UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Evaluation and Inspection Services

May 5, 2009

Memorandum

TO: James Manning
Acting Chief Operating Officer
Federal Student Aid

FROM: Wanda A. Scott /s/
Assistant Inspector General
Evaluation, Inspection, and Management Services

SUBJECT: Final Management Information Report
Review of Federal Student Aid's Enterprise Risk Management Program (ED-OIG/I13I0005)

This final management information report presents the results of our review of Federal Student Aid's (FSA) Enterprise Risk Management Program and FSA's response to those results.

BACKGROUND

In May 2006, FSA formally created the Enterprise Risk Management Group (ERMG). The ERMG is divided into two main areas: the Internal Review Division and the Risk Analysis and Reporting Division. The Internal Review Division is responsible for helping to ensure that an effective internal control framework is in place across the enterprise; however, it does not have any responsibilities related to the implementation of enterprise risk management. The Risk Analysis and Reporting Division is responsible for developing an enterprise risk management strategy and implementing an enterprise risk management program at FSA.

The ERMG is headed by the Chief Risk Officer who reports to the General Manager of Enterprise Performance Management Services. According to FSA's Five-Year Plan for 2006-2010, the enterprise risk management function was intended to develop risk assessments and provide a more strategic view of future risks, and was designed to better equip senior management to anticipate, analyze, and manage risks inherent in the federal student financial assistance programs.

FSA's enterprise risk management program is based on the Enterprise Risk Management – Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO Framework). The COSO Framework defines enterprise risk management as a "process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that

may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

The COSO Framework consists of eight interrelated components that are derived from the way management runs an enterprise and are integrated with the management process. The components are described as follows:

- *Internal Environment* – this component serves as the basis for enterprise risk management and is comprised of the entity's risk management philosophy; its risk appetite;[1] the integrity, ethical values, and competence of the entity's employees; and the environment in which those employees operate.
- *Objective Setting* – the entity ensures it has a process to set objectives and that the objectives support and are aligned with the entity's mission. Objective Setting is a precondition to Event Identification, Risk Assessment, and Risk Response.
- *Event Identification* – the entity identifies internal and external events affecting the achievement of its objectives, and distinguishes between risks (negative impact) and opportunities (positive impact).
- *Risk Assessment* – the entity analyzes identified risks, considering likelihood and impact, to determine how they should be managed.[2]
- *Risk Response* – the entity identifies and evaluates possible responses to risk, and selects a set of actions to align risks with the entity's risk tolerances[3] and risk appetite.
- *Control Activities* – the entity establishes and executes policies and procedures to help ensure that the risk responses are effectively carried out.
- *Information and Communication* – the entity identifies, captures, and communicates relevant information throughout the entity in a clear form and timeframe that enables people to carry out their responsibilities.
- *Monitoring* – the entire entity monitors itself through ongoing management activities and/or separate evaluations.

According to the ERMG, enterprise risk management at FSA is "a coordinated, culture-based approach to holistically addressing all of an organization's risks – including operational, financial, strategic, compliance and reputational risks under one umbrella."

The ERMG is implementing its COSO Framework-based enterprise risk management program in three phases.

[1] Risk appetite is defined as the amount of risk an entity is willing to accept in pursuit of its mission.
[2] Risks within the COSO Framework are discussed in terms of inherent risk and residual risk. Inherent risk is defined by the COSO Framework as the risk to an entity in the absence of any actions management might take to alter the risk's likelihood or impact. The ERMG uses a similar term, aggregate risk, which it defines as the total amount of exposure associated with a specified risk that does not include the effect of risk strategies, controls or other measures designed to mitigate the effect of the specified risk. Residual risk is defined by the COSO Framework and the ERMG as the risk that remains after action has been taken to alter the risk's likelihood or impact.
[3] Risk tolerances are defined by the COSO Framework as the acceptable levels of variation relative to the achievement of objectives. In other words, it is the amount of variation that an entity is willing to accept in pursuit of its goals and objectives.

- Phase I involves establishing the ERMG and committee, developing a strategy and methodology for implementation, obtaining contractor services, and communicating enterprise risk management information to FSA's executives.
- Phase II consists of formalizing the enterprise risk management strategy and project plan, adopting a risk framework, developing an enterprise risk management website, conducting a high-level risk assessment at FSA, developing a methodology for performing business unit risk assessments, developing a risk tracking system, and identifying, assessing, and inventorying risks for 25 percent of FSA's business units. These activities focus on the Event Identification and Risk Assessment components of the COSO Framework.
- Phase III involves identifying, assessing, and inventorying risks for the remaining 75 percent of the business units, creating enterprise level reports for senior management, documenting FSA's risk tolerances and appetites, and developing a methodology for fully implementing the remaining enterprise risk management components.

