

April 2017

Follow @Paul_Hastings



New Privacy Training Requirements for Covered Federal Contractor Employees

By [Federal Contractor and Privacy & Cybersecurity Practice Groups](#)

A recent rule amending the Federal Acquisition Regulations (“FAR”), effective January 19, 2017, requires federal contractors to provide initial and annual privacy training for three types of employees, namely those who, *on behalf of a federal agency*: (1) have access to a system of records (“SOR”); (2) design, develop, maintain or operate such a SOR; or (3) create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle (collectively “Process”) personally identifiable information (“PII”).¹

Notably, the rule *does not apply* to employees whose access is limited to the contractor’s *own* human resources information or personal information of other third parties. However, for the covered employees, the rule imposes important new training requirements.

I. Covered Contracts

Whether contracting officers are required to insert the privacy training contract clause (FAR 52.224-3) in solicitations and contracts will turn on whether contractor employees will Process PII or work on a SOR on behalf of the agency.

- *Personally Identifiable Information*: Under the FAR, PII is 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.²
- *System of Records*: The FAR defines a SAR as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to the individual.³

Notably, because the regulation is promulgated pursuant to the Privacy Act of 1974, which predates statutory exemptions applicable to laws enacted after October 13, 1994, it contains no exceptions for small contracts or contracts for commercial items. Thus, the new regulation applies to contracts and subcontracts that fall below the simplified acquisition threshold (“SAT”) and those for commercially available off-the-shelf (“COTS”) items.

Any contractor whose employees Process PII, or access, design, develop, maintain or operate a SOR on behalf of a federal agency, should carefully review any training requirement provisions added by contracting officers to new solicitations as well as any such provisions added through modification to



existing contracts. However, contractors most likely to be covered by the privacy training requirements include financial institutions, insurance companies, law firms, and accounting firms as they are more likely to Process PII of a federal agency. Covered contractors must flow down the privacy training requirement in contracts with any subcontractors who Process PII or work on an SOR on a federal agency's behalf.

II. Training Requirements

Covered employees must be trained prior to handling PII, and annually thereafter. Unless the agency requires that a contractor's covered employees receive such training from the agency directly, contractors may provide their own training.

The training must address the key elements for safeguarding PII and SORs. It must be "role based, provide foundational as well as more advanced levels of training" and include some form of testing.⁴

At a minimum, the privacy training must cover the following topics:

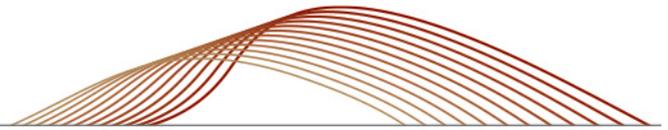
- Provisions of the **Privacy Act of 1974**, including penalties for violations of the Act;
- Appropriate **handling and safeguarding of PII**;
- **Authorized and official use** of a SOR or any other PII;
- **Restriction on the use of unauthorized equipment** to Process PII;
- **Prohibition against the unauthorized use** of a SOR or **unauthorized Processing** of PII; and
- **Procedures** to be followed in the event of a **suspected or confirmed breach** of a SOR or unauthorized Processing of PII.

Contractors must document the privacy training conducted and be prepared to provide such documentation to the relevant government agency upon request.

Additionally, contractors who opt to conduct their own training should consult legal counsel to ensure that the training satisfies the requirements of the new rule.

If you are interested, Paul Hastings' Privacy and Cybersecurity Practice Group is developing training that will comply with the new FAR.

◇ ◇ ◇



If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Federal Contractor Practice Group

Chicago

Jon A. Geier*
1.312.499.6054
jongeier@paulhastings.com

Alex J. Maturi*
1.312.499.6076
alexmaturi@paulhastings.com

Los Angeles

Nancy L. Abell
1.213.683.6162
nancyabell@paulhastings.com

Maria A. Audero
1.213.683.6307
mariaaudero@paulhastings.com

San Francisco

Zina Deldar
1.415.856.7207
zinadeldar@paulhastings.com

New York

Kenneth Gage
1.212.318.6046
kennethgage@paulhastings.com

Orange County

Blake R. Bertagna
1.714.668.6208
blakebertagna@paulhastings.com

Washington, D.C.

Barbara B. Brown
1.202.551.1717
barbarabrown@paulhastings.com

Tammy R. Daub
1.202.551.1894
tammydaub@paulhastings.com

Charles A. Patrizia*
1.202.551.1710
charlespatrizia@paulhastings.com

Privacy and Cybersecurity Practice Group

London

Ashley Winton
+44 02030235121
ashleywinton@paulhastings.com

New York

James H. Koenig
1.212.318.6005
jimkoenig@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Paul Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Washington, D.C.

Behnam Dayanim*
1.202.551.1737
bdyanim@paulhastings.com

Sherrese M. Smith*
1.202.551.1965
sherresesmith@paulhastings.com

Mary-Elizabeth M. Hadley*
1.202.551.1750
maryelizabethhadley@paulhastings.com

*Primary Authors

¹ 48 C.F.R. § 24.301(a).

² 48 C.F.R. § 52.224-3(a).

³ 48 C.F.R. § 24.101.

⁴ 48 C.F.R. § 24.301(b).

Paul Hastings LLP

PH Perspectives is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2017 Paul Hastings LLP.