

Guidance on the Protection of Personal Identifiable Information

Personal Identifiable Information (PII) is defined as:

Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

Department of Labor (DOL) contractors are reminded that safeguarding sensitive information is a critical responsibility that must be taken seriously at all times. DOL internal policy specifies the following security policies for the protection of PII and other sensitive data:

- It is the responsibility of the individual user to protect data to which they have access. Users must adhere to the rules of behavior defined in applicable Systems Security Plans, DOL and agency guidance.
- DOL contractors having access to personal information shall respect the confidentiality of such information, and refrain from any conduct that would indicate a careless or negligent attitude toward such information. Contract employees also shall avoid office gossip and should not permit any unauthorized viewing of records contained in a DOL system of records. Only individuals who have a "need to know" in their official capacity shall have access to such systems of records.

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Because DOL employees and contractors may have access to personal identifiable information concerning individuals and other sensitive data, we have a special responsibility to protect that information from loss and misuse.

With these responsibilities contractors should ensure that their employees:

- Safeguard DOL information to which their employees have access at all times.
- Obtain DOL management's **written** approval prior to taking any DOL sensitive information away from the office. The DOL manager's approval must identify the business necessity for removing such information from the DOL facility.
- When approval is granted to take sensitive information away from the office, the employee must adhere to the security policies described above.

Contractors should ensure their contract employees are aware of their responsibilities regarding the protection of PII at the Department of Labor. In addition to the forgoing, if contract employees become aware of a theft or loss of PII, they are required to **immediately** inform their DOL contract manager. In the event their DOL contract manager is not available, they are to **immediately** report the theft or loss to the DOL Computer Security Incident Response Capability (CSIRC) team at dolcsirc@dol.gov.