INL/CON-08-14446
PREPRINT

Achieving the Benefits of Safeguards by Design

49th Annual Meeting: Institute of Nuclear Materials Management

Trond Bjornard
Robert Bean
David Hebditch
Bruce Meppen
Scott DeMuth
Michael Ehinger
Jim Morgan
John Hockert

July 2008

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

ACHIEVING THE BENEFITS OF SAFEGUARDS BY DESIGN

Trond Bjornard, Robert Bean, David Hebditch, Bruce Meppen
Idaho National Laboratory
2525 N. Fremont Ave., Idaho Falls, ID 83415

Scott DeMuth
Los Alamos National Laboratory
P.O. Box 1663, Los Alamos, NM 87545

Michael Ehinger, Jim Morgan*
Oak Ridge National Laboratory
P.O. Box 2008, Oak Ridge, TN 37831

John Hockert
XE Corporation
P.O. Box 90818, Albuquerque, NM 87199-0818

ABSTRACT

The overarching driver for developing a formalized process to achieve safeguards by design is to support the global growth of nuclear power while reducing 'nuclear security' risks. This paper discusses an institutional approach to the design process for a nuclear facility, such that nonproliferation, international safeguards, and U.S. national safeguards and security are part of that design process. In the United States the need exists to develop a simple, concise, formalized, and integrated approach for incorporating international safeguards and other non-proliferation considerations into the facility design process. An effective and efficient design process is one which clearly defines the functional requirements at the beginning of the project and provides for the execution of the project to achieve a reasonable balance among competing objectives in a cost effective manner. Safeguards by Design is defined as "the integration of international and national safeguards, physical security and non-proliferation features as full and equal partners in the design process of a nuclear energy system or facility," [1] with the objective to achieve facilities that are intrinsically more robust while being less expensive to safeguard and protect. This Safeguards by Design process has been developed such that it:

- Provides improved safeguards, security, and stronger proliferation barriers, while reducing the life cycle costs to the operator and regulatory agencies,
- Can be translated to any international context as a model for nuclear facility design,
- Fosters a culture change to ensure the treatment of 'nuclear security' considerations as "full and equal" partners in the design process,
- Provides a useful tool for the project manager responsible for the design, construction, and start-up of nuclear facilities, and

* Contractor with Oak Ridge National Laboratory

49th Annual Meeting: Institute of Nuclear Materials Management. Nashville, TN. July 13th-17th, 2008.

- Addresses the key integration activities necessary to efficiently incorporate International Atomic Energy Agency safeguards into the design of nuclear facilities.

This paper describes the work that has been completed in the development of a Safeguards by Design process for a project, illustrated by flow diagrams based upon the project phases described in U.S. Department of Energy Order 413.3A, *Program and Project Management for the Acquisition of Capital Assets*. The institutionalization of the Safeguards by Design process directly supports the goals of the Next Generation Safeguards Initiative [2] and also aligns with goals and objectives of the International Atomic Energy Agency. Other benefits from institutionalizing this Safeguards by Design process are discussed within this paper.

INTRODUCTION

In the development of a process for Safeguards by Design (SBD), the example of a U.S. Department of Energy (DOE) nuclear facility was selected for evaluation during the design, construction, and start-up phases. The basic approach developed is expected to be applicable to nuclear facilities regardless of the regulations or directives governing their design, construction, and start-up. The guiding document for the design, construction and start-up of a large nuclear facility by the DOE is *Program and Project Management for the Acquisition of Capital Assets*, DOE Order 413.3A. One of the primary goals of this order is:

> *To provide the Department of Energy (DOE), including the National Nuclear Security Administration, with the project management direction for the acquisition of capital assets with the goal of delivering projects on schedule, within budget, and fully capable of meeting mission performance, safeguards and security, safety and health standards.* [3]

The DOE Acquisition Management System establishes principles and gated project management processes to translate user needs and technological opportunities into reliable and sustainable facilities, systems, and assets that achieve a required mission capability. The system is organized by project phases, which represent a logical maturing of broadly stated mission needs into well-defined requirements resulting in operationally effective, suitable, and affordable facilities, systems and products.