The ERMG's project plan indicates that all phases will be complete by September 30, 2010.

REVIEW RESULTS

The objective of our inspection was to evaluate FSA's implementation of enterprise risk management. The ERMG has not fully addressed any of the COSO Framework's eight components. The COSO Framework states that determining whether an enterprise risk management program is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. While it has developed plans and begun business unit activities related to three components (Objective Setting, Event Identification, and Risk Assessment), the plans for fully addressing the remaining five components at FSA (Internal Environment, Risk Response, Control Activities, Information and Communication, and Monitoring) have received limited attention. As a result, FSA has not implemented enterprise risk management. This report will present information on FSA's progress toward implementation as of December 2008.

The Chief Risk Officer began working at FSA in June 2004. FSA's former Chief Operating Officer formally approved the ERMG in May 2006, nearly two years later. Prior to formal approval, the ERMG began conducting activities associated with Phase I of its program. After receiving formal approval, the ERMG officially started its enterprise risk management program and began strategic planning. The Chief Risk Officer and the Risk Analysis Team Leader informed us that FSA management also assigned them multiple high priority special projects, such as a regional workforce effectiveness study, conducted for approximately seven months, which limited the amount of time available to implement enterprise risk management. The ERMG completed Phase I of its program on December 30, 2006, and has nearly completed all activities associated with Phase II.

The ERMG began work in FSA's business units in May 2007. As of December 2008, the ERMG has completed risk identification, aggregate risk assessment, and inventory activities for 3 of 26 business units. As part of these initial business unit activities the ERMG also aligned

each business unit's goals and objectives with FSA's strategic objectives. These three business units are:

- Communications, Reporting, and Analysis;
- Facilities, Security, and Emergency Management Services; and
- Workforce Development Services.

The ERMG has nearly completed risk identification in two other business units:

- Conferences and Administration Services; and
- Human Resources and Workforce Services.

The ERMG has initiated work in three more business units:

- Strategic Planning;
- Financial Management; and
- Budget.

None of FSA's business units directly responsible for administering the federal student aid programs have been examined or included in ERMG's business unit activities to date. The Chief Risk Officer anticipates that the ERMG will have risks documented in all 26 business units by the end of calendar year 2009, and has hired a contractor to help accomplish this task within this timeframe. In addition, as a training tool for new risk analysts, the ERMG is planning a review of the Enterprise Risk Management business unit.

After risk identification, aggregate risk assessment, and inventory activities have been completed for all business units, the ERMG plans to return to each business unit to identify the risk responses and assess the amount of residual risk given the control activities in place. According to the ERMG's project plan, the end date for these activities is September 30, 2010. The ERMG does not have a formal methodology in place for identifying risk responses and assessing the amount of residual risk.

The business unit risk activities thus far have concentrated on Event Identification and Risk Assessment at the aggregate level. The ERMG has also given attention to the Objective Setting component at the FSA-wide level and as part of each business unit review. The Chief Risk Officer said that the Risk Assessment component is more straightforward than the Internal Environment and Objective Setting components of the COSO Framework. The ERMG has not focused on the Internal Environment component, including defining FSA's risk appetite and risk philosophy, nor has it begun to conduct activities specifically related to the Risk Response, Control Activities, Information and Communication, and Monitoring components.

The ERMG's limited attention to the Internal Environment component is noteworthy given the importance placed on it throughout the COSO Framework and in the ERMG's own definition. The COSO Framework states that the Internal Environment "sets the basis for how risk and control are viewed and addressed by an entity's people." The ERMG's definition of the Internal Environment, based on the COSO Framework's description of that component, states that the Internal Environment is "the tone of an organization, influencing the risk consciousness of its people, and is the basis for all other components of risk management." According to the ERMG's definition, Internal Environment elements include an entity's risk management philosophy; its risk appetite; the integrity, ethical values, and competence of the entity's people; and the way management assigns authority and responsibility. The COSO Framework states that

the "effectiveness of enterprise risk management cannot rise above the integrity and ethical values of the people who create, administer, and monitor entity activities."

While both the COSO Framework and the ERMG, as expressed in its definition, agree that the Internal Environment serves as a basis for all other components of enterprise risk management, the ERMG's work has not addressed the specific elements of the Internal Environment. The ERMG has not ensured that FSA has a defined risk management philosophy or risk appetite. Additionally, the ERMG has not given attention to existing information on FSA's Internal Environment such as FSA-wide surveys indicating that there are perceptions on the part of FSA staff concerning a lack of integrity, ethical values and commitment to competence from FSA leadership or Office of Inspector General audits that have also found issues with FSA's Internal Environment. The COSO Framework emphasizes that the negative impact of an ineffectual Internal Environment can be far-reaching.

