name	Abuse Noted (Yes/No)	Number of Images	Account Used
NCCC-011407	YES	9	Administrator
NCCC-011345	YES	26	Guest

Table 1: Desktop Computers (Sacramento)

Recommendation #1 –

In order to ensure that NCCC officials can determine who inappropriately utilized information resources and take action, the Corporation should:

a. Deploy an access control scheme to permit logging of individual access to information resources .

b. Deploy content filtering software to prevent access to prohibited content.

AmeriCorps NCCC – Perry Point, Maryland

The NCCC Eastern Regional Center is located on the grounds of the Perry Point Veteran's Center in Perryville, MD. This campus is publicly accessible and personnel at the VA facility enjoy unrestricted access to the grounds and facilities at all times. During our assessment, it was noted that the leadership of the center had posted the acceptable use standards on a bulletin board in the lab and had posted reminders to follow policies when using the lab's resources. Management had also taken actions to implement access controls by establishing passwords for both member and administrator accounts.

Observation #2
The NCCC campus at Perry Point does not effectively control physical access to its computer lab.

We found that the lab's doors were unlocked during the normal workday, allowing for unrestricted physical access. According to CNCS Policy ISP-P-13-8080, *Acceptable Use of Information Resources,* dated August 15, 2008; *Attachment: CNCS Information Security User Agreement* users are responsible for protecting the information resources in their possession. Permitting unrestricted physical access to the Corporation's information resources in an open campus environment may permit unauthorized personnel to gain access. Although there are cable locks securing both the computers and monitors, personnel not associated with NCCC could remove or damage the resources, or use the resources inappropriately.

Recommendation #2 –

Consider physical security controls such as the card readers used at the NCCC campus in Sacramento.

Observation #3

No technologies or manual methodologies were employed to detect, assign responsibility for, or limit unacceptable use of in formation resources at the Perry Point campus.

According to CNCS Policy ISP-P-13-8080, *Acceptable Use of Information Resources,* dated August 15, 2008, users are responsible for using Corporation information resources responsibly and in compliance with all CNCS information security policies and guidelines. Supervisors must ensure that their personnel are informed of the acceptable use policy, and must monitor usage.

It does not appear that supervisors at Perry Point are currently monitoring how their personnel use information resources, as evidenced by the pornographic materials discovered on desktop and laptop computers (see table below).

Computer Serial Number	Number of Images	Account Used
MXL506046K	237	CORPS MEMBER
MXL506049Y	40	CORPS MEMBER
MXL506046Q	94	CORPS MEMBER
MXL506049V	2	CORPS MEMBER

Table 2: Perry Point Desktops

Laptop Serial Number	Number of Images	Account Used
MXL6420M3M	3	TEAM LEAD
MXL6420M11	11	CORPS MEMBER

Table 3: Perry Point Laptops

Recommendation #3 –

We recommend that the Corporation determine who inappropriately utilized information resources and deter such abuse by:

a. Deploying an access control scheme to permit logging and identification of individual users.

b. Deploying content filtering software to prevent access to prohibited content.

Privacy

The Corporation's ISP-P-12-8080, *Information Privacy,* and CIO-2008-001, *Information Privacy* policies served as the foundation for the 2008 information privacy assessment at the NCCC campuses in Sacramento and Perry Point. Interviews were conducted with leadership at both campuses and all desktop and laptop computers were evaluated manually to detect evidence of privacy information. We did not find privacy information on any of the desktops or laptop computers.

During our assessment, we noted that management at both locations was aware of established Corporation privacy policies. Both sites were in the process of implementing Corporation privacy rules of behavior as required and indicated that all members will be required to sign the rules of behavior before gaining access to access Corporation-owned computers. Both campuses had posted signs in the computer labs to communicate that the storing of PII on the computers is prohibited.

Appendix A: NCCC Responses to Acceptable Use and Privacy Observations

An AmeriCorps Program

National
Civilian
Community
Corps

MEMORANDUM

TO: Merlene Mazyck, National Director NCCC

FROM: LaQuine Roberson, Region Director NCCC

DATE: January 12, 2009

SUBJECT: IG Security Infractions

In response to the infractions described in the IG Report issued in November 2008, the Atlantic Region has taken the following corrective action:

Unsecured computer lab – As of January 9, 2009, we have secured the doors to computer lab pursuant to VA requirements and NCCC guidelines. In addition, we have removed excess locking devices that were found in the lab. The computer lab will now be opened during designated hours, which will be posted on the door of the lab and in Building 15. The duty Team Leaders (one of which will be located in the computer lab) will be responsible for opening, closing and monitoring the lab. The hours of operation are as follows: Sunday – Thursday 7 pm until midnight and Friday – Saturday 7 pm until 1 am. The duty Team Leaders located in the lab will be responsible for assigning computers to individual users and maintaining a computer log.

Unsecured Member Houses --The Atlantic Region is currently investigating the cost effectiveness of acquiring a swipe key entry system to install in 9H. Such a system is cost prohibitive for the individual houses. As such, we will continue to issue keys to the residents and enforce a locked-door policy to maintain security. The SSS in collaboration with the Unit Leaders will be responsible for conducting a 25% (28 houses) health and welfare inspection on a weekly basis. The inspection will consist of checking for locked doors for security, cleanliness of houses and inspection of smoke and CO2 alarms. An inspection log will be kept to verify all inspections.

Corporation for
NATIONAL &
COMMUNITY
SERVICE

AMERICORPS NATIONAL CIVILIAN COMMUNITY CORPS

February 4, 2009

TO: Kenneth C. Bach
Assistant Inspector General for Support

FROM: Mikel Herrington
Acting Director AmeriCorps NCCC

SUBJECT: Comments on the Office of the Inspector General's (OIG) Draft Report *Corporation Internet Use & Information Privacy Study Report 09-03*

AmeriCorps NCCC management has reviewed the findings and recommendations included in the *Corporation Internet Use & Information Privacy Study Report, OIG Report Number 09-03*. The OIG made three observations from its review at the Western and Atlantic Region campuses; two of the three observations are the same. Below is our response to the two discrete observations made in the OIG report. All NCCC campuses that maintain computer labs for their members have assessed the risk of the physical and logical access controls and compliance with Corporation acceptable information resources use and privacy policy. Please note that the Southwest region campus member computer facilities and equipment are not owned or maintained by the Corporation. The lab is owned and operated by the campus's landlord, Teikyo University.

Observations No. 1 and No. 3 (observed at both campuses)
No technology or manual methodology was in place to detect, assign responsibility for, or limit unacceptable use of information resources.

CNCS, AmeriCorps NCCC response: As a preliminary measure, NCCC will implement a sign-in/sign-out sheet for any member using computer resources. These lists will be kept by the campuses' Deputy Directors. This measure will be implemented by February 13, 2009.

NCCC will work with the Corporation's Office of Information Technology (OIT) to identify and purchase content filtering software to prevent future abuses. Campus staff will be trained in the use of the software. The Deputy Director at each campus will be responsible for monitoring the member computers in the labs. NCCC will meet with OIT by February 13, 2009 and shortly thereafter provide an update to the OIG on the implementation timeline.

Observation No. 2
NCCC - Perry Point does not effectively control physical access to its computer lab.

CNCS, AmeriCorps NCCC response: All campuses will be required to identify computer lab hours and post them on the lab doors. This will be implemented by February 13, 2009.

NCCC member computer labs have now been properly secured either through a locked or card access system.

cc: Richard Friend, Acting Chief Information Officer
Juliette Sheppard, Director of Information Assurance
Nick Zefran, Director of Member Services, AmeriCorps NCCC