

Mandatory Privacy Training

Written by Nick Sanders

Friday, 23 December 2016 00:00

A recent [final rule](#) revised the FAR to require contractors whose employees have access to “a system of records” or that “handle personally identifiable information” (PII) to complete training on privacy. The final rule applies to acquisitions of commercial items and to acquisitions valued below the simplified acquisition threshold (SAT). The privacy training must be “role-based [and provide for] foundational as well as more advanced levels of training” and include tests of the knowledge levels of users.

Training must cover—

-

The provisions of the Privacy Act of 1974 ([5 U.S.C. 552](#) a), including penalties for violations of the Act;

-

The appropriate handling and safeguarding of PII;

-

The authorized and official use of a system of records or any other PII;

-

Restrictions on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access, or store PII;

-

The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of PII or systems of records; and

-

Procedures to be followed in the event of a potential or confirmed breach of a system of records or unauthorized disclosure, access, handling, or use of PII.

Mandatory Privacy Training

Written by Nick Sanders

Friday, 23 December 2016 00:00

The requirement is a flow-down, meaning that prime contractors are required to include it in subcontracts, where applicable (i.e., where the subcontractor handles PII).

The contractor (or subcontractor) must maintain documentation evidencing that the privacy training requirements were met, and must provide that documentation upon request.

A new subpart (24.3) is added to the FAR to address the issue.

What is PII? According to the new rule, “*Personally identifiable information* means 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.”

What do we think of the new rule?

Well, we just finished up a lot of compliance training. And in that training we learned that a company—not just a government contractor, but any publicly traded entity—should have a policy on PII protection and that employees should be trained in that policy, and that compliance with the policy should be tested. So from that point of view, this is something that many companies should already have in place. For them, it will be no big deal.

But we also know that there are many upon many small businesses and other contractors for whom this will be a brand new and disconcerting requirement. For them, it will be a big deal indeed.

We also think that the rule is unnecessarily prescriptive and creates a bureaucratic solution to what is essentially a free market problem. For example, the government could have chosen to create a mandatory source evaluation factor that covered the same requirements. That would have pushed companies toward the same end state without actually prescribing it.

Mandatory Privacy Training

Written by Nick Sanders

Friday, 23 December 2016 00:00

But whatever. Here we are.

If you would like assistance in designing your training program or in training your employees, Apogee Consulting, Inc., is here to help you.