

**SUPPORTING STATEMENT
HOMELAND SECURITY ACQUISITION REGULATION (HSAR)
OMB CONTROL NO. 1601-NEW
INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING
AND
PRIVACY TRAINING**

A. JUSTIFICATION

1. Need for the Information Collection

This is a request for the establishment of a new information collection to implement the DHS requirement that all contractor and subcontractor employees that require access to:

- a) DHS information systems and information resources or contractor-owned and/or operated information systems or information resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information take information technology (IT) security awareness training and sign the DHS Rules of Behavior (RoB) before access to DHS information systems and information resources is granted; and
- b) a Government system of records; handle Personally Identifiable Information (PII) or Sensitive PII (SPII); or design, develop, maintain, or operate a system of records on behalf of the Government to complete privacy training initially upon award of the procurement and at least annually thereafter.

This information collection is necessary to ensure compliance with the IT security awareness training, DHS RoB, and privacy training requirements across DHS contracts. Authorities applicable to this requirement include:

- Federal Information Security Modernization Act (FISMA) of 2014;
- Title III of the E-Government Act of 2002;
- Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296;
- National Institute of Standards and Technology (NIST), Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Office of Management and Budget (OMB) Memorandum M-10-23, *Guidance for Agency Use of Third-Party Web sites and Applications*, (June 25, 2010);
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, (May 22, 2007);
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006);
- OMB Circular No. A-130 (Revised), *Management of Federal Information Resource*, (November 28, 2000); and
- DHS Sensitive Systems Policy Directive 4300A.

2. Use of the Information

DHS is proposing amendments to the Homeland Security Acquisition Regulation (HSAR) to require contractor and subcontractor employees to take Information Technology Security Awareness Training, sign the DHS Rules of Behavior, and take Privacy Training when required. Specifically, these amendments would make the following changes to the HSAR:

- Add a new HSAR subpart 3039.70, Information Technology Security Awareness Training, and associated clause at HSAR 3052.239-7X, Information Technology Security Awareness Training, to require contractor and subcontractor employees that may have access to DHS information systems and/or information resources or contractor-owned and/or operated information systems or information resources capable of processing, storing or transmitting sensitive information to:
 - i. Complete Information Technology Security Awareness Training within thirty (30) days of contract award and on an annual basis thereafter not later than October 31st of each year.
 - ii. Maintain evidence that the training has been completed and provide copies of the training completion certificates to the Contracting Officer and/or Contracting Officer's Representative (COR).
 - iii. Sign the DHS Rules of Behavior (RoB) before access to a DHS information system or information resource is granted or a contractor-owned and/or operated information system/information resource that will be used to process, store or transmit sensitive information is granted.
 - iv. Maintain signed copies of the DHS RoB for all contractor and subcontractor employees as a record of compliance and provide signed copies of the DHS RoB to the Contracting Officer and/or COR.

- Add a new HSAR subpart 3024.70, Privacy Training, and associated clause at HSAR 3052.224-XX, Privacy Training, to require contractor and subcontractor employees that require access to a Government system of records; handle Personally Identifiable Information (PII) or Sensitive PII (SPII); or design, develop, maintain, or operate a Government system of records to:
 - i. Complete Privacy Training within thirty (30) days of contract award and on an annual basis thereafter not later than October 31st of each year.
 - ii. Maintain evidence that the training has been completed and provide copies of the training completion certificates to the Contracting Officer and/or COR.

3. Use of Information Technology.

Collection of the required information is a contractual condition of the clauses at HSAR3052.224-7X Privacy Training and 3052.239-7X, Information Technology Security Awareness Training. The information collection requirements imposed on contractors are contained in each solicitation and provide the specified contracting officer's name, email, mailing address and other salient characteristics that contractors would use to submit its response. Where both the Department and contractors are

capable of electronic interchange, contractors may submit the information collection requirements electronically (i.e. email), unless the solicitation specifically prohibits it. This approach is consistent with section 2.101 of the Federal Acquisition Regulation which permits the use of electronic submissions. Because the information collection requirements imposed on contractors must meet specific timeframes, a centralized mailbox or website would not be an expeditious or practical method of submission.

4. Efforts to Identify Duplication

As a matter of policy, DHS reviews the Federal Acquisition Regulation (FAR) and HSAR to determine if adequate language already exists. This information collection implements a unique provision and does not duplicate any other requirement. If the FAR is revised to incorporate language that is comparable to parts of these rules, the duplicative text will be removed from the HSAR.

