SUPPORTING STATEMENT
HOMELAND SECURITY ACQUISITION REGULATION (HSAR)
OMB CONTROL NO. 1601-NEW
SAFEGUARDING OF SENSITIVE INFORMATION

A. JUSTIFICATION

1. Need for the Information Collection

This request is for the establishment of a new information collection to implement the Department of Homeland Security (DHS) requirements for safeguarding sensitive information. Part of the mission of the DHS is to protect the nation's cybersecurity and to coordinate responses to cyber-attacks and security vulnerabilities. In keeping with this mission, DHS is proposing to amend the HSAR to implement requirements that contractors and subcontractors must meet to protect sensitive information. This information collection is necessary to ensure adequate security measures are in place to safeguard sensitive information and to improve incident reporting to DHS.

The requirement to ensure the security of sensitive information has been a HSAR requirement for a number of years. This rule expands on the existing IT security requirements in HSAR 3052.204-70, Security Requirements for Unclassified Information Technology resources, which this rule proposes to remove. This requirement will be prescribed in HSAR 3004.470-4(b) and the associated clause will be incorporated at HSAR 3052.204-7X, Safeguarding of Sensitive Information. The Safeguarding of Sensitive Information clause includes the following:

i. HSAR 3052.204-7X, Paragraph (b) *Handling of Sensitive Information.* Require contractors and subcontractors to provide adequate security to protect sensitive information from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award.

ii. HSAR 3052.204-7X, Paragraph (d) *Incident Reporting Requirements.* Require a contractor to report all known or suspected incidents to the Component Security Operations Center (SOC), or the DHS Enterprise SOC if the Component SOC is not available, within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Attachment F Incident Response*. All others shall be reported within eight hours of discovery. Any remaining data elements not provided in the timeframes listed above shall be provided within 24 hours of submission of the initial incident.

iii. HSAR 3052.204-7X, Paragraph (e) *Incident Response Requirements.* Require a contractor to provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

iv. HSAR 3052.204-7X, Paragraph (f) *PII and SPII Notification Requirements.* Require a contractor to have in place procedures and the capability to notify any individual whose PII and/or SPII was under the control of the contractor or resided in the contractor information system at the time of the incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer.

v. HSAR 3052.204-7X, Paragraph (g) *Credit Monitoring Requirements.* Require a contractor to provide credit monitoring services in the event that an incident involves PII and/or SPII. Credit monitoring services are to be provided to an individual whose PII and/or SPII was under the control of the contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the contractor has no affiliation.

vi. HSAR 3052.204-7X, Paragraph (h) *Certification of Sanitization of Government and Government-Activity-Related Files and Information*. Require a contractor to certify and confirm the sanitization of Government and Government-Activity related files and information, and submit the certification to the Contracting Officer's Representative (COR) and Contracting Officer in accordance with the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization, Appendix G*.

vii. HSAR 3052.204-7X, Paragraph (i) *Other Reporting Requirements*. Clarifies that the incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s).

viii. HSAR 3052.204-7X, Paragraph (j) *Subcontracts*. Clarifies that contractors shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower-tier subcontracts.

In addition to the above, the following requirements must be met when information systems are used to process, store or transmit sensitive information:

i. HSAR 3052.204-7X, Paragraph (c) *Authority to Operate*. The Contractor shall not process, store or transmit sensitive information within an information system until an Authority to Operate (ATO) has been accepted and signed by the Component or Headquarters CIO, or designee. Once the ATO has been accepted and signed by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Security Authorization (SA) documentation includes the following: Security Plan (SP), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), Security Control Assessor Transmittal Letter (documents the Security Control Assessor's recommendation (i.e., Authorization to Operate or Denial to Operate), and any supplemental information

requested by the Government (e.g., Contingency Plan, final Risk Assessment, Configuration Management Plan, Standard Operating Procedures, Concept of Operations).

ii. HSAR 3052.204-7X, Paragraph (c)(1)(i) *Security Authorization Documentation*. Requires a contractor to complete and submit the SA documentation. The Security Authorization (SA) process shall proceed according to *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 11.0, January 14, 2015), or any successor publication, and the *Security Authorization Process Guide*.

