2952.224-70 Privacy Breach Notification Requirements.

As prescribed in 2924.103-70, insert the following clause:

Privacy Breach Notification Requirements (APR 2018)

A. Definitions

“Breach” is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where—

(a) A person other than an authorized user accesses or potentially accesses Personally Identifiable Information (PII); or

(b) An authorized user accesses or potentially accesses PII for an unauthorized purpose.

“Information” is defined as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular No. A-130, Managing Federal Information as a Strategic Resource).

“Information System” is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

“Personally Identifiable Information” is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual (see OMB Circular No. A-130, Managing Federal Information as a Strategic Resource).

B. Requirements

(a) Contractors and subcontractors that collects or maintains federal information on behalf of the agency or uses or operates an information system on behalf of the agency shall comply with federal law *e.g.,* FISMA 2014, E-Government Act and the Privacy Act. Additionally, the contractor shall meet OMB directives and National Institute of Standards and Technology Standards to ensure processing of PII is adequately managed.

(b) The contractor shall:

(1) Properly encrypt PII in accordance with appropriate laws, regulations, directives, standards, or guidelines;

(2) Report to DOL any suspected or confirmed breach in any medium or form, including paper, oral, and electronic within one hour of discovery;

(3) Cooperate with and exchange information with DOL (contracting officer and Contracting Officer's Representative) as well as allow for an inspection, investigation, forensic analysis, as determined necessary by the DOL, to effectively report and manage a suspected or confirmed

breach;

(4) Maintain capabilities to determine what DOL information was or could have been compromised and by whom, construct a timeline of user activity, determine methods and techniques used to access federal information, and identify the initial attack vector;

(5) Ensure staff who have access to DOL systems or information are regularly trained to identify and report a security incident. This includes the completion of any DOL mandatory training for contractors;

(6) Take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised.

(7) Report incidents per DOL incident management policy and US-CERT notification guidelines.

(c) Remedy:

(1) A report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII. If the contractor is determined to be at fault for the breach, the contractor may be financially liable for government costs incurred in the course of breach response and mitigation efforts;

(2) The contractor shall take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised. Additionally, the individual or individuals directly responsible for the data breach shall be removed from the contract within 45 days of the breach of data; and

(3) The Government reserves the right to exercise all available contract remedies including, but not limited to, a stop-work order on a temporary or permanent basis to address a breach or upon discovery of a contractor's failure to report a breach as required by this clause. If the contractor is determined to be at fault for a breach, the contractor shall provide credit monitoring and privacy protection services for one year to any individual whose private information was accessed or disclosed. The individual shall be given the option, but the decision is theirs. Those services will be provided solely at the expense of the contractor and will not be reimbursed by the Federal Government.

(End of Clause)

Parent topic: Subpart 2952.2—Text of Provisions and Clauses