5. Impact on Small Business or Other Small Entities

The burden applied to small businesses is the minimum consistent with applicable laws, Executive Orders, regulations, and prudent business practices.

6. Consequences of Collection the Information Less Frequently

Collection of this information on a less frequent basis is not practical. The consequence of not collecting this data is that DHS is not ensuring that contractor and subcontractor employees are adequately trained on (a) their responsibilities when accessing information systems that process, store, or transmit sensitive information and (b) how to properly handle PII and SPII.

7. Special Circumstances Relating to the Guidelines of 5 CFR 1320.5

The collection of this information is consistent with the general information collection guidelines in 5 CFR 1320.5 (d) (2).

8. Efforts to Consult Outside the Agency

Public comment will be solicited in the Federal Register as required by 5 CFR 1320.8(d). This supporting statement will be modified to address any public comments received.

9. Explanation of Payments and Gifts to Respondents

No payment or gift will be provided to respondents other than remuneration of contractors under their contracts.

10. Assurance of Confidentiality Provided to Respondents

This information is disclosed only to the extent consistent with statutory requirements, current regulations, and prudent business practices. All information collection activities will conform to the requirements for the protection of the confidentiality of nonpublic information and personally identifiable information and for data security and integrity.

11. Additional justification for questions of a sensitive nature.

No sensitive questions are involved.

12. Estimated total annual public hour and cost burden.

Annual reporting and recordkeeping burden estimates are based on Fiscal Year (FY) 2014 data reported to the Federal Procurement Data System (FPDS) on contract actions for products and services (including IT services). It is anticipated that this information collection will be primarily applicable to actions with a Product and Service Code (PSC) of “D” Automatic Data Processing and Telecommunication and “R” Professional, Administrative and Management Support. For FY 2014, DHS made more awards to small businesses for PSCs “D” and “R” than large businesses. The PSCs will be adjusted as additional data becomes available through HSAR clause implementation to validate future burden projections.

A. HSAR subpart 3039.70, Information Technology Security Awareness Training:

Based on a review and analysis of FPDS data and internal DHS contract data, it is estimated that this clause would apply to approximately 874 unique vendors, including 485 small businesses and 389 large businesses. However, this proposed revision to the HSAR includes a flow-down provision that applies to subcontractors. It is estimated that the number of subcontractors required to complete IT security awareness training is 1.5 times the number of contractors or 1,311, including 727 small and 584 large businesses. Therefore, the estimated number of respondents is 2,185 of which 1,212 are projected to be small businesses. The total annual projected number of responses per respondent is projected to be four (4). The burden hours estimated per response is 30 minutes. The annual total burden hours are estimated as follows:

Annual Reporting Burden and Cost

Estimated respondents/yr.....	2,185
Responses annually.....	<u>x 4</u>
Total annual responses.....	8,740
Estimated hrs/response.....	<u>x .50</u>
Estimated total burden/hrs.....	4,370.00
Average wages + overhead.....	<u>x</u>
<u>\$40.00*</u>	
Estimated cost to the public.....	
.....	
\$174,800.00	

The estimated number of record-keepers per year is 2,185. It is further estimated that each contractor will provide approximately four (4) responses annually. The burden hours estimated per response is 10 minutes.

Annual Recordkeeping Burden

Number of recordkeepers.....	2,185
Number of responses	<u>x 4</u>
Total Annual Responses.....	8,740

Number of hours per recordkeeper.....	<u>x .17</u>
Total response and recordkeeping burden hours.....	1,485.80
Average wages + overhead.....	<u>x \$40*</u>
Estimated cost to the public.....	
.....	
\$59,432.00	

B. HSAR subpart 3024.70, Privacy Training:

Based on a review and analysis of FPDS data, it is estimated that this clause would apply to approximately 2,651 unique vendors, including 1,665 small businesses and 986 large businesses. However, this proposed revision to the HSAR includes a flow-down provision that applies to subcontractors. It is estimated that the number of subcontractors required to complete privacy training is 1.5 times the number of contractors or 3,977, including 2,497 small and 1,480 large businesses. Therefore, the estimated number of respondents is approximately 6,628 of which 4,162 are projected to be small businesses. The total annual projected number of responses per respondent is projected to be four (4). The burden hours estimated per response is 30 minutes. The annual total burden hours are estimated as follows:

