Office of Inspector General
Corporation for National and Community Service

STUDY OF CORPORATION FOR NATIONAL AND COMMUNITY SERVICE'S INTERNET USE AND MANAGEMENT CONTROLS

OIG REPORT NUMBER 06-39

Corporation for NATIONAL & COMMUNITY SERVICE

Prepared by:

Carson & Associates, Inc.
4720 Montgomery Lane, Suite 800
Bethesda, Maryland 20814

This report was issued to Corporation management on August 1, 2006. Under the laws and regulations governing follow-up, the Corporation is to make final management decisions on the report's observations and suggestions no later than February 1, 2007, and complete its corrective actions by August 1, 2007. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

Corporation for NATIONAL & COMMUNITY SERVICE

OFFICE OF INSPECTOR GENERAL

Study of Corporation for National and Community Service's Internet Use and Management Controls

Report 06-39

OIG Summary

The Office of Inspector General (OIG), Corporation for National and Community Service (Corporation), contracted with Richard S. Carson and Associates, Inc. (Carson) to assess the Corporation's management controls for monitoring, identifying, and resolving noncompliance with its Internet use policy.

The study focused on compliance with the Corporation's Policy 375, *Internet and E-mail Access and Acceptable Use*, dated August 23, 1999. It also assessed the design, documentation, and implementation of corresponding management controls. The study generally covered Internet usage on networked and non-networked Corporation-owned computers from January 4, 2006, through April 5, 2006.

The study, in general, concluded that the Corporation should include its *Network Rules of Behavior* as part of Policy 375 and update both documents. It also revealed apparent inappropriate Internet use on networked and non-networked Corporation-owned Computers. The study provides observations, representing opportunities for improvement, and suggestions for change.

In its response to the study, the Corporation indicated it has prepared an action plan to resolve the issues raised and also plans to revise Policy 375. The Corporation's response is included as the Appendix.

Carson is responsible for this study and the conclusions expressed therein. However, our review disclosed no instances in which Carson did not comply, in all material respects, with the standards issued by the President's Council on Integrity and Efficiency (*Quality Standards for Inspections*, January 2005).

This study is a matter of public record, and its distribution is not limited.

July 31, 2006

Ms. Carol Bates
Assistant Inspector General
Office of Inspector General
Corporation for National & Community Service
1201 New York Ave., N.W., Suite 830
Washington DC 20525

Dear Ms. Bates:

This letter is to inform you that we have completed the attached Study of Internet Use and Management Controls on behalf of the Office of Inspector General (OIG) of the Corporation for National and Community Service (CNCS).

Sincerely,

Diane C. Reilly

Diane C. Reilly
Vice President

Enclosures:
Study of Internet Use and Management Controls

RICHARD S. CARSON & ASSOCIATES, INC.
www.carsoninc.com
4720 Montgomery Lane • Suite 800 • Bethesda, MD 20814-3444 • 301.656.4565 • Fax: 301.656.4806

Executive Summary

This Office of Inspector General (OIG) study examines the Corporation for National and Community Service's (Corporation) Internet use and management controls. It is issued under an OIG engagement with Richard S. Carson and Associates, Inc. (Carson), which conducted the study from January 10, 2006, through May 26, 2006. This independent study provides conclusions and observations, identifies areas for improvement and, where applicable, makes suggestions for improvement. Compliance with the Corporation's Policy 375 and other applicable Federal laws and guidelines are the basis for formulating our conclusions, observations, and suggestions.

A major focus of this study is the Corporation's degree of compliance with its Policy 375, *Internet and E-mail Access and Acceptable Use*, dated August 23, 1999. It also addresses the design, documentation, and implementation of corresponding management controls for monitoring, identifying, and resolving noncompliance.

This study found that the Corporation needs to update Policy 375 and formally include its Network Rules of Behavior (ROB) in the document. It also needs to update the ROB to include details on all inappropriate Internet uses that are contained in Policy 375. The Corporation should also configure its Internet monitoring technologies in accordance with Policy 375. In the area of management controls, the Corporation should formalize its methodology, monitoring processes and procedures used to enforce compliance with Policy 375.