iii. HSAR 3052.204-7X, Paragraph (c)(1)(ii) *Independent Assessment.* Require the contractor to have an independent third party validate the security and privacy controls in place for the information system. The contractor must demonstrate that deficiencies are addressed before submitting the SA package to the COR for acceptance.

iv. HSAR 3052.204-7X, Paragraph (c)(2) *Renewal of ATO*. Requires the contractor to renew the ATO every three (3) years unless otherwise specified in the ATO letter. The contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls.

v. HSAR 3052.204-7X, Paragraph (c)(3) *Security Review.* Clarifies that the Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced.

vi. HSAR 3052.204-7X, Paragraph (c)(4) *Federal Reporting and Continuous Monitoring Requirements.* Requires contractors operating information systems on behalf of the Government or operating information systems containing the Government's sensitive information to comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication. The contractor is required to provide the Government with all information to fully satisfy Federal reporting requirements for information systems within three (3) business days of receipt of the request.

The following statutes, Executive Order, Governmentwide policy, DHS policy identify the safeguarding of sensitive information as a national-level priority and support this collection of information:

- Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. 3551, *et seq*.);

- Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296
- Executive Order 13556, Controlled Unclassified Information (CUI);
- Office of Management and Budget (OMB) Circular A-130 Management of Federal Information Resources;
- Relevant National Institutes of Standards and Technology (NIST) guidance;
- OMB Memorandum M-14-03 Enhancing the Security of Federal Information and Information Systems (November 18, 2013);
- 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); and
- DHS Sensitive Systems Policy Directive 4300A (or successor).

2. Use of the Information

DHS is proposing amendments to the HSAR to implement adequate security measures to safeguard sensitive information and to facilitate improved incident reporting to DHS. These amendments would make the following changes to the HSAR:

- Revises HSAR Subpart 3002.101, Definitions: This section is revised to add or redefine the following terms: Adequate Security, Handling, Information Resources, Information Security, Information System, and Sensitive Information.

- Revises HSAR Subpart 3004.470, Security requirements for access to unclassified facilities, information resources, and sensitive information. This section is revised to change the title of the subpart and to clarify the applicability of the subpart to the acquisition lifecycle. The revision/addition of scope, definitions, policy and contract clauses sections are additional changes resulting from this rule.

- Removes HSAR Clause 3052.204-70, Security Requirements for Unclassified Information Technology Resources, and reserves the section number.

- Add a new clause at HSAR 3052.204-7X, Safeguarding of Sensitive Information, to protect sensitive information. The new clause also identifies incident reporting and response requirements, notification and credit monitoring requirements for PII and SPII, and requires that contractors certify and confirm the sanitization of Government and Government-Activity related files and information.

- Revises HSAR 3052.212-70, Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items. This rule proposes to remove HSAR 3052.204-70 Security Requirements for Unclassified Information Technology Resources; identify Alternate II as an option under HSAR 3052.204-71 Contractor Employee Access; and add HSAR 3052.204-7X Safeguarding of Sensitive Information.

3. **Use of Information Technology.**
Collection of the required information is a contractual condition of the clause at HSAR 3052.204-7X, Safeguarding of Sensitive Information. 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. However, contractors may submit renewal documentation via DHS' web-based security management tool (Information Assurance Compliance System).

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 some parts of this rule, 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 the adequate security of sensitive information. Further, having an HSAR clause to address the safeguarding of sensitive information will greatly reduce the proliferation of Department, Component, or buying office-level requirements that offerors now respond to in a variety of different and non-standard ways. Failure to collect this information may result in the compromise of sensitive information hampering the Department's ability to carry out its mission.

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**
This information collection is consistent with the guidelines in 5 CFR 1320.5(d). A revised supporting statement will be provided to OMB to address any comments received on the information collection portion of the proposed HSAR rule.

9. **Explanation of Payments and Gifts to Respondents**
No payment or gift will be provided to respondents other than remuneration of contractors under their contacts.

