UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, DC 20202

GEN 15-17

JUL 29 2015

Subject: Protecting Student Information

Summary: This Dear Colleague Letter (DCL) reminds Guaranty Agencies (GAs) of their obligation to submit a self-assessment as part of a recent security program initiated by Federal Student Aid (FSA) and advises GAs of the steps FSA will take to ensure appropriate management and protection of personally identifiable information (PII) under the control of GAs.

Dear Colleague:

The nationwide instances of data breaches impacting organizations entrusted with PII continue to proliferate and reinforce the need for focused action by the U.S. Government to combat cybersecurity threats and to strengthen the Government's cybersecurity infrastructure. We write to remind you that as part of these Government-wide efforts, and FSA's own continuing steps to improve the security of information – including PII – that is used, stored, and transmitted by FSA partners, FSA has recently established a process for a detailed self-assessment of the information technology security of our GA partners. This security self-assessment requires your response by July 31, 2015 (this deadline was extended from the original deadline of June 30, 2015).

In a June 8, 2015, letter to all GAs from Mr. Keith Wilson, FSA's Chief Information Officer, FSA initiated a formal program for the assessment of GAs that will identify any security deficiencies based on the Federal standards described in the National Institute of Standards and Technology (NIST)[1] publications. The comprehensive security self-assessment for GAs aligns each question to a NIST control.

Consistent with NIST's standards, FSA expects all of its partners who possess student information to continuously implement strong security policies and controls, implement improvements, as needed, and monitor their operations for adherence to those policies and controls, as well as applicable security requirements. The Higher Education Act of 1965, as amended (HEA) requires GAs to maintain the administrative capability to perform their responsibilities under their guaranty agreements, which includes maintaining information

[1] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf NIST 800-53 Rev. 4 provides a catalog of security and privacy controls for Federal information systems and organizations and a process for selecting controls to protect organizations and information systems. The controls are implemented as part of an organization-wide process that manages information security and privacy risk and address a diverse set of security and privacy requirements across the Federal government and critical infrastructure. An additional standard to consider can be found at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf. NIST 800-171 provides Federal agencies with recommended requirements for protecting the confidentiality of controlled unclassified information (CUI) in Non-Federal systems.

security capabilities.[2] FSA's new self-assessment program will assist GAs and FSA in assessing the capabilities of GAs to secure the PII they have, including by:

- Assessing the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- Determining the levels of information security appropriate to protect information and information systems;
- Implementing and enforcing policies and procedures to cost-effectively reduce risks to an acceptable level; and
- Conducting regular testing and evaluation of information security controls and techniques to ensure effective implementation of such controls and techniques.

Following submission of the detailed security self-assessments from our GA partners, FSA will analyze the results to identify the strengths and weaknesses of the security of the information maintained by GAs. GAs that have significant weaknesses in their controls and other security gaps will be required to submit within 45 days an acceptable management plan that includes corrective action plans (CAPs) to resolve weaknesses in their controls and security gaps within approved time-frames. In order to protect PII of students and borrowers, if a GA fails to submit a required management plan, the management plan is not acceptable to FSA, or such plan's CAPs are not implemented according to the approved schedules, FSA is prepared to take appropriate action under its legal authorities.[3]

FSA's continuing security efforts are intended to be a partnership between FSA and GAs that will ensure the continued security and integrity of data entrusted to us by students and families. FSA also strongly encourages GAs to collaborate with, and utilize the resources of, US-CERT and other organizations dedicated to protection of information systems and the sensitive data they process. FSA recognizes the contributions of GAs to the Federal student financial aid system and appreciates that GAs understand the seriousness of our efforts to address increasing cybersecurity threats. If you have any questions about the information contained in this DCL, please submit them to FSA_GAsecurity@ed.gov.

Sincerely,

James W. Runcie
Chief Operating Officer
Federal Student Aid

Ted Mitchell
Under Secretary

---

[2] See §428(c)(9)(C) of the HEA.
[3] See §428(c)(9)(C) and (E) of the HEA.