FINAL REGULATORY FLEXIBILITY ANALYSIS
DFARS Case 2011-D039
Safeguarding Unclassified Controlled Technical Information

This final regulatory flexibility analysis has been prepared consistent with 5 U.S.C. 604.

1. Statement of the need for and the objectives, of the rule.

The objective of this rule is for DoD to avoid compromise of unclassified computer networks on which DoD controlled technical information is resident on or transiting through contractor information systems, and to prevent the exfiltration of controlled technical information on such systems. The benefit of tracking and reporting DoD information compromises is to—

- Assess the impact of compromise;
- Facilitate information sharing and collaboration; and
- Standardize procedures for tracking and reporting compromise of information.

2. Statement of the significant issues raised by the public comments in response to the initial regulatory flexibility analysis, a statement of the assessment of the agency of such issues, and a statement of any changes made to the rule as a result of such comments.

Several respondents stated that this rule will be financially burdensome for small businesses to the point that they will not be able to participate. Two respondents stated that the numbers used in the Initial Regulatory Flexibility Analysis grossly underestimate the number of businesses the rule will affect and the cost as a percentage of revenue that will be required to meet the requirements of the new rule. One respondent suggested that a gradually phased-in approach to implement these safeguards would ease the significant financial burden they impose.

No changes were made to the final rule as a result of these comments. The estimated burden in the final regulatory flexibility analysis has been reduced because the scope of the rule was modified to reduce the categories of information covered and only addresses safeguarding requirements that cover the unclassified controlled technical information and reporting the compromise of unclassified controlled technical information. The final rule is drafted with the aim of minimizing the burden of compliance on contractors while implementing the necessary safeguarding requirements.

3. The response of the agency to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration in response to the rule, and a detailed statement of any change made in the final rule as a result of the comments;

No comments were received from the Chief Counsel for Advocacy of the Small Business Administration.

4. Description of and an estimate of the number of small entities to which the rule will apply.

This final rule requires information assurance planning; including reporting of information compromise for DoD contractors that handle DoD unclassified controlled technical information. This requirement will also flow down to subcontracts. DoD believes that most information passed down the supply chain will not require special handling and recognizes that most large contractors handling sensitive information already have sophisticated information assurance programs and can take credit for existing controls with minimal additional cost. However, most small businesses have less sophisticated programs and will realize costs meeting the additional requirements. Based on figures from the Defense Technical Information Center it is estimated that 6,555 contractors would be handling unclassified controlled technical information and therefore affected by this rule. Of the 6,555 contractors it is estimated that less than half of them are small entities.

5. Description of the projected reporting, recordkeeping, and other compliance requirements of the rule.

Projected reporting and other compliance requirements shall be executed with known and approved industrial standards, and best practices for protecting unclassified networks and information systems, National Institute of Standards and Technology, Federal Information Processing Standards: For example:

- e-authentication mechanism in-place (e.g., PKI)
- Tracking and reporting mechanism, tools, and processes
- Access control procedures
- Training
- Assessment and compliance process, which may include collaboration with DoD on a damage assessment

This rule will apply to small entities with controlled technical information resident on or transiting through their unclassified networks or information systems.

The professional skills necessary for preparation of the report include knowledge of adequate network and information systems to recognize unauthorized intrusions.

6. Description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes.

The final rule reduces the categories of information that must be protected and clarifies the protection that must be implemented to more effectively define what contractors are required to do thus preventing small businesses from unnecessarily spending time and money on additional protection beyond what is required. The specified unclassified controlled technical information that must be protected can be present on contracts regardless of the size on the contractor; therefore exemptions in the applicability of the rule would significantly decrease the effectiveness of the rule.