

SUPPORTING STATEMENT  
OMB Control Number 0750-0004  
Assessing Contractor Implementation of Cyber Security Requirements

A. JUSTIFICATION

1. Need for the Information Collection

This information collection is necessary to implement the NIST SP 800-171 DoD Assessment Methodology. This information collection is imposed on offerors and contractors that information systems that process controlled unclassified information through the use of the following solicitation provision and contract clause:

a. DFARS 252.204-70XX, Notice of NIST SP 800-171 DoD Assessment Requirement, is prescribed for use in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items. Per the new provision, if an Offeror is required to have implemented NIST SP 800-171 per DFARS clause 252.204-7012, then the Offeror shall have a current assessment for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order in order to be considered for award.

b. DFARS 252.204-70YY, NIST SP 800-171 DoD Assessment Requirements, is prescribed for use in in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items. The clause requires the contractor to provide the Government access to its facilities, systems, and personnel in order to conduct a Medium or High Assessment, if necessary. Medium Assessments are assumed to be conducted by DoD Components, primarily by Program Management Office cybersecurity personnel, in coordination with the DCMA's DIBCAC, as part of a separately scheduled visit (e.g., for a Critical Design Review). High Assessments will be conducted by, or in conjunction with, DCMA's DIBCAC. The Department may choose to conduct a Medium or High Assessment when warranted based on the criticality of the program(s)/technology(ies) associated with the contracted effort(s). For example – a Medium Assessment may be initiated by a Program Office who has determined that the risk associated with their programs warrants going beyond the Basic self-assessment. The results of that Medium Assessment may satisfy the Program Office, or may indicate the need for a High assessment.

2. Use of the Information

The information obtained through DFARS 252.204-70XX and 252.204-70YY, which enables DoD to strategically assess a contractor's implementation of NIST SP 800-171 on existing contracts that include DFARS clause 252.204-7012 and to obtain an objective assessment of a contractor's NIST SP 800-171 implementation status.

3. Use of Information Technology

Information technology is used to the maximum extent practicable. Specifically, the Supplier Risk Management System (SPRS) is used to electronically store and retrieve the NIST SP 9800-171 DoD Assessments. SPRS is DoD's authoritative source for supplier and product performance information. Use of this electronic system reduces duplicate submission of

information by contractors to multiple DoD requiring activities. It also serves as a single repository for Government access to assessment results.

#### 4. Non-duplication

As a matter of policy, DoD reviews the Federal Acquisition Regulation to determine if adequate language already exists. DoD requires a DoD–unique provision related to contractor self-assessments.

#### 5. Burden on Small Business

According to data available in the Electronic Data Access system for fiscal years (FYs) 2016, 2017, and 2018, on an annual basis DoD awards on average 485,859 contracts and orders that contain DFARS clause 252.204-7012 to 39,204 unique awardees, of which 262,509 awards (54%) are made to 26,468 small entities (68%). The need for a Basic Assessment will begin to impact entities as they compete on solicitations that include the new solicitation provision and contract clause, and the clause at DFARS 252.204-7012, if the entity has covered contractor information systems that are required to be in compliance with NIST SP 800-171. This will occur gradually over time as DoD issues new solicitations. It is assumed that 1/3 of the total unique awardees (13,068 entities) would be subject to the basic assessment requirements, 68% (8,823 entities) of which are estimated to be small entities. The Medium Assessment is expected to be conducted on 148 of the 13,068 small entities each year. The High Assessment is expected to be conducted on 81 of the 13,068 small entities each year. In addition, DoD Assessments are valid for three years, so entities will need to renew, at minimum, their basic assessment every three years. The burden applied to small business is the minimum consistent with applicable laws, Executive orders, regulations, and prudent business practices.

#### 6. Less Frequent Collection

Assessment results will be posted in SPRS. This will provide DoD Components with visibility to summary level scores and an alternative to addressing implementation of NIST SP 800-171 on a contract-by-contract approach—significantly reducing the need to conduct assessments at the program level, thereby reducing the cost to both DoD and industry..

#### 7. Paperwork Reduction Act Guidelines

There are no special circumstances for collection. Collection of this information is consistent with the guidelines at 5 CFR 1320.5(d)(2).

#### 8. Consultation and Public Comments

a. Special advisers from the DoD CISO and Contracting e-Business were consulted with regard to some of the burden estimates for which supporting data is not available in the Federal Procurement Data System.

b. This information collection is consistent with the guidelines in 5 CFR 1320.6. Public comments were solicited in the *Federal Register* on date (XX FR XXXX). \_\_\_\_ comments were received in response to this notice. The comments are available at regulations.gov and are summarized below.

c. A notice of submission to OMB for clearance of this information collection was published in the *Federal Register* on \_\_\_\_\_.

9. Gifts or Payment

DoD will not provide a payment or gift to respondents to this information collection requirement.

10. Confidentiality

This information is disclosed only to the extent consistent with statutory requirements, current regulations, and prudent business practices. The collection of information does not include any personally identifiable information; therefore, no Privacy Impact Assessment or Privacy Act System of Records Notice is required.

