The Secretary of Energy
Washington, D.C. 20585

July 9, 2012

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

FROM: STEVEN CHU Steven Chu

Subject: Enterprise Risk Management (ERM) Framework for Directives

This memorandum explains a new standardized framework that the Department will be using to develop, revise, and review Departmental Directives. This framework is being called "Enterprise Risk Management," or ERM. It creates a uniform process to evaluate: (1) the risks that a proposed Directive is intended to address; (2) for each risk, the probability of that risk occurring and the potential impact if it does; (3) the existing Directives or other controls that are already in place to mitigate that risk; and (4) if there are unacceptable risks that are not already controlled, the best way of protecting against that risk. The attached document provides additional detail on each of these four steps of the ERM framework.

This standardized framework to review Directives will help the Department to weigh the wide-ranging risks (e.g., technical, financial) inherent in our work in a consistent way, as new Directives are being considered or existing Directives are evaluated and revised. By applying ERM to all Directives, we can further ensure that when a Directive is issued or revised, that the Department has considered all of the known risks and made a thoughtful determination of how to best mitigate them. This process will also help avoid duplicative or overlapping Directives, and the creation of Directives when another effective means of mitigating the risk is already in place.

In order to institutionalize the ERM process framework for Directives, I am directing the following activities:

- By July 15, 2012, the Office of Management, led by Ingrid Kolb, and the Integrated Management System team, led by Mike Weis, will develop a training and facilitation program to guide offices that will be proposing new or revised Directives on how to use ERM to frame and present their proposed Directives.

- By September 1, 2012, all offices submitting new or revised Directives will ensure that Justification Memoranda submitted to the Directives Review Board are accompanied by a document reflecting the initial application of the four ERM steps to the proposed Directive.

- By September 30, 2012, the Office of Management will incorporate ERM into DOE Order 251.1C and will make any necessary edits to processes and procedures of the Directives Program to ensure that the ERM framework is used to consider all proposed or revised Directives.

- The Associate Deputy Secretary, in his role as Chair of the Chief Operating Officers Board, and the members of the Directives Review Board will be responsible for ensuring that all management decisions relating to the issuance or revision of DOE Directives have fully applied the ERM framework.

- The Office of Management and the Integrated Management System team will continue to look for other opportunities to apply the ERM framework within the Department.

Attachment

Enterprise Risk Management Framework

The Enterprise Risk Management (ERM) framework includes four steps: identify the risks, determine the probability and impact of each one, identify controls that are already in place that mitigate that risk, and propose additional controls if needed.

Step 1: Identify Risks – What can go wrong? This step should identify the negative outcomes that could result from an action or decision. It is important to consider a wide range of risks, and so the Department's ERM framework includes five broad categories:

(1) Mission – can a system, action, or decision hinder accomplishment of the mission?
(2) People – will a failure impact the well-being of an employee or the public?
(3) Physical Assets – could there be loss or damage to a physical asset (e.g., property)?
(4) Financial – could there be loss of funds or unavailability of funds?
(5) Reputation and Trust – will the Department suffer damage to its credibility with the public or other stakeholders?

Step 2: Determine the probability and impact. Through either a quantitative or qualitative analysis, this step captures the probability of the risk occurring and the impact to the Department if it does. For this step, it is important to assume that no controls are in place or mitigating actions are taken. Probability and impact are then combined, using the table below, to arrive at an overall risk level. Common definitions help ensure consistency.

Impact:
Negligible – impact is easily and quickly corrected with little effort or time
Low – short-term impact, easily corrected without long-term consequences
Medium – significant short-term impacts, significant time and resources to recover
High – impacts are catastrophic and long-term, significantly affecting the mission

		Impact			
Probability		Negligible	Low	Medium	High
	Certain	Minor	Moderate	Extreme	Extreme
	Likely	Minor	Moderate	Significant	Extreme
	Possible	Minor	Moderate	Significant	Extreme
	Unlikely	Minor	Minor	Moderate	Significant
	Rare	Minor	Minor	Minor	Moderate

Probability:
Rare – probability is incredible during the time period of interest
Unlikely – unlikely to occur to during the time period of interest
Possible – an even possibility of occurrence exists during the time period of interest
Likely –more likely than not during the time period of interest
Certain – nearly certain in the time period of interest

Step 3: Identify the risk-mitigating controls that already exist. For each identified risk, actions can be taken to reduce that risk's probability and/or impact. First, any existing external requirements or standards that are applicable to address the risk should be identified. Next, identify any existing DOE directives that address the risk. These steps identify existing controls.

Step 4: If unacceptable risks remain, identify additional controls. In this step, the remaining risks in Step 3 are considered and each one is either accepted (i.e., the risk level does not warrant further action) or mitigated by making a different decision or developing an additional control. Additional controls can include things like a mandatory process, a required report, or a specified DOE approval.