FSA COMMENTS

On March 17, 2009, we provided FSA with a copy of our draft management information report for comment. We received FSA's comments to the report on April 14, 2009. FSA did not take issue with any of the factual information presented in the report, but did have comments on the way in which the information was presented. We have summarized FSA's concerns and provided our responses below. FSA's response, in its entirety, is attached.

FSA Comment

FSA stated that we did not elaborate on what is meant by the statement in the report that "ERMG has not fully addressed any of the COSO Framework's eight components," and that this implies that the ERMG's efforts relating to the eight components of COSO are in some way deficient. FSA also stated that OIG's assertion that FSA has "not implemented enterprise risk management" is somewhat misleading because it states the obvious and could undermine the ERMG's efforts because many of the benefits associated with enterprise risk management can be and are realized prior to the "full implementation."

OIG Response

The statement that the "ERMG has not fully addressed any of the COSO Framework's eight components" is a conclusion based on a review of the ERMG's activities thus far. The Review Results section of the report fully explains the status of each of the eight components. For example, on page 3 we explained that the ERMG has developed plans and begun activities related to three components and that the plans for fully addressing the remaining five components have received limited attention. On page 4 we noted that none of FSA's business units directly responsible for administering the federal student aid programs have been examined or included in ERMG's business unit activities to date. The statement that FSA has "not implemented enterprise risk management" is also a conclusion in answer to our objective and is supported by all of the facts presented in our report. This conclusion is necessary for a full understanding of the current state of enterprise risk management at FSA. To the extent that FSA management recognizes value in the efforts of the ERMG, the facts presented in our report should not undermine the work of the ERMG. We note that in its response, FSA did not provide

any specific benefits that have been realized as a result of its enterprise risk management implementation efforts.

FSA Comment
FSA stated that while the business unit activities referred to in the report represent a significant part of FSA's enterprise risk management program, the ERMG conducted other activities between May 2007 and December 2008. FSA provided a list of activities the ERMG had conducted during this time. FSA stated that OIG's failure to recognize these activities in the 'Review Results' section of the report could present an unbalanced view of the status of FSA's enterprise risk management program and associated implementation efforts.

OIG Response
OIG did not recognize all of the ERMG's activities in the Review Results section. In the Background section of our report, we noted that Phase I of FSA's enterprise risk management program included "obtaining contractor services," and "communicating enterprise risk management information to FSA executives" and Phase II included "conducting a high-level risk assessment" and "developing a risk tracking system." In the Review Results section of our report, we stated that the ERMG had completed Phase I of its program and had nearly completed all activities associated with Phase II.

The report did not discuss the development of tools, resources, policies, procedures, and process documents to guide and support the program because they are typical activities when starting new programs and are not unique to the implementation of enterprise risk management at FSA. The report is not designed to be a catalog of all the activities conducted by the ERMG since its inception, but rather to explain the current state of enterprise risk management at FSA.

FSA Comment
FSA stated that it disagrees with the characterization that it has devoted limited attention to the Internal Environment component and stated that it has performed or is in the process of performing significant efforts relating to FSA's internal environment. The specific example that FSA provided was the high-level risk assessment performed under a purchase agreement with Grant Thornton LLP which, according to FSA, provided a high-level baseline review and documentation of FSA's internal environment.

OIG Response
We reviewed Grant Thornton's high-level risk assessment and the associated purchase order during the course of our fieldwork. We found that a review of FSA's internal environment was not the primary purpose of the work as it was not mentioned in the task order and was not included in the initial draft report provided to FSA. In fact, the Risk Analysis Team Leader, who also served as the Contracting Officer's Representative for the purchase order, told us during our fieldwork that the internal environment section was not very involved. When discussing the assessment, the Chief Risk Officer said that he wanted the contractor to do a quick review of the internal environment so the ERMG could check off that it had been completed.

The listing of documents reviewed by Grant Thornton, found in Appendix B of its final report, does not contain OIG reports or FSA-wide employee surveys. At the time of Grant Thornton's work, OIG had completed audits that identified significant internal control weaknesses at FSA. Additionally, there were employee survey results suggesting a concern among FSA staff about a

lack of integrity, ethical values and commitment to competence from FSA leadership. Because the high-level risk assessment is the only area in which the ERMG claims to have addressed Internal Environment on an enterprise-wide level and based on the weaknesses related to the report noted above, we concluded that the ERMG has given limited attention to the Internal Environment component.