11. Sensitive Questions

No sensitive questions are involved in the information collection.

12. Respondent Burden and its Labor Costs

The following is summary of the estimated cost to comply with the NIST SP 800-171 DoD Assessment Requirements:

Estimation of Total Public Burden: NIST SP 800-171 DoD Assessments	
Total Number of Respondents	13,068
Total Number of Responses	13,378
Total Estimated Hours	57,601
Total Annual Cost	\$6,727,153

a. Basic Assessment.

i. *Calculating the self-assessment.* It is estimated that the burden to calculate the Basic Assessment score is thirty minutes per entity at a journeyman-level-2 rate of pay. This

results in a total estimated annual public cost of \$647,388 (13,068 entities \* (0.50 hour \* \$99.08/hour<sup>1</sup> = \$49.54/assessment)).<sup>2</sup>

ii. *Submission of assessment for posting in SPRS.* It is estimated that the burden to submit a Basic Assessment for posting in SPRS is 15 minutes per entity at a journeyman-level-2 rate of pay. This results in a total estimated annual public cost of \$323,695 (13,608 entities \* (0.25 hour \* \$99.08/hour = \$24.77/assessment)).

iii. *Total Annual Cost.* The total estimated annual public cost for 13,608 entities to complete a Basic Assessment is \$971,083 (13,608 \* \$74.31/assessment).

Estimation of Respondent Burden: NIST SP 800-171 DoD Basic Assessments	
Number of respondents	13,068
Responses per respondent	1
Number of responses	13,068
Hours per response	.75
Estimated hours	9,801
Cost per hour	\$99.08
Annual public burden	\$971,083
Cost per response	\$74.31

b. Medium Assessment.

i. *Preparing for assessment.* It is estimated that the burden to make the system security plan and supporting documentation available for review by the DoD assessor is one hour per entity at a journeyman-level-2 rate of pay. This results in a total estimated annual public cost of \$19,816 (200 entities \* (1 hour \* \$99.08/hour = \$99.08/assessment)).

ii. *Participating in assessment.* It is estimated that the burden to participate in the review and discussion of the system security plan and supporting documents with DoD assessor is three hours per entity, with one journeyman-level-2 and one senior-level-2 contractor employee participating in the assessment. This results in a total estimated annual public cost of \$142,080 (200 entities \* [(3 hours \* \$99.08/hour = \$297.24) + (3 hours \* \$137.72/hour = \$413.16) = \$710.40/assessment]).

<sup>1</sup> The journeyman-level-2 rate of pay is equivalent to the Office of Personnel Management (OPM) General Schedule (GS) FY20 rate of pay for a GS-13/step 5 employee for the locality pay area of “rest of the U.S.” plus a fringe factor of 2.0 (\$49.54 \* 2 = \$99.08).

<sup>2</sup> Note, the cost for contractors to assess their compliance with NIST SP 800-171 to ensure they are in compliance with the existing terms of their contracts (i.e. DFARS clause 252.204-7012), are not included in summary of costs associated with this rule. The rule calculates the cost of completing the Strategic Assessment; in the case of the basic assessment, the contractor is calculating a score based on where they stand in implementation of the NIST SP 800-171.

iii. *Establishing response date.* Assuming issues are identified, it is estimated that the burden to determine and provide to DoD the date by which the issues will be resolved is one hour per entity at a journeyman-level rate of pay. This results in a total estimated annual public cost of \$19,816 (200 entities \* (1 hour \* \$99.08/hour = \$99.08/assessment)).

iv. *Total Annual Cost.* The total estimated annual public cost for 200 entities to complete a Medium Assessment is \$181,712 (200 entities \* \$908.56/assessment).

Estimation of Respondent Burden: NIST SP 800-171 DoD Medium Assessments	
Number of respondents	200
Responses per respondent	1
Number of responses	200
Hours per response	8.0
Estimated hours	1,600
Cost per hour	\$113.57
Annual public burden	\$181,712
Cost per response	\$908.56

c. High Assessment.

i. *Participating in the assessment.* It is estimated that the burden to participate in the review and discussion of the system security plan and supporting documents to the DoD assessors is 116 hours per entity. The cost estimate is based on 2 senior-level-2 employees dedicating 32 hours each, 8 senior-level-1 employees dedicating 4 hours each, and 10 journeyman-level employees dedicating 2 hours each. This results in a total estimated annual public cost of \$1,599,645 (110 entities \* [(2 \* 32 hours \* \$137.72/hour = \$8,814.08) + (8 \* 4 hours \* 117.08/hour = \$3,746.56) + (10 \* 2 hours \* \$99.08/hour = 1,981.60) = \$14,542.24/assessment]).

ii. *Preparation and post review activities.* It is estimated that the burden to make the system security plan and supporting documentation available for review by the DoD assessors, prepare for demonstration of requirements implementation, and to conduct post review activities is 304 hours per entity. The cost estimate is based on 2 senior-level-2 employees dedicating 48 hours each, 8 senior-level-1 employees dedicating 16 hours each, and 10 journeyman-level employees dedicating 8 hours each. This results in a total estimated annual public cost of \$3,974,713 (110 entities \* [(2 \* 48 hours \* \$137.72/hour = \$13,221.12) + (8 \* 16 hours \* 117.08/hour = \$14,986.24) + (10 \* 8 hours \* \$99.08/hour = \$7,926.40) = \$36,133.76/assessment]).

iii. *Total Annual Cost.* The total estimated annual public cost for 110 entities to complete a High Assessment is \$5,574,358 (110 entities \* \$50,675.98/assessment).

