



Homeland  
Security

MEMORANDUM FOR Heads of Contracting Activities  
Component Acquisition Executives

FROM: Paul Courtney  
Chief Procurement Officer

PAUL R  
COURTNEY

Digitally signed by PAUL R  
COURTNEY  
Date: 2023.07.20 15:42:27 -04'00'

SUBJECT: Homeland Security Acquisition Regulation (HSAR) Class Deviation 15-01, Revision 1: Safeguarding of Controlled Unclassified Information

## 1. Introduction:

Effective July 21, 2023, this Revision 1 changes the title of HSAR Class Deviation 15-01 from “Safeguarding of Sensitive Information” to “Safeguarding of Controlled Unclassified Information” and updates HSAR Class Deviation 15-01 for implementation of the Final Rule on HSAR Case 2015-001 Safeguarding of Controlled Unclassified Information. Contracting officers shall immediately:

- Discontinue use of special clause Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015); and
- Insert FAR 52.224-3 Privacy Training – Alternate I (DEVIATION) in applicable solicitations and contracts (see FAR Class Deviation 17-03, Revision 1); and
- Insert special clause Information Technology Security Awareness Training (July 2023), which is a revision to special clause Information Technology Security and Privacy Training (MAR 2015), in applicable solicitations and contracts.

## 2. Background:

The Final Rule on HSAR Case 2015-001 Safeguarding of Controlled Unclassified Information, effective July 21, 2023, was published on June 21, 2023 to:

- Revise HSAR 3001.106 to add OMB Control No. 1601–0023 (Safeguarding of Controlled Unclassified Information);
- Amend HSAR 3002.101 to add definitions for “Adequate security”, “Controlled unclassified information (CUI)”, “Federal information”, “Federal information system”, “Handling”, “Information resources”, “Information security”, and “Information systems”;
- Modify HSAR subpart 3004.4, Safeguarding Classified and Controlled Unclassified Information within Industry;
- Remove the clause at HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources, and reserve the clause number;
- Update the clauses at HSAR 3052.204-71, Contractor Employee Access, and 3052.212- 70, Contract terms and conditions applicable to DHS acquisition of commercial items; and

- Add two new contract clauses, HSAR 3052.204-72, Safeguarding of Controlled Unclassified Information, and HSAR 3052.204-73, Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents.

**3. Applicability of DHS Special Clause Safeguarding of Sensitive Information (MAR 2015):**

- Contracting officers shall:
  - a) Effective July 21, 2023, **discontinue** use of special clause Safeguarding of Sensitive Information (MAR 2015);
  - b) Amend existing solicitations to remove special clause Safeguarding of Sensitive Information (MAR 2015) and add HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information and its Alternate I, as applicable; and
  - c) Modify existing contracts (as defined in FAR 2.101) with a remaining period of performance of twelve months or more to remove special clause Safeguarding of Sensitive Information (MAR 2015) and add HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information and its Alternate I, as applicable.

**4. Applicability of DHS Special Clause Information Technology Security and Privacy Training (MAR 2015):**

- Contracting officers shall:
  - a) Effective July 21, 2023, **discontinue** use of special clause Information Technology Security and Privacy Training (MAR 2015);
  - b) Amend existing solicitations to remove special clause Information Technology Security and Privacy Training (MAR 2015) and add special clause Information Technology Security Awareness Training (JULY 2023) **and** FAR 52.224-3 Privacy Training – Alternate I (DEVIATION), as applicable; and
  - c) Modify existing contracts (as defined in FAR 2.101) with a remaining period of performance of twelve months or more to remove special clause Information Technology Security and Privacy Training (MAR 2015) and add special clause Information Technology Security Awareness Training (JULY 2023) **and** FAR 52.224-3 Privacy Training – Alternate I (DEVIATION), as applicable.

**5. Applicability of DHS Special Clause Information Technology Security Awareness Training (JULY 2023) (see Attachment 1):**

- Contracting officers shall incorporate this special clause into solicitations and contracts issued on or after July 21, 2023, when:
  - a) a contractor will have access to CUI, as defined in HSAR 3002.101; or

- b) Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI.
- Contracting officers shall incorporate the special clause as follows:
  - a) For existing solicitations, contracting officers shall amend the solicitation to include this special clause and ensure the special clause is included in the resultant contract.
  - b) For new solicitations, contracting officers shall include this special clause in the solicitation and resultant contract.

## **6. Expiration Date:**

This class deviation is applicable until the HSAR is changed by publication in the Code of Federal Regulations.

## **7. Additional Information:**

- DHS Component contracting activities should update their contract writing systems to remove special clauses Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) and include the clause in Attachment 1.
- Questions regarding this class deviation should be directed to Shaundra Ford at [Shaundra.Ford@hq.dhs.gov](mailto:Shaundra.Ford@hq.dhs.gov).

## **8. Attachments:**

- Attachment 1: Special Clause Information Technology Security Awareness Training (July 2023)

**INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)**

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31<sup>st</sup> of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer’s Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31<sup>st</sup> of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(End of clause)