FSA Comment

FSA stated that it believes the ERMG efforts related to the Internal Environment component are substantial; however, it stated that it did not intend to audit or opine on the strength or effectiveness of this component. FSA further stated that to do so would be premature and offer little or no added value.

OIG Response

We stand by our conclusion that the ERMG's efforts related to the Internal Environment component are limited. The ERMG defines the Internal Environment component as "the tone of an organization, influencing the risk consciousness of its people, and is *the basis for all other components of risk management*." [Emphasis added.] According to the ERMG definition, Internal Environment elements include an entity's risk management philosophy; its risk appetite; the integrity, ethical values, and competence of the entity's people; and the way management assigns authority and responsibility. As we stated in our report, "[t]he ERMG has not ensured that FSA has a defined risk management philosophy or risk appetite. Additionally, the ERMG has not given attention to existing information on FSA's Internal Environment such as FSA-wide surveys indicating that there are perceptions on the part of FSA staff concerning a lack of integrity, ethical values and commitment to competence from FSA leadership…." The COSO Framework states that the "effectiveness of enterprise risk management cannot rise above the integrity and ethical values of the people who create, administer, and monitor entity activities."

The ERMG's efforts related to the Internal Environment component are not substantial due to the fact that the ERMG has not addressed the specific elements of the component. The fact that FSA believes that determining the strength or effectiveness of this component would be premature and offer little or no added value is contradictory to the importance placed on it in the COSO Framework and by the ERMG's own definition.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our inspection was to evaluate FSA's implementation of Enterprise Risk Management.

We began our fieldwork on July 17, 2008 and conducted an exit conference on February 10, 2009.

The scope of our review included the ERMG's implementation activities at FSA from the hiring of the Chief Risk Officer in June 2004 to December 2008.

We reviewed COSO's *Enterprise Risk Management – Integrated Framework*. To evaluate FSA's implementation of enterprise risk management, we reviewed the ERMG's Strategic Plan, Project Plan, methodology for conducting business unit risk activities, risk categories, risk ratings, risk heat map, risk terminology, and listing of special projects. We also reviewed seven of the ERMG's PowerPoint presentations and documents related to Business Unit Risk Activities in five business units, including summary reports for three of those business units. We reviewed documents associated with both of the ERMG's purchase agreements for enterprise risk management support services, ED-06-AG-0039 with Grant Thornton and ED-08-AG-0003 with ADI Consulting, including the High-Level Risk Assessment created by Grant Thornton under Task Order 1 of their purchase agreement. We also interviewed FSA staff in the ERMG.

Our inspection was performed in accordance with the *2005 President's Council on Integrity and Efficiency Quality Standards for Inspections* appropriate to the scope of the inspection described above.

ADMINISTRATIVE MATTERS

In accordance with the Freedom of Information Act (5 U.S.C. §552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

Electronic cc: Linda Hall, Acting General Manager, Enterprise Performance Management Services
Stan Dore, Chief Risk Officer
Marge White, Director, Internal Review Division
Cynthia Vitters, Team Leader, Risk Analysis Team

April 10, 2009

Mr. W. Christian Vierling
Director, Evaluation and Inspection Services
U.S. Department of Education
Office of Inspector General
550 12th Street, S.W., Room 8153
Washington, DC 20024

Dear Mr. Vierling:

Thank you for providing us with an opportunity to respond to the Office of Inspector General's (OIG) draft management information report entitled, "Review of Federal Student Aid's Enterprise Risk Management Program" (Control Number ED-OIG/I13I0005). While we understand that since this report did not contain any recommendations for corrective action, no response is required, we appreciate the opportunity to address some of the information, comments and assertions contained therein.

As noted in the background section of this management information report (MIR), Federal Student Aid's Enterprise Risk Management Group (ERMG) was created in May 2006 to provide a more strategic view of risks at Federal Student Aid (FSA) and better enable senior management to identify, assess, manage and monitor those risks. In support of those objectives, ERMG's Risk Analysis & Reporting Division is leading the effort to implement an Enterprise Risk Management (ERM) Program at FSA. This effort, which is among the first of its kind in the federal government, represents a forward-looking and proactive approach to evaluating and managing risk, especially at the enterprise or strategic level.

Since much of the focus of this inspection was centered on evaluating FSA's implementation of its ERM program against its adherence to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework, we feel compelled to respond to some assertions contained in the OIG Inspection report that we do not believe to fairly characterize the results of our effort to date. One such example of this is the statement that "ERMG has not fully addressed any of the COSO Framework's eight components." The report does not elaborate on what is meant by "fully addressing" the components, yet implies that ERMG's efforts relating to the eight components of COSO are in some way deficient.

