DETERMINATION FOR EMERGENCY CLEARANCE

1. DoD has a requirement to collect information from offerors and contractors regarding the status of their implementation of implement the 110 system security requirements identified in the National Institute of Standards and Technology Special Publication (NIST SP) 800-171 on their information systems that process controlled unclassified information (CUI). This information is being collected through either a contractor's submission of a Basic self-assessment in DoD's Supplier Performance Risk System, or a Medium or High assessment of contractors conducted by DoD assessors. Results of a NIST SP 800-171 DoD Assessment reflect the net effect of NIST SP 800-171 security requirements not yet implemented by a contractor.

2. This collection of information is needed prior to the expiration of the time periods normally associated with a routine submission for review under the provisions of the Paperwork Reduction Act, to enable the Department to immediately begin assessing the current status of contractor implementation of NIST SP 800-171 on their information systems that process CUI. Several industry association questionnaires, Defense Contract Management Agency assessments of defense contractors, and a DoD Inspector General (IG) Report (DODIG-2019-105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that defense contractors have not fully or consistently implemented the NIST SP 800-171 security requirements on their covered information systems.

3. The collection of information is essential to DoD's mission. The National Defense Strategy (NDS) and DoD Cyber Strategy highlight the importance of protecting the Defense Industrial Base (DIB) to maintain national and economic security. To this end, DoD has required defense contractors and subcontractors to have implemented the NIST SP 800-171 security requirements on information systems that handle CUI since 2017, pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. This DoD Assessment Methodology enables the Department to assess strategically, at a corporate-level, contractor implementation of the NIST SP 800-171 security requirements. Results of a NIST SP 800-171 DoD Assessment reflect the net effect of NIST SP 800-171 security requirements not yet implemented by a contractor.

4. Moreover, DoD cannot comply with the normal clearance procedures, because public harm is reasonably likely to result if current clearance procedures are followed. Authorizing collection of this information on the effective date will motivate defense contractors and subcontractors who have not yet implemented existing NIST SP 800-171 security requirements, to take action to implement the security requirements on covered information systems that process CUI, in order to protect our national and economic security interests. The aggregate loss of sensitive controlled unclassified information and intellectual property from the DIB sector could undermine U.S. technological advantages and increase risk to DoD missions.

5. The information that is requested is the minimum necessary to ensure the Department's ability to conduct this strategic assessment current status of contractor implementation of NIST SP 800-171. A notice will be published in the *Federal Register* prior to the submission

of a subsequent information collection package to OMB under regular processing timeframes.