Estimation of Respondent Burden: NIST SP 800-171 DoD High Assessments	
Number of respondents	110
Responses per respondent	1
Number of responses	110
Hours per response	420
Estimated hours	46,200
Cost per hour	\$120.66
Annual public burden	\$5,574,360
Cost per response	\$50,676.00

13. Respondent Costs Other Than Burden Hour Costs

DoD does not estimate any annual cost burden apart from the hourly burden in Item 12 above.

14. Cost to the Federal Government

The following is summary of the estimated cost to comply with the NIST SP 800-171 DoD Assessment Requirements:

Estimation of Total Public Burden: NIST SP 800-171 DoD Assessments	
Total Number of Responses	486,169
Total Estimated Hours	83,546
Total Annual Cost	\$9,536,160

a. Basic Assessment.

i. It is estimated that the burden for a Contracting Officer to validate that a potential awardee has a current Assessment (not older than years) in SPRS is 5 minutes at a journeyman-level rate of pay.

ii. This results in a total estimated annual Government cost of \$3,851,113 (485,859 awards \* (0.08 hours \* \$99.08/hour = \$7.93/award))

Estimation of Government Burden: NIST SP 800-171 DoD Basic Assessments	
Number of responses	485,859

Hours per response	.08
Estimated hours	38,869
Cost per hour	\$99.08
Annual Government burden	\$3,851,113
Cost per response	\$7.93

b. Medium Assessment.

i. *Conducting the assessment.* It is estimated that the burden for the DoD assessor to review the system security plan and supporting documentation made available by an entity is 3 hours at a journeyman-level rate of pay. This results in a total estimated annual Government cost of \$59,448 (200 entities \* 1 assessment \* (3 hours \* \$99.08/hour = \$297.24/assessment)).

ii. *Submission of assessment for posting in SPRS.* It is estimated that the burden to submit a Medium Assessment for posting in SPRS is 15 minutes per entity. This results in a total estimated annual Government cost of \$4,954 (200 entities \* (0.25 hour \* \$99.08/hour = \$24.77/assessment)).

iii. *Total Annual Cost.* The total estimated annual cost for the Government to complete 200 Medium Assessments is \$64,402 (200 entities \* \$322.01/assessment).

Estimation of Government Burden: NIST SP 800-171 DoD Medium Assessments	
Number of responses	200
Hours per response	3.25
Estimated hours	650
Cost per hour	\$99.08
Annual Government burden	\$64,402
Cost per response	\$322.01

c. High Assessment.

i. *Conducting the assessment.* It is estimated that the burden for the DoD assessors to review the system security plan and supporting documentation made available by an entity is 400 hours. The cost estimate is based on 1 senior-level-1 employee dedicating 80 hours and 4 journeyman-level employees dedicating 80 hours each. This results in a total estimated annual Government cost of \$4,517,920 (110 entities \* 1 assessment \* [(1 \* 80 hours \* 117.08/hour = 9,366.40) + (4 \* 80 hours \* \$99.08/hour = 31,705.60) = \$41,072/assessment]).

ii. *Travel.* The estimated travel costs per assessment are \$2,000 per person for 5 DoD assessors. This results in a total estimated annual Government cost of \$1,100,000 (110 entities \* (5 people \* \$2,000/person = \$10,000/assessment)).

iii. *Submission of assessment for posting in SPRS.* It is estimated that the burden to submit a Basic Assessment for posting in SPRS is 15 minutes per entity. This results in a total estimated annual Government cost of \$2,725 (110 entities \* (0.25 hour \* \$99.08/hour = \$24.77/assessment)).

iv. *Total Annual Cost.* The total estimated annual Government cost to complete 110 High Assessments is \$5,620,645 (110 entities \* \$51,096.77).

Estimation of Government Burden: NIST SP 800-171 DoD High Assessments	
Number of responses	110
Hours per response	400.25
Estimated hours	44,028
Cost per hour	\$102.68
Government Burden for Effort	\$4,520,645
Travel	1,100,000
Annual Government Burden	\$5,620,645
Cost per response	\$51,096

15. Reasons for Change in Burden

This is a new information collection requirement.

16. Publication of Results

Results of this collection will not be published.

17. Non-Display of OMB Expiration Date

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

18. Exceptions to "Certification for Paperwork Reduction Submissions"

There are no exceptions to the certification accompanying this Paperwork Reduction Act submission.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS



Statistical methods will not be employed.