The study also revealed instances of apparent inappropriate Internet use on networked and non-networked Corporation-owned computers. During visits to National Civilian Community Corps (NCCC) campuses at Perry Point, MD, and Sacramento, CA, we determined that approximately 20 percent of the personal computers tested contained inappropriate images that are expressly prohibited by Policy 375.

At the exit conference held on May 15, 2005, Corporation officials generally concurred with the observations and suggestions. In its formal response on July 18, 2006, included verbatim in the Appendix, the Corporation states that it has begun to resolve the issues raised in the areas of policy, technology, and management controls. The Corporation prepared a management action plan, which included plans for revising Policy 375. The management action plan, when fully implemented, should strengthen controls over Internet use.

Acronyms and Abbreviations

CIO	Chief Information Officer
IM	Instant Messaging
ICQ	I Seek You
IT	Information Technology
NCCC	AmeriCorps*NCCC (National Civilian Community Corps)
OIG	Office of Inspector General
OIT	Office of Information Technology
ROB	Rules of Behavior

Table of Contents

Executive Summary i
Acronyms and Abbreviations ii
Table of Contents iii
Purpose 1
Observations 1
Policy 1
  Observation – Policy 375 Does Not Address All Users of Corporation IT Resources 1
  Observation – Policy 375 Does Not Reflect Current Internet Use and Technologies 2
Technology 2
  Observation – Output Produced by Internet Monitoring Technologies Should be Tested 2
Management Controls 3
  Observation – Lack of a Unified, Cohesive, and Effective Methodology 3
  Observation – Lack of Consistent Review of Monitoring Data 3
  Observation – Network Rules of Behavior Need Improvement 4
Consolidated List of Suggestions 5
  Policy 5
  Technology 5
  Management Controls 5
Methodology 6
  Networked Computers 6
  NCCC Site Visits 7

APPENDIX – CORPORATION RESPONSE TO THE STUDY

Purpose

The objectives of this independent study were to:

- Assess the Corporation's degree of compliance with Policy 375 and the design, documentation, and implementation of corresponding management controls.
- Assess the Corporation's management controls for monitoring, identifying, and resolving noncompliance with Policy 375.
- Conduct testing of Internet use on networked Corporation-owned equipment to identify prohibited practices and instances of abuse.
- Conduct testing of Internet use on non-networked Corporation-owned equipment to identify prohibited practices and instances of abuse.

Observations

We found that the Corporation needs to update Policy 375 and include its Network Rules of Behavior (ROB). The ROB should detail prohibited use as specified in Policy 375. The ROB, which employees must review and then sign a document attesting to that review, does not specifically list all types of inappropriate and banned Internet use. The ROB merely references Policy 375, which includes such detailed information. Also, not all persons with access to Corporation-owned computers are currently required to review the ROB and sign attesting documentation.

The Corporation should also configure its Internet monitoring technologies to align with Policy 375. In the area of management controls, the Corporation should formalize its methodology, monitoring processes and procedures used to enforce compliance with Policy 375.

The following observations and suggestions, based on our research, analysis, and assessment of the Corporation's Internet use and management controls, fall into in three main areas: policy, technology, and management controls. Our suggestions for improvement are intended to assist the Corporation in determining corrective actions.

Policy

Policy 375 was written in 1999. Since that time, the Internet has evolved, as has its use, greatly expanding the numbers and technological types of abuses that may occur.

Observation – Policy 375 Does Not Address All Users of Corporation IT Resources

Our review of Policy 375 determined that there are inconsistencies in the definition of who is covered. The policy states that any person who uses Corporation-provided information technology resources is subject to the provisions of Policy 375. However, throughout the document, it also states that the Corporation is extending the privilege of Internet and e-mail use

only to employees. There is no mention of members, volunteers, contractors, or other possible users.

Suggestion –

1. Update Policy 375 to include all users of Corporation-owned IT resources. As part of the update, include Network Rules of Behavior for Internet use as part of the Policy.

Observation – Policy 375 Does Not Reflect Current Internet Use and Technologies

Categories of inappropriate use described in Policy 375 do not address such recently developed areas as chat sites/rooms, webcam sites, ICQ (I seek you) sites, instant messaging (IM), and others. Published Internet Usage studies have shown that some users access such Internet technologies and use them as tools to locate, contact, and victimize children and other persons.

