U. S. Department of Justice

MAR 20 2008

Washington, D.C. 20530

MEMORANDUM FOR BUREAU PROCUREMENT CHIEFS

FROM: Michael H. Allen
Senior Procurement Executive

SUBJECT: *DOJ Procurement Guidance Document 08-04, Security of Systems and Data, Including Personally Identifiable Information*

My memorandum of January 18, 2008, notified you of recent instances of contractor loss of equipment containing sensitive data relating to Department programs or personnel. Section A of this guidance document sets forth a required security clause addressing Department systems and data, including provisions governing the use of laptops by contractors, to be included in all current and future contracts where a contractor handles data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel. Please note that in Section A, paragraphs a, b, and d apply to all data, even data that may not be personally identifiable information (PII)[1]. Section B of this guidance document sets forth a required clause that must be used in contracts involving personally identifiable information obtained by the Department from a contractor, such as an information reseller or data broker. This guidance document supersedes Procurement Guidance Document 06-10.

A. Security of Systems and Data, Including Personally Identifiable Information.

The following clause must be used in any contract where the contractor handles data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel.

[1] The term "personally identifiable information," as defined by OMB, means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Security of Systems and Data, Including Personally Identifiable Data.

a. Systems Security

The work to be performed under this contract requires the handling of data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel.

For all systems handling such data, the contractor shall comply with all security requirements applicable to Department of Justice systems, including but not limited to all Executive Branch system security requirements (*e.g.*, requirements imposed by OMB and NIST), DOJ IT Security Standards, and DOJ Order 2640.2E. The contractor shall provide DOJ access to and information regarding the contractor's systems when requested by the Department in connection with its efforts to ensure compliance with all such security requirements, and shall otherwise cooperate with the Department in such efforts. DOJ access shall include independent validation testing of controls, system penetration testing by DOJ, FISMA data reviews, and access by the DOJ Office of the Inspector General for its reviews.

The use of contractor-owned laptops or other media storage devices to process or store data covered by this clause is prohibited until the contractor provides a letter to the contracting officer (CO) certifying the following requirements:

1. Laptops must employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 approved product;
2. The contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;
3. Mobile computing devices will utilize anti-viral software and a host-based firewall mechanism;
4. The contractor shall log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is sensitive information unless designated as non-sensitive by the Department;
5. Contractor-owned removable media, such as removable hard drives, flash drives, CDs, and floppy disks, containing DOJ data, shall not be removed from DOJ facilities unless encrypted using a NIST FIPS 140-2 approved product;
6. When no longer needed, all removable media and laptop hard drives shall be processed (sanitized, degaussed, or destroyed) in accordance with security requirements applicable to DOJ;
7. Contracting firms shall keep an accurate inventory of devices used on DOJ contracts;
8. Rules of behavior must be signed by users. These rules shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and personally identifiable information;

9. All DOJ data will be removed from contractor-owned laptops upon termination of contractor work. This removal must be accomplished in accordance with DOJ IT Security Standard requirements. Certification of data removal will be performed by the contractor's project manager and a letter confirming certification will be delivered to the CO within 15 days of termination of contractor work;

b. Data Security

By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified in paragraph a, in the event of any actual or suspected breach of such data (*i.e.*, loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the contractor will immediately (and in no event later than within one hour of discovery) report the breach to the DOJ CO and the contracting officer's technical representative (COTR).

If the data breach occurs outside of regular business hours and/or neither the CO nor the COTR can be reached, the contractor shall call the DOJ Computer Emergency Readiness Team (DOJCERT) at 1-866-US4-CERT (1-866-874-2378) within one hour of discovery of the breach. The contractor shall also notify the CO as soon as possible during regular business hours.

c. Personally Identifiable Information Notification Requirement

The contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification shall be coordinated with the Department, and shall not proceed until the Department has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor shall be coordinated with, and be subject to the approval of, the Department. The contractor assumes full responsibility for taking corrective action consistent with the Department's Data Breach Notification Procedures, which may include offering credit monitoring when appropriate.

d. Pass-through of Security Requirements to Subcontractors

The requirements set forth in Paragraphs a through c above, apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the contractor.

B. Information Resellers or Data Brokers

For contracts where the Department obtains PII from a contractor (such as an information reseller or data broker) but the contractor does not handle the data described in Section A of this guidance document, the following clause must be used:

> Information Resellers or Data Brokers
>
> Under this contract, the Department obtains personally identifiable information about individuals from the contractor. The contractor hereby certifies that it has a security policy in place which contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, lost or acquired by an unauthorized person while the data is under the control of the contractor. In any case in which the data that was lost or improperly acquired reflects or consists of data that originated with the Department, or reflects sensitive law enforcement or national security interest in the data, the contractor shall notify the Department contracting officer so that the Department may determine whether notification would impede a law enforcement investigation or jeopardize national security. In such cases, the contractor shall not notify the individuals until it receives further instruction from the Department.

In my memorandum dated January 18, 2008, I encouraged you to identify all current and upcoming contracts that require the exchange of PII and other Departmental data between the contractor and the Department that need to include this security coverage. All current contracts to be covered will need to be modified to include the applicable clause, within 60 days of the date of this memorandum. Thus, there is a 60-day grace period on all current contracts, after which, under the security clause, laptops or devices not covered by certification letters may not be used on DOJ contracts. Contracting officers should alert contractors of this requirement as soon as possible in order to avoid disruption in the use of laptops. A request for a waiver from the requirement to include these clauses, or deviations from the language of these clauses (except those that are more stringent), must be made in writing to the Senior Procurement Executive. Permission for a deviation or waiver will only be granted in unusual circumstances.