Office of Inspector General
Legal Services Corporation

Inspector General
Jeffrey E. Schanz

3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

FRAUD ALERT
17-01

TO: **Executive Directors**

FROM: **Jeffrey E. Schanz**
Inspector General

DATE: **May 30, 2017**

SUBJECT: **Computer Warning Banners**

The purpose of this Fraud Alert is to inform you of issues that have come to the attention of the Office of Inspector General (OIG) during recent investigations at Legal Service Corporation (LSC) grantees.

In many cases, information vital to OIG investigations is contained on grantee-owned computers used by employees who may be engaged in misconduct, fraud, or LSC restricted activities. It appears, however, that many grantees do not have written policies giving employees notice concerning prohibited uses of their computer equipment. In addition to such policies, grantees should have a warning banner (banner) that appears while employees are logging on and notifies employees of their rights when using their grantee-owned computer.

A "banner" is verbiage that an end-user sees at the point of access to a system which sets forth the expectations for users regarding authorized and acceptable use of a grantee-owned computer system, data, and network access capabilities. Banners also provide a warning to any external intruder who may attempt to gain access to your data. A banner and related policy protects the organization, its users, and customers by informing those who would exploit the computer system or network that unauthorized activities are not permitted.

An effective banner provides notice to employees and external threats that unauthorized use of the computer system may result in administrative or criminal consequences. Failure to include a banner regarding authorized and acceptable use of your computer system may make it difficult for management to investigate potential violations when they occur. In some cases,

organizations have been held accountable for alleged violations of individual privacy because no notice was given and acknowledged regarding authorized monitoring of users' activities on company-owned computers.

Express, comprehensive, written policies can remove an employee's expectation of privacy regarding the use of workplace technology because a continued expectation of privacy, after such notice has been communicated, would not be reasonable. Written policies should include notification from the employer that improper use of the computer or e-mail system is prohibited; that the employer monitors the use of the employee's computer or e-mail; and that the employer and authorized third parties can access the employee's work computer or e-mails. In addition to such policies, the employer should create a banner that appears when the computer is turned on or the e-mail system is accessed that expressly warns the user about the lack of privacy and the employer's right to monitor.

The following is an example of a banner that might appear on a grantee's computer:

> Warning: This system is restricted to XYZ Grantee authorized users for official business purposes only. Unauthorized access or use is a violation of XYZ Grantee policy and the law. This system may be monitored for administrative and security reasons. By proceeding, you acknowledge that (1) you have read this notice and understand you have no reasonable expectation of privacy as you use this XYZ-owned computer, (2) you consent to system monitoring, and (3) you understand improper use of the system may result in administrative discipline, including civil or criminal penalties.

An employer that fails to adopt policies or banners or, having adopted them, does not enforce the policies or does not enforce them consistently for all employees, may unwittingly encourage employees to believe they have a reasonable expectation of privacy concerning the contents of their work computers.

Finally, because laws regarding workplace privacy differ from jurisdiction to jurisdiction, grantees should consult relevant state and local laws in developing policies or warnings regarding use of program computers.

For any questions concerning this Fraud Alert, please contact Dan O'Rourke, Assistant Inspector General for Investigations, at 202-295-1651 or dorourke@oig.lsc.gov.

I hope you find this Fraud Alert useful. Our Fraud Hotline telephone number is 800-678-8868 or 202-295-1670; e-mail hotline@oig.lsc.gov; fax 202-337-7155.