Annual Reporting Burden and Cost

Estimated respondents/yr.....	6,628
Responses annually.....	<u>x 4</u>
Total annual responses.....	26,512
Estimated hrs/response.....	<u>x .50</u>
Estimated total burden/hrs.....	13,256
Average wages + overhead.....	<u>x</u>
<u>\$40.00*¹</u>	
Estimated cost to the public.....	
.....	
\$530,240.00	

Annual Recording Keeping Burden

The estimated number of record-keepers per year is 6,628 based off of FY 2014 data from FPDS and internal DHS contract data. It is further estimated that each contractor will provide approximately four (4) responses annually. The burden hours estimated per response is 10 minutes.

Annual Recordkeeping Burden

Number of recordkeepers.....	6628
------------------------------	------

¹Note: Based on the OPM salary table for calendar year 2015, we estimated an hourly rate equivalent to a GS-11, Step-2, or \$29.00 per hour, plus 36.25 percent overhead burden, and rounded to the nearest whole dollar, or \$40.00

Number of responses	<u>x 4</u>
Total Annual Responses.....	26,512
Number of hours per recordkeeper.....	<u>x .17</u>
Total response and recordkeeping burden hours.....	4,507.04
Average wages + overhead.....	<u>x \$40*</u>
Estimated cost to the public.....	
.....	
\$180,281.60	

Total Annual Reporting and Recordkeeping Burden and Cost for HSAR 3024.70, Privacy Training and HSAR 3039.70, Information Technology Security Awareness Training

It is estimated that there are 8,813 respondents applicable to this information collection (2,185 for Information Technology Security Awareness Training and 6,628 for Privacy Training).

Estimated respondents/yr.....	8813
Responses annually.....	<u>x 4</u>
Total annual responses.....	35,252
Estimated hrs/response.....	<u>x .50</u>
Estimated total burden/hrs.....	17,626
Average wages + overhead.....	<u>x</u>
<u>\$40.00*</u>	
Estimated cost to the public.....	
.....	
\$705,040.00	

Number of recordkeepers.....	8,813
Number of responses	<u>x 4</u>
Total Annual Responses.....	35,252
Number of hours per recordkeeper.....	<u>x .17</u>
Total response and recordkeeping burden hours.....	5,992.84
Average wages + overhead.....	<u>x \$40*</u>
Estimated cost to the public.....	
.....	
\$239,713.60	

*Note: Based on the OPM salary table for calendar year 2015, we estimated an hourly rate equivalent to a GS-11, Step-2, or \$29.00 per hour, plus 36.25 percent overhead burden, and rounded to the nearest whole dollar, or \$40.00

13. Total capital and start-up cost.

There are no capital/start-up or ongoing operation/maintenance costs associated with this information collection.

14. Estimated cost to the Government.

The Government’s burden associated with this information collection would be limited to the receipt, review, and analysis of IT security awareness training completion certificates, signed copies of the DHS RoB, and privacy training completion certificates from contractors. Time required for review is estimated at 10 minutes per response.

A. HSAR subpart 3039.70, Information Technology Security Awareness Training:

Total Annual responses.....	2,185	
Review time per response.....		<u>x .17</u>
Estimated total burden/hrs.....		371.45
Average wages + overhead.....		<u>x</u>
<u>\$40.00*</u>		
Total Government Cost.....		
.....		
\$14,858.00		

B. HSAR subpart 3204.70, Privacy Training:

Total Annual responses.....	6,628	
Review time per response.....		<u>x .17</u>
Estimated total burden/hrs.....		1126.76
Average wages + overhead.....		<u>x</u>
<u>\$40.00*</u>		
Total Government Cost.....		
.....		
\$45,070.40		

*Note: Based on the OPM salary table for calendar year 2015, we estimated an hourly rate equivalent to a GS-11, Step-2, or \$29.00 per hour, plus 36.25 percent overhead burden, and rounded to the nearest whole dollar, or \$40.00

15. Explanation of Program Changes or Adjustments

This is a new information collection requirement.

16. Outline plans for published results of information collections.

Results will not be tabulated or published.

17. Approval not to display expiration date.

DHS does not seek approval to not display the expiration dates for OMB approval of the information collection.

18. Explanation of exception to certification statement.

Not applicable.

B. Collections of Information Employing Statistical Methods.
Statistical methods are not used in this information collection.