wiley

ALERT

Final FAR Rule Imposes Privacy Training Requirements on a Wide-Range of Contractors

January 12, 2017

WHAT: The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) finalized a five-year-old proposed rule that requires three categories of contractors (and subcontractors) to provide privacy training to their employees: contractors that (i) have access to a system of records; (ii) create, collect, use, store, maintain, disseminate, disclose or otherwise handle personally identifiable information (PII) on behalf of the contracting agency; or (iii) design, develop, maintain, or operate a system of records must provide initial privacy training to their employees and annual training thereafter. Because of the increasing portability of data, highly publicized instances of loss (data breaches), as well as the potential for improper disclosures of PII, the Councils believed imposing this new obligation is vital.

WHEN: The rule was finalized December 20, 2016 and is effective January 19, 2017.

WHAT DOES IT MEAN FOR INDUSTRY: Contracts involving the handling of PII or any involvement with a system of records will now have privacy training obligations for the contractors and any of their subcontractors that also handle PII or are involved with a system of records. Because the rule is focused on the protection of certain types of data (PII and data contained in a system of records), it applies to any FAR-based contract that involves this type information. Thus, there is no exemption for contracts or subcontracts for commercial items, including contracts and subcontracts for commercially available off-the-shelf (COTS) items. While the rule is prescriptive concerning which employees must be trained, the frequency of the training, and the training content, there is some much needed flexibility. For example, the rule acknowledges that some contractors already might be under

Authors

Dorthula H. Powell-Woodson
Partner
202.719.7150
dpowell-woodson@wiley.law

J. Ryan Frazee
Of Counsel
202.719.3751
jfrazee@wiley.law

Practice Areas

Employment & Labor

Employment and Labor Standards Issues in Government Contracting

Government Contracts

Privacy, Cyber & Data Governance

an obligation to provide workforce privacy training (e.g., contractors that must meet the obligations of the HIPAA Privacy Rule). Thus, unless the contracting agency specifies that only agency-provided training is acceptable, any training that meets the minimum content requirements will be deemed acceptable under the rule. However, for contractors to determine whether they can rely on their existing privacy training programs, they must understand each obligation imposed under the rule and assess whether—and if so, to what extent—they must establish a new or enhanced framework for compliance.

- **Who must receive training.** Contractor employees who have access to, design, develop, maintain, or operate a system of records or who handle PII must receive the privacy training. A "system of records" is a term of art that means any group of records, which allows for information retrieval based on an individual's name or other personally identifying characteristic. "PII" includes information that can be used to personally identify an individual, either on its own or when combined with other information that is linked or linkable to that individual.
- **When the training must occur.** Contractors must ensure employees are trained prior to granting them access to a system of records or to any PII. Following the initial training, employees must receive additional training on an annual basis.
- **What the training must cover.** Here, the rule provides some general guidelines, but leaves significant room for variation as to how those guidelines are met. The training must be role-based, cover key elements of safeguarding a system of records or PII, and include both foundational and more advanced levels of training. It must also include testing to demonstrate the knowledge level of employees. And at a minimum, it must cover the following elements:
  - The provisions of the Privacy Act of 1974,
  - The appropriate handling and safeguarding of PII,
  - The authorized and official use of a system of records or PII,
  - The restriction on the use of unauthorized equipment to access or handle PII,
  - The prohibition of unauthorized use of a system of records, or access, use, or disclosure of PII, and
  - The procedures to be used in the event of a suspected or confirmed breach.
- **Who designs and provides the training.** Here is where the rule introduces the most uncertainty. The rule allows the contractor "to provide its own training or to use the training of another agency," unless the contracting agency requires that its own training be used. A point worth noting: agency-developed or agency-conducted training will be deemed to satisfy the content requirements, making it "safer" for contractors to rely on; contractor or independently developed training will not receive the same deference.

  It is unclear, in practice, how many agencies will offer privacy training, either through agency-developed curricula or by providing the training directly. If agencies choose not to do so (which is a real possibility given the expense and labor attached to such an effort), contractors will have no choice but to step in and develop a compliant training program. Moreover, even if an agency offers the initial, foundational training session, there is no guarantee that it will also offer the advanced-level training or

the subsequent, annual training sessions. Accordingly, as a result of this rule most contractors will need to assess their current privacy infrastructure and determine whether they can comfortably rely upon any existing privacy training their employees might receive in connection with the performance of other government contracts. For contractors with employees who perform applicable work across multiple government contracts, establishing an enterprise-wide privacy training program could greatly ease the burden of compliance.

- **Record-keeping requirements.** Regardless of which entity provides the training (an agency or the contractor), all contractors must maintain records documenting that each applicable employee has completed the mandatory initial training and the follow-up annual training. Contractors will be required to provide these records to the contracting officer upon request.
- **No exemption for subcontractors.** All the requirements identified above for contractors also apply to all subcontractors that handle the type of information and records implicated by the rule. Thus, contractors must flow down training requirements to all such subcontractors, and it will be incumbent upon contractors to take those steps necessary to ensure their subcontractors are compliant with all aspects of the rule.