UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audits and Computer Crime Investigations

DATE: July 20, 2010

TO: Danny Harris
Chief Information Officer
Office of the Chief Information Officer

Richard Gordon
Chief Information Officer
Federal Student Aid

FROM: Charles E. Coe, Jr. /s/
Assistant Inspector General

SUBJECT: Investigative Program Advisory Report (IPAR)
Bypassing of Web Content Filtering (Case #10-110249)
Control No. L21K0001

Department Program: Information Assurance

The Information Assurance (IA) Program serves as a major component within the Department of Education (Department) for protecting information that is collected, processed, transmitted, or disseminated in any form. The mitigation of risks to prevent the unauthorized disclosure, alteration, or destruction of Department information is vital to the successful execution of the Department's many business functions. The IA Security Policy establishes policies to ensure compliance with Federal laws and regulations, thus ensuring adequate protection on the Information Technology (IT) resources.

In the Office of the Chief Information Officer's (OCIO's) Security Policy Handbook, OCIO-01, section 4.1.3.3, Internet, and OCIO 1-104, Personal Use of Government Equipment and Information Resources, Section D, Policy to Filer Inappropriate Internet Material, the Department outlines policies related to the use of the Internet. The Department provides employees with appropriate Internet access to facilitate research, learning, and the accomplishment of the Department's mission. In so doing, the Department exercises sound judgment in identifying suitable and worthwhile material for general access. The policy also addresses how an employee may legitimately access filtered sites through OCIO.

Deficiencies and/or Mismanagement

Recent investigations have revealed multiple users throughout the Department and specifically in Federal Student Aid (FSA) and OCIO have circumvented web filtering by [redacted] Specifically, users use the [redacted] to bypass

Blue Coat web content filtering configurations. The [redacted] goes undetected under the current Blue Coat configurations.

The most common usage has been to access web-based email and social networking sites. However, a user can access virtually any blocked site utilizing this technique if the [redacted] When interviewed, one employee indicated this practice was common throughout FSA.

Recommendations

1. It is recommended that OCIO and FSA OCIO educate users that bypassing web filtering is a violation of Department policy that can expose the user and the Department to risks.

2. It is recommended that OCIO and FSA OCIO assess whether it is practical to monitor [redacted] through Blue Coat, and if not consider other monitoring or filtering methods.

Please advise this office within 90 days of any corrective action taken or planned because of the recommendations contained in this IPAR.