Suggestions –

1. Update Policy 375 to reflect current Internet use and technologies.

2. Review and update Policy 375 on an annual basis to reflect current Internet technology levels.

Technology

Observation – Output Produced by Internet Monitoring Technologies Should be Tested

During the course of the study, we found data problems in firewall log files and Internet monitoring reports. Due to these problems, custom on-demand Internet monitoring reports were run by the Office of Information Technology (OIT) that indicated inappropriate Internet use.

This system, which is most heavily relied upon by the Corporation to detect Internet abuse, is not configured to report on all of the prohibited categories included in Policy 375.

Suggestions –

1. Perform regular testing on Internet monitoring technology systems and/or settings to ensure that they are operating as effectively as possible.

2. Configure the Internet monitoring technology to detect and report on Policy 375 categories of inappropriate Internet use.

Management Controls

Management processes and procedures to implement Policy 375 are not formal or consistently applied. The Corporation also lacks a unified, cohesive, and effective methodology that spells out these management processes and procedures. The Corporation conducts network security awareness training, which addresses Internet use. The ROB references Policy 375, but it does not supplement the policy because it is lacking in detail on prohibited and inappropriate Internet uses.

Observation – Lack of a Unified, Cohesive, and Effective Methodology

The Corporation's current Internet abuse monitoring protocol is not documented; it lacks written procedures for acting upon different violations and for the collection of supporting evidence. The current monitoring does not apply a multi-dimensional approach (multiple category comparison), which is critical to profiling high-risk users. Further, no trend analyses are conducted that would show current or emerging patterns of inappropriate Internet use behavior.

Suggestions –

1. Develop procedures to act upon various types of Internet use violations. These procedures should take into account Federal statutes, which specifically prohibit certain types of Internet use behavior.

2. Develop procedures for documenting violations.

3. Perform multi-dimensional analyses.

4. Perform analyses to identify Internet usage trends for prohibited categories.

5. Conduct periodic reviews of Policy 375.

6. Remind users of their responsibilities, as set forth in Policy 375, on a regular basis.

Observation – Lack of Consistent Review of Monitoring Data

We found that, while monitoring was performed, it was not conducted on a regularly scheduled basis. It is essential that monitoring be timely and consistent in order for enforcement to be effective.

Suggestions –

1. Formalize monitoring processes and procedures, including frequency.

Observation – Network Rules of Behavior Need Improvement

The ROB do not adequately supplement Policy 375. The existing ROB states, "Use of all CNS computer resources (personal computers, laptops, the CNS Network, communication lines, and computing facilities) are restricted in accordance with CNS's Internet and Email Access and Acceptable Use Policy 375." The ROB references Policy 375, but contains no additional information or description of what behaviors constitute inappropriate Internet use.

Also, non-networked users who use Corporation-owned equipment are not currently required to sign a document attesting to their agreement to abide by the ROB.

Suggestion –

1. Improve Network Rules of Behavior to adequately supplement Policy 375.

2. Require all users of Corporation-owned equipment to sign the documentation related to the Network Rules of Behavior.

Consolidated List of Suggestions

Policy

1. Update Policy 375 to include all users of Corporation IT resources. As part of the update, include Network Rules of Behavior for Internet use as part of the Policy.

2. Update Policy 375 to reflect current Internet use and technologies.

3. Review and update Policy 375 on an annual basis to reflect current Internet technology levels.

Technology

1. Perform regular testing on Internet monitoring technology systems and/or settings to ensure that they are configured correctly and/or operating.

2. Configure the Internet monitoring technology to detect and report on Policy 375 categories of inappropriate Internet use.

Management Controls

1. Develop procedures to act upon various types of Internet use violations. These procedures should take into account Federal statutes, which specifically prohibit certain types of Internet use behavior.

2. Develop procedures for documenting violations.

3. Perform multi-dimensional analyses.

4. Perform analyses to identify Internet usage trends for prohibited categories.

5. Conduct periodic reviews of Policy 375.

6. Remind users of their responsibilities, as set forth in Policy 375, on a regular basis.

7. Formalize monitoring processes and procedures, including frequency.

8. Improve Network Rules of Behavior to adequately supplement Policy 375.

9. Require all users of Corporation-owned equipment to sign the documentation related to the Network Rules of Behavior.

Methodology

We conducted our examination in three major areas: policy, technology, and management controls; using analytical and forensic tools and methodologies to review the Corporation's monitoring, identification and resolution of incidents of noncompliance with its Internet use policy.