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.**
A detailed discussion of when respondents must provide a response and for what purpose is listed below. The estimated cost to the public for this information collection is addressed by this supporting statement. The estimated costs include time and effort to—

- Review and understand the requirements;
- Search data sources;
- Review and approve the release of the information;
- Disclose the information to the Government or prospective contractor or contractor; and
- Recordkeeping and retention of the disclosed information as substantiating documentation of determinations and actions.

The below estimates assume that not all efforts, e.g., retrieving and retaining records, are attributed solely to this information collection; only those actions resulting from this rule that are not customary to normal business practices are attributed to this estimate. Therefore, the estimated hours considers the time needed for an average disclosure, recognizing that the hours required may vary based on the contractors overall operational security readiness.

Annual reporting and recordkeeping burden estimates are based on Fiscal Year (FY) 2014 data reported to the Federal Procurement Data System (FPDS) on procurements actions for products and services (including IT services) and internal DHS contract award data. 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. PSCs will be adjusted as additional data becomes available through HSAR clause implementation to validate future burden projections.

A number of factors determine what data would be considered applicable to this proposed clause and would require analysis on a case-by-case basis. For FY 2014, DHS awarded nearly 13,000 new contract awards to large and small businesses, with over 35 percent of all contracts awarded to small businesses. The estimate of the number of small entities to which the proposed rule will apply was established by reviewing FPDS data for FY 2014, internal DHS contract data, experience with similar safeguarding requirements used in certain DHS contracts, and the most likely applicable Product and Service Codes. The data review identified 492 existing contracts to 330 unique vendors, awarded over a four-year period including small and large businesses. Based on the data reviewed, the projected number of annual respondents subject to Safeguarding of Sensitive Information clause is estimated at 123 respondents. Based on the DHS historical data of awarding at least 30 percent of new contact awards to small business, it is assumed that 30 percent of the projected annual number of respondents will be small businesses, or approximately 37 respondents.

The projections are as follows:

HSAR subpart 3052.204-7X, Safeguarding of Sensitive Information:

i. No ATO Required.

Prior to these proposed safeguarding requirements, DHS had a limited number of incidents affecting sensitive information. It is expected that the implementation of these safeguarding requirements will further reduce risks and potential vulnerabilities. Contractors that are not required to meet the ATO requirements because information systems will not be used to process, store or transmit sensitive information are still required to provide adequate security measures to protect sensitive information from unauthorized access and disclosure. It is estimated that approximately 2 respondents annually will report a known or suspected incident. If the incident involves Personally Identifiable Information (PII) or sensitive PII, the contractor will be subject not only to the incident reporting requirements but also the notification and credit monitoring requirements. Known or suspected incidents involving PII or SPII shall be reported within one (1) hour of discovery. All other incidents must be reported within eight (8) hours of discovery. Requirements include:

- Incident Reporting
- Notification (if incident involves PII/SPII)
- Credit Monitoring (if incident involves PII/SPII)
- Certification of Sanitization

3052.204-7X, Safeguarding of Sensitive Information – No ATO Required							
Reporting Requirement	**Estimated Respondents**	**Responses Annually**	**Total Annual Responses**	**Estimated Hours per Response**	**Total Estimated Burden Hours**	**Average wages + overhead**	**Estimated cost to the public**

See bullets in section (i)	2	1	2	8	16	$60.00	$960.00

ii. ATO Required.

Although the proposed HSAR clause is new, a majority of DHS IT services contractors are familiar with the current requirements to comply with Departmental IT security policy and guidance. It is assumed that the average DHS contractor applicable to this clause will have a high operational security readiness posture. However, the requirements of the proposed clause have been expanded to include professional services contractors that have access to sensitive information and use information systems to process, store or transmit sensitive information to perform the requirements of their contract(s). Therefore, the documentation and any follow-up corrective action or additional documentation are estimated to require an average of 72 total hours of effort.

