

NEW PRIVACY TRAINING REQUIREMENT FOR CONTRACTORS OF THE FEDERAL GOVERNMENT

Effective January 19, 2017, the Department of Defense (DOD), General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) issued a final rule amending the Federal Acquisition Regulation (FAR) to require that contractors, whose employees have access to a system of records or handle personally identifiable information (PII), complete privacy training. This requirement will apply only to those contractors who have a contract with a federal agency, and whose work on behalf of the federal agency involves accessing a system of records or otherwise handling PII.

Under the new guidelines, the contractor must do the following:

1. Identify employees who handle PII; have access to a system of records; or design, develop, maintain or operate a system of records.
2. Provide initial privacy training and annual privacy training thereafter.
3. Maintain records indicating that the employees have completed the requisite training and provide these records to the contracting officer upon request; and
4. Flow-down these requirements to all applicable subcontractors.

I. Background

The Privacy Act of 1974, 5 U.S.C. § 552a, governs the collection, maintenance, use and dissemination of information about individuals by federal government agencies. The Privacy Act prohibits the disclosure of an individual's information without consent, unless the disclosure is pursuant to a statutory exception.¹

There are times when a federal agency may enter into a contract with a private entity to acquire goods or services. In such instances, the FAR

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:



Al Saikali
dd 305.960.6923
asaikali@shb.com



Mayela Montenegro
dd 949.975.1741
mmontenegro@shb.com

¹ U.S. Department of Justice, Privacy Act of 1974, <https://www.justice.gov/opcl/privacy-act-1974>.

PRIVACY AND DATA SECURITY ALERT

MARCH 15, 2017

comes into play. The FAR is a set of rules regulating government acquisition contracts between the federal agency and the private entity. The FAR provides rules on a wide array of topics, including publicizing contract actions, acquisition planning, required sources of supplies and services, contractor qualifications, contract types and other contracting requirements. The FAR also provides rules on the protection of privacy and freedom of information in government contracts (Part 24).² While the DOD, GSA, and NASA are responsible for issuing and revising the rules under the FAR, the FAR applies to all agencies in the executive branch. The FAR is codified at 48 C.F.R. Chapter 1.³

Given the enhanced scrutiny of the federal government's management and handling of private information, in 2011 the DOD, GSA, and NASA proposed to amend the FAR to require government contractors to complete training to safeguard private information. This is in accordance with the Privacy Act to safeguard the maintenance and use of information about individuals. In December 2016, after receiving public comments about the proposed amendments, the agencies issued the final rule. As such, effective January 19, 2017, the new privacy training requirement went into effect.⁴

II. New Privacy Training Requirement

The new privacy training requirements are set forth in FAR subsection 24.3. In sum:

To what type of contractors do the new privacy training requirements apply?

The privacy training requirement applies to contractors and subcontractors for commercial items when they involve access to a system of records.

Which employees must participate in the new privacy training?

The new privacy training applies to employees who:

1. Have access to a system of records;

2 Federal Acquisition Regulation, <https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf>.

3 Small Business Administration, Federal Acquisition Regulations, <https://www.sba.gov/contracting/contracting-officials/federal-acquisition-regulations-far>.

4 Federal Register, Federal Acquisition Training, Privacy Training, <https://www.federalregister.gov/documents/2016/12/20/2016-30213/federal-acquisition-regulation-privacy-training#print>.

PRIVACY AND DATA SECURITY ALERT

MARCH 15, 2017

2. Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle PII; or
3. Design, develop, maintain or operate a system of records.

How are “PII” and “system of records” defined?

Pursuant to FAR subsection 24.101, PII 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. This concerns information about an individual who is a United States citizen or permanent resident.

System of records means a group of records from which information is retrieved by the name of the individual or some identifying number, symbol or other identifier assigned to an individual. These records include information such as birthdate, address, Social Security number, education, financial transactions, medical history, and criminal or employment history, and that contains the individual’s name, or the identifying number, symbol or other identifier assigned to the individual, such as a fingerprint, voiceprint, or photograph.

What must be discussed at the privacy training?

The new privacy training must address the key elements necessary for ensuring the safeguarding of PII or a system of records. At a minimum, the privacy training must cover the following:

1. The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;
2. The appropriate handling and safeguarding of PII;
3. The authorized and official use of a system of records or any other PII;
4. The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access PII;
5. The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling or use of PII; and
6. Procedures to be followed in the event of a suspected or confirmed breach of a system of records or unauthorized disclosure, access, handling or use of PII.

The training must be role-based, provide foundational and advanced levels of training, and have measures in place to test the knowledge level of users.

PRIVACY AND DATA SECURITY ALERT

MARCH 15, 2017

Who provides the training?

The contractor may provide its own training or use the training of another agency, unless the contracting agency specifies that only its agency-provided training is acceptable.

How often does the contractor have to offer training?

The contractor must offer the initial privacy training, and then annually thereafter.

Does the contractor have to document the training after completion?

Yes. The contractor must maintain documentation showing the completion of privacy training for all applicable employees. Upon request, the contractor must show such documentation to the contracting officer of the government agency making the request.

Minimal recordkeeping is required. The contractor can maintain the employee training records for privacy training similar to the way it maintains employees' other training records. There are no required formats or templates for documentation.

What happens if an employee does not participate in the training?

The employee will not be permitted to have or retain access to a system of records or handle PII.

Do these requirements also apply to subcontractors?

Yes. The prime contractor is required to flow-down these requirements to all subcontractors involved with the handling and safeguarding of PII.

Will there be a new clause in government contracts?

Yes. FAR [52.224-3](#) is a clause that will be inserted in solicitations and contracts when, on behalf of an agency, employees will engage in functions that fall within the new privacy training requirements. The language of 52.224-3 mirrors the language set forth above in subsection 24.3.

Why did the government impose these new regulations?

There has been greater scrutiny regarding the government's information collection practices and information security management, given the increased portability of data and instances of loss or potential disclosure of protected information.

PRIVACY AND DATA SECURITY ALERT

MARCH 15, 2017

III. Ideas for Training

As long as the contractor meets the minimum requirements set forth by the new regulation, the contractor has wide latitude in how to conduct the training. Some ideas include:

- After identifying all applicable employees, gather all employees in a meeting room to conduct the training. Alternatively, create online-based training so employees can participate at a time most convenient for them.
- Discuss required topics of discussion using factual scenarios, such as through video vignettes.
- At the end of the training, have employees complete a short quiz about the content they have just learned. The contractor should save these quizzes in the employees' files as evidence of the training.

SOURCES

Federal Acquisition Regulation subpart 24.3:

<https://www.acquisition.gov/?q=/browse/far/24>

Federal Acquisition Regulation 52.224-3:

https://www.acquisition.gov/far/html/52_223_226.html

Federal Register re: Federal Acquisition Training; Privacy Training:

<https://www.federalregister.gov/documents/2016/12/20/2016-30213/federal-acquisition-regulation-privacy-training#print>

DISCLAIMER

This information is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

The choice of a lawyer is an important decision and should not be solely upon advertisements.

For more information about data security law, please visit Al Saikali's [blog](#).