FSA has chosen to adopt a framework, which is based on the ERM Integrated Framework issued in 2004 by COSO. Since the COSO Framework was developed primarily with public stockholder-owned corporations in mind, Federal Student Aid has spent considerable time evaluating and considering how to utilize various aspects of this Framework to be most applicable and beneficial to a federal entity.

Federal Student Aid has made the decision to address all eight components in its ERM Program, Strategy, and/or Project Plan documents, which were provided to the OIG inspectors at the beginning of their fieldwork. At no point during the inspection did ERMG represent that all activities related to these components were complete and some are not yet even in process. However, we are not applying the COSO Framework in the exact manner or order described in the COSO guidance. The guidance in COSO all but mandates this approach. Specifically, COSO states: "No two entities will, or should, apply enterprise risk management in the same way. Companies and their enterprise risk management capabilities and needs differ dramatically by industry and size, and by management philosophy and culture. Thus, while all entities should have each of the components in place and operating effectively, one company's application of enterprise risk management – including the tools and techniques employed and the assignments of roles and responsibilities – often will look very different from another's."

The implementation and execution of an effective ERM program is a multi-year effort that requires time, commitment, support and resources. Therefore, we believe that the OIG's assertion that FSA has "not implemented enterprise risk management" is somewhat misleading. Our concern is that since it merely states the obvious, it tends to undermine ERMG's efforts as this is not a realistic expectation or goal at this point in time. In fact, only a very small percentage of publicly traded companies have fully implemented ERM programs, despite having a significant head start over their government counterparts. Most ERM programs, like FSA's, are works-in-progress. Despite this, many of the benefits associated with ERM can be and are realized prior to the "full implementation" of ERM.

FSA's ERM Program competes with other ERMG efforts including special projects, risk assessments and internal reviews. It was developed internally with extensive planning, analysis and research, which was a necessity as there is no governmental guidance directly related to ERM, or other federal ERM programs to model after. The ERM Program consists of various additional efforts beyond the business unit risk activities referred to in the OIG's report. While the business unit risk activities represent a significant part of FSA's ERM Program, numerous other activities were underway during the May 2007 through December 2008 time period referenced by this report. These activities include:

- Conduct a high-level risk assessment to identify and assess FSA's strategic risks;
- Development and finalization of various risk resources and tools to guide and support the ERM Program;
- Development and implementation of an advanced risk tracking database;
- Training and presentations provided to internal business units, senior management and entities outside of Federal Student Aid;
- Conduct various activities required to acquire contractor support for the ERM effort; and
- Completion of various policies, procedures and/or process documents in support of FSA's ERM Program.

We believe that failure to recognize these activities in the 'Review Results' section of this report can present an unbalanced view of the status of FSA's ERM Program and associated implementation efforts.

Considerable attention in this report also focuses on what OIG characterizes as "ERMG's limited attention to the Internal Environment component" of the COSO ERM Framework. We respectfully disagree with this characterization and maintain that significant efforts relating to FSA's Internal Environment have been performed or are in process. Prior to beginning the detailed risk activities currently underway, ERMG engaged an independent contractor, Grant Thornton, LLP (GT), to perform a high-level risk assessment at FSA. As part of that effort, GT also performed a high-level baseline review and documentation of FSA's Internal Environment as defined by the COSO ERM Framework. The results of that review were contained in the high-level risk report presented to executive management. At the same time, efforts to document and evaluate the Internal Environment at FSA continue as part of other activities associated with the implementation of FSA's ERM Program.

We believe that the combined ERMG efforts discussed above and relating to the COSO Internal Environment component are substantial. Nonetheless, we appear to have fundamental differences with the OIG about the timing of activities associated with incorporating this component into FSA's framework. Although the baseline review and documentation of the Internal Environment were performed as planned, we did not intend as part of that effort to audit or opine on the strength or effectiveness of this COSO component. To do so, in our opinion, would be premature and offer little or no added value.

While efforts to implement an ERM Program at FSA are not free from challenges or mistakes, they do offer a unique opportunity to enhance the organization's risk management practices, understanding and culture. Our process of implementing an ERM Program is one of continuous enhancement, refinement and adoption of best practices. As such, we appreciate the chance to share our efforts and progress with the OIG's inspection team and hope to further improve FSA's ERM Program based on the feedback provided.

Sincerely,

/s/

James F. Manning
Acting Chief Operating Officer