It estimated that approximately 121 respondents will be required to respond to ATO requirements, and therefore are required to submit the SA documentation. The SA documentation includes the following: Security Plan (SP), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), Security Control Assessor Transmittal Letter (documents the Security Control Assessor's recommendation (i.e., Authorization to Operate or Denial to Operate), and any supplemental information requested by the Government (e.g., Contingency Plan, final Risk Assessment, Configuration Management Plan, Standard Operating Procedures, Concept of Operations). Additional requirements include:

- Incident Reporting
- Notification (if incident involves PII/SPII)
- Credit Monitoring (if incident involves PII/SPII)
- Certification of Sanitization
- Independent Assessment
- Renewal of ATO
- Federal Reporting & Continuous Monitoring

3052.204-7X, Safeguarding of Sensitive Information – ATO Required							
Reporting Requirement	**Estimated Respondents**	**Responses Annually**	**Total Annual Responses**	**Estimated Hours per Response**	**Total Estimated Burden Hours**	**Average wages + overhead**	**Estimated cost to the public**
See bullets in section (ii)	121	1	121	72	8,712	$60.00*	$522,,720

Total Annual Reporting Burden and Cost:

3052.204-7X, Safeguarding of Sensitive Information

Reporting Requirement	Estimated Respondents	Responses Annually	Total Annual Responses	Estimated Hours per Response	Total Estimated Burden Hours	Average wages + overhead	Estimated cost to the public
Estimated Totals	123	1	123	80	9,840	$60.00*	$590,400

Total Annual Record-keeping Burden and Cost:

3052.204-7X, Safeguarding of Sensitive Information: It is estimated that the number of record-keepers associated with this clause will be 123. Further, it is estimated that the number of records per record-keeper will be four (4) per unique vendor. Preparation time and maintenance per response is estimated to average sixteen (16) hours.

3052.204-7X, Safeguarding of Sensitive Information						
Estimated Record-keepers	Estimated Records per Record-keeper	Total Annual Records	Estimated Hours per Record	Total Record-keeping Burden Hours	Average wages + overhead	Estimated cost to the public
123	4	492	16	7,872	$60.00*	$472,320

* Means estimated hourly wage according to the OPM salary table for calendar year 2015, GS-13, Step-4 (or equivalent), or $43.99 per hour, plus 36.25 percent (15.95) overhead burden, and rounded to the nearest whole dollar, or $60.00.

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 the clause at 3052.204-7X is minimal if an ATO is not required. Government burden would be limited to receipt, review, and action taken from Incident Reporting, Incident Response activities, PII and SPII Notification requirements, Credit Monitoring, and receipt of Certification of Sanitization of Government and Government-Activity-Related Files and Information. Time required for review is averaged as follows:

3052.204-7X, Safeguarding of Sensitive Information – No ATO Required					
Estimated Cost To Government	Annual Responses	Review Time Per Response	Estimated Burden Hours	Average Wage + Overhead	Total Cost to Government

Gov't burden - No ATO Requirement.	2	6	12	$60.00*	$720.00

The Government's burden associated with the Safeguarding of Sensitive Information clause when an ATO is required would be limited to receipt, review and acceptance of the SA documentation, Independent Assessment, Renewal of the ATO, Federal Reporting and Continuous Monitoring Requirements, Incident Reporting requirements, Incident Response activities, PII and SPII Notification requirements, Credit Monitoring and receipt of Certification of Sanitization of Government and Government-Activity-Related Files and Information.

3052.204-7X, Safeguarding of Sensitive Information - ATO Required					
Estimated Cost To Government	**Annual Responses**	**Review Time Per Response**	**Estimated Burden Hours**	**Average Wage + Overhead**	**Total Cost to Government**
Gov't burden - ATO Requirement.	121	40	4,840	$60.00*	$290,400.00

Total estimated cost to the Government:

3052.204-7X, Safeguarding of Sensitive Information					
Estimated Cost To Government	**Annual Responses**	**Review Time Per Response**	**Estimated Burden Hours**	**Average Wage + Overhead**	**Total Cost to Government**
Total estimated cost to the Government.	123	46	5,658	$60.00*	$339,480.00

* Means estimated hourly wage according to the OPM salary table for calendar year 2015, GS-13, Step-4 (or equivalent), or $43.99 per hour, plus 36.25 percent ($15.95) overhead burden, and rounded to the nearest whole dollar, or $60.00.

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.