We coordinated all meetings at Corporation Headquarters and NCCC campus site visits with Corporation personnel, who also accompanied the reviewers during campus visits and notified campus directors in advance. Campus directors assisted the reviewers in locating and accessing non-networked computers and provided information on the computers' methods of accessing the Internet.

Networked Computers

We reviewed Policy 375 to determine whether it was comprehensive and relevant to the current information technology environment and interviewed Corporation OIT staff to identify any practices and written procedures used to manage Internet use and enforce Internet use policy. We also examined the Corporation's network security awareness training program and Network Rules of Behavior to verify the level of user understanding of the allowed and disallowed Internet uses defined in Policy 375.

We reviewed the Corporation's infrastructure to determine what technology-based Internet management mechanisms existed and whether they were correctly placed, configured, and operating.

We collected and analyzed static data provided by the Corporation. Static data consisted of copies of the Internet monitoring solution's HTML reports for June through December 2005, as well as the reports for January 4, 2006, through April 5, 2006. Copies of the firewall logs taken from the Corporation's firewall for the corresponding period January 4, 2006, through April 5, 2006 were also provided for analysis. Data availability issues with the Internet monitoring solution's HTML reports caused us to adjust our methodology and focus on the January 4, 2006, through April 5, 2006, firewall logs as the primary source of data for our analysis.

For networked computers, the Internet monitoring solution's HTML reports were manually inspected. During this process, each event listed in the report was verified as either a legitimate event or false positive for the category for which the report was generated (adult, sexually explicit, gambling, games, freeware downloads, hosting-personal, relationship-dating, hate-extremism, or violence-profanity). The verification was performed by going to the URL referenced in the report and confirming that it had or had not been legitimately identified as an inappropriate Internet use.

The automated log file analyzer Cyfin Reporter was used to analyze the source data provided from the Corporation's firewall. Cyfin Reporter was run on converted ASCII files using all the categories of potential Internet use/abuse reported upon in the Internet monitoring solution, as well as additional categories defined in our analysis tool. Again, events identified by the tool were verified as legitimate or false positive.

NCCC Site Visits

Visits were made to two NCCC campuses in the following order: Perry Point, MD, and Sacramento, CA.

At each location, we scanned the hard drives of individual non-networked computers that use DSL and cable modem for Internet access. The scanning tools were used to read, gather, and interpret data contained on the computers. The scans were run on both active files and on deleted files that were recovered using an undelete tool. The scanning tool produced HTML reports, which were examined on site for violations. As a quality check, these reports were also saved and examined in more detail following the visit.

We scanned the temporary Internet files stored on each computer, as well as the remainder of the hard drive for any other downloaded Internet files.

We used the scanner Snitch Professional to scan each computer hard drive for inappropriate images, movies, and audio files, as well as Internet history files, zipped and other data files, including zipped files. We then used a keyword database and SkinScan technology to identify possible violations. Suspected violations were then manually verified.

At the NCCC campuses, data collection and automated analysis occurred concurrently due to the nature of the tool being used.

This independent study was conducted in accordance the President's Council on Integrity and Efficiency's Inspection and Evaluation Guidelines and best practices for evaluating Internet use and management controls.

Corporation for
NATIONAL & COMMUNITY SERVICE

July 18, 2006

TO: Carol Bates
Assistant Inspector General for Audit

FROM: David Eisner
Chief Executive Officer

CC: Rudy Mazariegos, Chief Information Officer
Amy Mack, Chief of Staff
Frank Trinity, General Counsel
William Anderson, Deputy Chief Financial Officer
Kim Sweet, Senior Advisor

SUBJECT: Request for Comments on OIG Draft Report, *"Corporation for National and Community Service's Internet Use and Management Controls"*

Thank you for the opportunity to comment on the draft.

The Chief Information Officer has already begun to resolve the issues raised, as noted in our Incident Response Management Action Plan, our planned revision of Policy 375, and a review of the management, operation and technical controls on monitoring internet use.

We appreciate the work that the OIG and Carson put into this effort, and will continue to base our actions on the report's observations and suggestions.