LEGAL SERVICES CORPORATION
LSC 2011 Grant Assurances

Guidance on Grant Assurance #8(a) regarding "Information Security"

LSC grant Assurance 8(a) informs Applicants for 2011 grants that:

"No later than December 31, 2011, it will have information security system that ensures confidentiality and security of its operations, assets, data, and files."

Note: Information security should be practical and based on a risk assessment and a cost/benefit analysis.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1. *integrity*, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

2. *confidentiality*, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information

3. *availability*, which means ensuring timely and reliable access to and use of information.

Below are suggested solutions for internal information security. These suggestions will help ensure that Applicant staff is aware of and do not breach information security requirements and protocols:

1. written information security policy that ensures confidentiality of operations, assets, data, and files
2. staff nondisclosure agreements
3. verification procedures
4. access authorization mechanisms
5. staff training and notice to end-users regarding the grantee's security requirements and policy
6. encryption for external instant messaging used to communicate confidential client data

Below are suggested solutions for external information security. These suggestions will help ensure that external entities are aware of and do not breach Applicant's information security requirements and protocols.

1. current patches and definition updates for operating systems and antivirus software
2. maintenance of backup systems
3. plans for disaster recovery
4. policies regarding the use of the Internet and office technology
5. policies regarding the retention and deletion of data
6. policies to ensure that electronic equipment (e.g., laptop computers, PDAs) is secure from unauthorized access when the equipment is not in use by staff
7. notice to end-users that unauthorized access to information, access to information systems and use of information will be prosecuted

What LSC will look for when onsite:

1. Description of the risk assessment conducted and cost/benefit analysis conducted
2. Written procedures on how the grantee ensures the security of confidential information in digital and print form internal and external sources
3. The schedule and process for regular and systematic evaluation of the security system

Please contact the LSC competitive grants service desk at competition@lsc.gov if you have any questions regarding this matter.