UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Working for America

www.opm.gov

CFC MEMORANDUM 2009 – 6 **May 19, 2009**

TO: **LOCAL FEDERAL COORDINATING COMMITTEES, AND PRINCIPAL COMBINED FUND ORGANIZATIONS**

FROM: **MARK W. LAMBERT**
DIRECTOR, OFFICE OF CFC OPERATIONS

SUBJECT: **LOCAL CAMPAIGN RESPONSIBILITY TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION AND OTHER SENSITIVE INFORMATION**

The U.S. Office of Personnel Management (OPM) is dedicated to ensuring donor and charity information is adequately protected within the operations of the Combined Federal Campaign (CFC). This memorandum provides guidance to local campaigns on the responsibilities and procedures for handling Personally Identifiable Information (PII) and Other Sensitive Information (OSI).

Definitions

OPM generally defines PII as information that:

1. Can be used to discern or trace a person's or entity’s identity; and
2. Alone, or combined with other information, can be used to compromise the integrity of agency records relating to a person by permitting access to unauthorized disclosure of these records.

For example, a name alone would generally not constitute PII, but when linked to his or her social security number (SSN), date of birth, or mother's maiden name, would constitute PII.

OPM defines OSI as any information related to the Federal donor or charitable entity that could alone, or combined with other information, be used to commit fraudulent acts against the Federal donor or charitable entity. For example, a donor's home address, bank account number or routing number or a charitable entity's bank account number or routing number would constitute other sensitive information.

Background

Local campaigns handle certain information that alone and or combined would constitute PII or OSI (see definitions above for examples). Local campaigns use this information to process Federal donor pledges and pay charitable entities via electronic funds transfers.

CFC regulations only allow the use or release of donor and charitable information in specific circumstances, including pledge processing, accounting, disbursements to charities, and in the design and implementation of award programs. For further information on these authorized uses and release of information, please reference 5 CFR §§ 950.105(d)(6), 105(d)(8), 105(d)(11), 601(a), 601(c) and 901(i)(2).

As communicated in CFC Memorandum 2007-8, campaigns are reminded it is not permissible to collect, store, or temporarily use a donor's SSN. This includes use by any vendor hired to implement online giving within the campaign. The only authorized online giving system that can handle SSNs is Employee Express, as it is an official Federal Human Resource system subject to all Federal laws and requirements related to PII and security. Any campaign collecting or storing donor SSNs must immediately remove that data from their records and files, permanently destroy such records, whether held in electronic or paper format, and cease all future collections of this data. Local campaigns not in compliance are subject to sanctions and penalties as provided in CFC regulations at 5 CFR § 950.603.

Campaign Responsibilities

It is the local campaign's responsibility to ensure it has implemented adequate controls to protect against the unauthorized release and misuse of personally identifiable and other sensitive information. Local campaigns are responsible for the proper handling of PII and OSI, regardless of location. OPM recommends the following safeguards:

1. Proper control and handling of PII and OSI residing on computers, on removable media, and on paper and electronic documents;
2. Ensuring portable data storage and communication devices are properly controlled and secured at all times;
3. Proper marking, control and storage of printouts and other paper documents containing PII and OSI in the campaign's possession; and
4. Encrypting any PII or OSI as an attachment when transmitting it through email. Do not send PII or OSI in the content of an email.

Note: Proper control and handling of PII and OSI may include:

- Ensuring systems containing PII or OSI, which are accessible by computer:
    - require the use of user IDs and passwords for system access and
    - make use of timeout during short as well as long periods of inactivity;

- Restricting access to PII and OSI to only those individuals who have a business need for it;
- Prohibiting copies of PII or OSI files to unsecured drives, storage devices and personal home computers/laptops; and
- Keeping paper documents with PII or OSI in locked storage rooms or safes which can only be accessed by authorized users or security personnel.

Note: Proper marking, control and storage of information containing PII or OSI may include:

- Labeling and communicating to staff which information is considered PII or OSI;
- Restricting access to PII and OSI to those individuals who require access; and
- Keeping paper documents with PII or OSI in locked storage rooms or safes which can only be accessed by authorized users or security personnel.

Local Federal Coordinating Committees (LFCC) should ensure any organization applying for the Principal Combined Fund Organization (PCFO) understands these responsibilities and addresses its plan for protecting PII and OSI in the written campaign plan provided with its application to administer the CFC.

Reporting PII Breaches

A breach of PII or OSI includes the actual or suspected loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of PII or OSI whether physical or electronic. In accordance with 5 CFR § 950.104(b)(13) a LFCC is required to immediately report to OPM all potential PII data and OSI breaches -- whether they involve paper documents or electronic information. Potential PII data and OSI breaches must be reported within 30 minutes of discovery via telephone on (202) 606-2564 or email at cfc@opm.gov to OPM. Both actual and suspected breaches should be reported, even if it is believed the breach is limited, small, or insignificant. In addition, the LFCC is reminded of its obligation to report all security incidents involving PII to US-CERT within the Department of Homeland Security (see US- CERT web site at http://www.us-cert.gov/federal/reportingRequirements.html) and providing notification to victims of PII or OSI breaches, as appropriate.

Your cooperation in protecting donor and charity privacy and preventing identity theft is appreciated. Questions and comments on this guidance should be directed to the Office of Combined Federal Campaign Operations at cfc@opm.gov.