Figure 1 illustrates a high level perspective of the typical implementation of the DOE Acquisition Management System for large, complex projects. This system utilizes four major phases for guiding the development and execution of a project:

- Initiation Phase: pre-conceptual planning activities focus on the Program's strategic goals and objectives,
- Definition Phase: alternative concepts, based on user requirements, risks, costs, and other constraints, are analyzed to develop a recommended alternative,
- Execution Phase: initial design concepts and the preliminary design are developed into detailed and final designs and plans, and
- Transition/Closeout Phase: construction, final testing, inspection, and documentation are completed, and the project is prepared for operation.

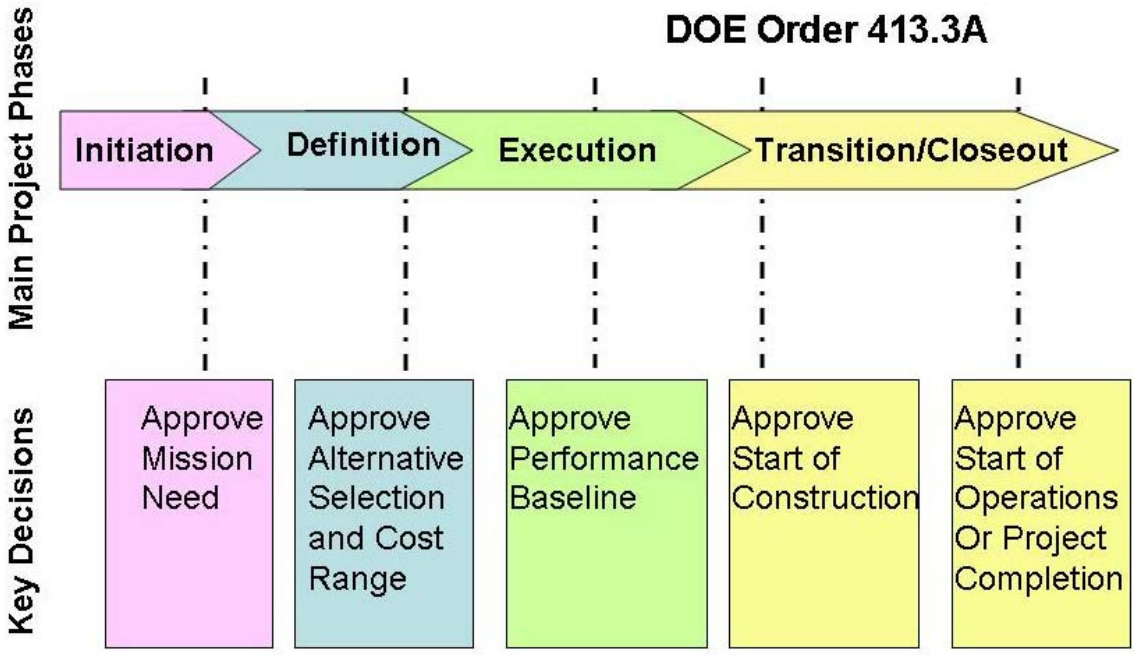

Figure 1. Typical Project Under the DOE Acquisition Management System

The amount of time between the phases will vary. Additional descriptions and information regarding these decisions can be found in DOE O 413.3A. In March 2008, DOE issued DOE-STD-1189-2008, [4] *DOE Standard for the Integration of Safety Into the Design Process*. The purpose of this new standard is to define a design process that ensures that safety is designed into the facility, in full integration with the remainder of the project. This standard contains some excellent new requirements, and was therefore chosen as a possible model for approaching the task of integrating international safeguards, together with national safeguards and security, into the design process.

INSTITUTIONALIZING THE SAFEGUARDS BY DESIGN PROCESS

The main objective of the Institutionalizing Safeguards by Design project is to develop and institutionalize a formalized, clear, simple process to guide the project team in the integration of nonproliferation, safeguards, and security into the design, construction, readiness review, and start-up of nuclear facilities that:

- Requires the early creation of the Safeguards By Design (SBD) team with clearly defined roles and responsibilities,
- Focuses on early identification of intrinsic design features that enhance safeguards, security, or proliferation barriers, or that facilitate the implementation of extrinsic safeguards, security, or nonproliferation measures,
- Requires the use of life-cycle cost analysis as a key criterion for capital expenditure decisions between intrinsic (early) and extrinsic (later) design alternatives, and
- Utilizes “systems engineering” processes to develop the optimum integration of operation, safety, safeguardability, protectability and nonproliferation into the facility design.

