DATE: July 10, 2015

TO: Sharon Mar
Office of Information and Regulatory Affairs
Office of Management and Budget

THROUGH: Kathy Axt
Privacy, Information Collection Clearance Division
U.S. Department of Education

FROM: for Keith Wilson Patsy Garnett
Chief Information Officer, Federal Student Aid

SUBJECT: Emergency Clearance of Information Collection to Allow for Use of Guaranty Agencies IT Security Self-Assessments of their Protection of Personally Identifiable Information

The nation-wide instances of data breaches impacting organizations entrusted with Personally Identifiable Information (PII) continue to proliferate. The latest breach of current and former federal employees' PII has reinforced the need for focused action by the U.S. Government to combat cybersecurity threats and to strengthen the Government's cybersecurity infrastructure. Federal Student Aid (FSA) is participating in this focused action and continues to work with its partners to improve the confidentiality and integrity of students' financial information collected in connection with the Federal student financial aid programs. FSA expects all of its guaranty agency (GA) partners who possess student information to quickly assess and implement strong security policies and controls, implement improvements, as needed, and continue to monitor their operations for adherence to those polices and controls, and continue to comply with all applicable security requirements.

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security.

A GA is a State or private nonprofit agency that has agreements with the Department of Education to administer aspects of the Federal Family Education Loan (FFEL) Program, including insuring private lenders against losses due to a borrowers default. GAs connect to the National Student Loan Data System, which is the central database for Title IV student financial aid and stores information about loans, grants, borrowers, lenders, schools, and servicers. At least monthly, GAs provide loan data to the Department on FFEL Program loans including, but not limited to loan origination information and loan repayment information about a loan until the loan is paid in full or closed.

FSA is initiating a formal assessment program of the GAs that will ensure the continued confidentiality and integrity of data entrusted to FSA by students and families. The assessment will identify security deficiencies based on the Federal standards described in the National Institute of Standards and Technology (NIST) publications. The comprehensive IT Security Self-Assessment links all questions on the assessment to a NIST control.

The Department requests that OMB approve the attached IT Security Self-Assessment and Attestation by July 20, 2015 and waive the requirements under 1320.5(a)(1)(iv) to publish notice of the Information Collection and Attestation in the Federal Register, as authorized under 1320.13(d). To assure the security of the student's financial information, FSA must implement processes with its external partners to assess and implement strong security policies and controls.

Due to the nature of expanding examples of PII security breaches and the sensitive nature of the data that our GA partners possess and access meet the standards for emergency clearance in 1320.13(a)(2)(i) and (iii). We also believe that the inability to collect the security information would prevent the Department from ensuring the integrity, of system data, including personally identifiable information, and the protection of the information from unauthorized access, misuse, disclosure, and destruction. The use of normal clearance procedures would delay the Department's ability to ensure the continued confidentiality and integrity of data entrusted to us by students and families.

Thank you for your prompt consideration of this request. If you have additional questions, please contact Linda Wilbanks at Linda.Wilbanks@ed.gov or (202) 377-3396.