Figure 2 provides a simplified illustration of the activities that are performed during the initiation phase of the project that culminates in the approval of mission need.

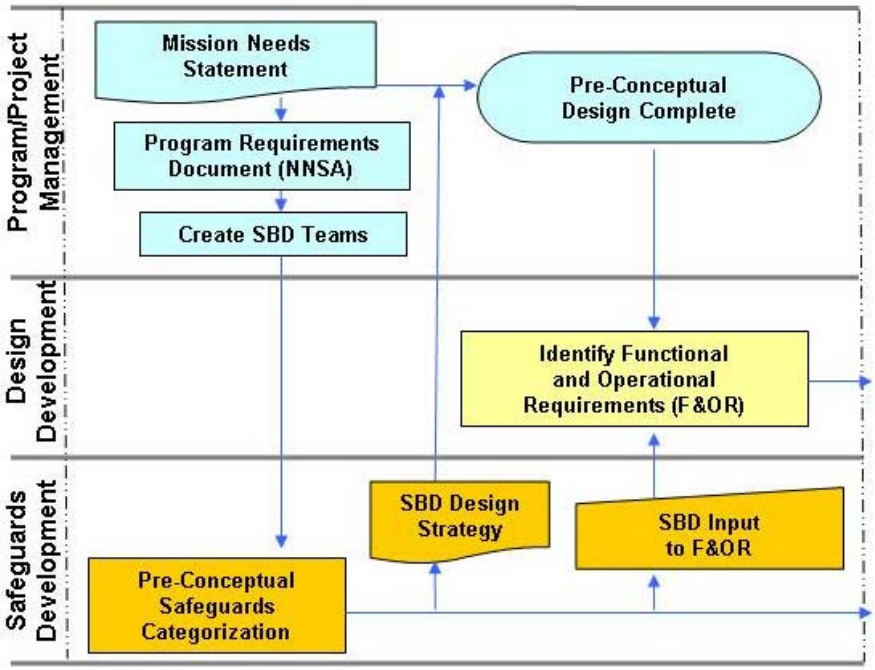

Figure 2. Initiation Phase Activities

The creation of the SBD team at the beginning of the project is a key fundamental step of the SBD process. This step is where the project manager establishes the Safeguards by Design team to support the project team in ensuring the integration of safeguards, security, and proliferation barriers into the design process, and to manage the preparation of relevant deliverables required to support each critical decision. The SBD Design Strategy is a tool to guide project design and SBD documentation development planning, and to provide approving authorities sufficient information upon which to base decisions. It provides a single, integrated compilation of the SBD policies, philosophies, major requirements, and goals for the project. This strategy will be revised and updated as the project matures. The SBD Design Strategy is structured to evolve into the information source needed for revising the Site Safeguards and Security Plan and the Nuclear Material Control and Accountability Plan. For National Nuclear Security Administration (NNSA) projects, a Program Requirements Document (PRD), which defines the ultimate goals the project must satisfy, is also prepared. The PRD is a document intermediate between the high level Mission Needs Statement and the more detailed Functional and Operational Requirements (F&OR). The SBD team identifies the high level requirements that must be included with the programmatic requirements that the facility must meet. For a successful project, a complete and clear statement of Functional and Operational Requirements must be generated and analyzed for iterative discussion among and approval by project disciplines and stakeholders. Completely analogous to other disciplines, including safety-in-design, the SBD team identifies those high level requirements that must be met in order to achieve the desired performance. Note that the F&OR document captures the necessary requirements and constraints, but normally does not prescribe in detail *how* those needs are to be met. The Design Criteria are criteria used to examine how well the F&OR are being met by the current evolution of the process and facility design.

Figure 3 provides a simplified illustration of activities that are performed during the definition phase of the project that culminates in the approval of alternatives selection. For clarity, the term 'safeguards' is used in this paper to encompass national safeguards, international safeguards, nonproliferation considerations, and physical security.

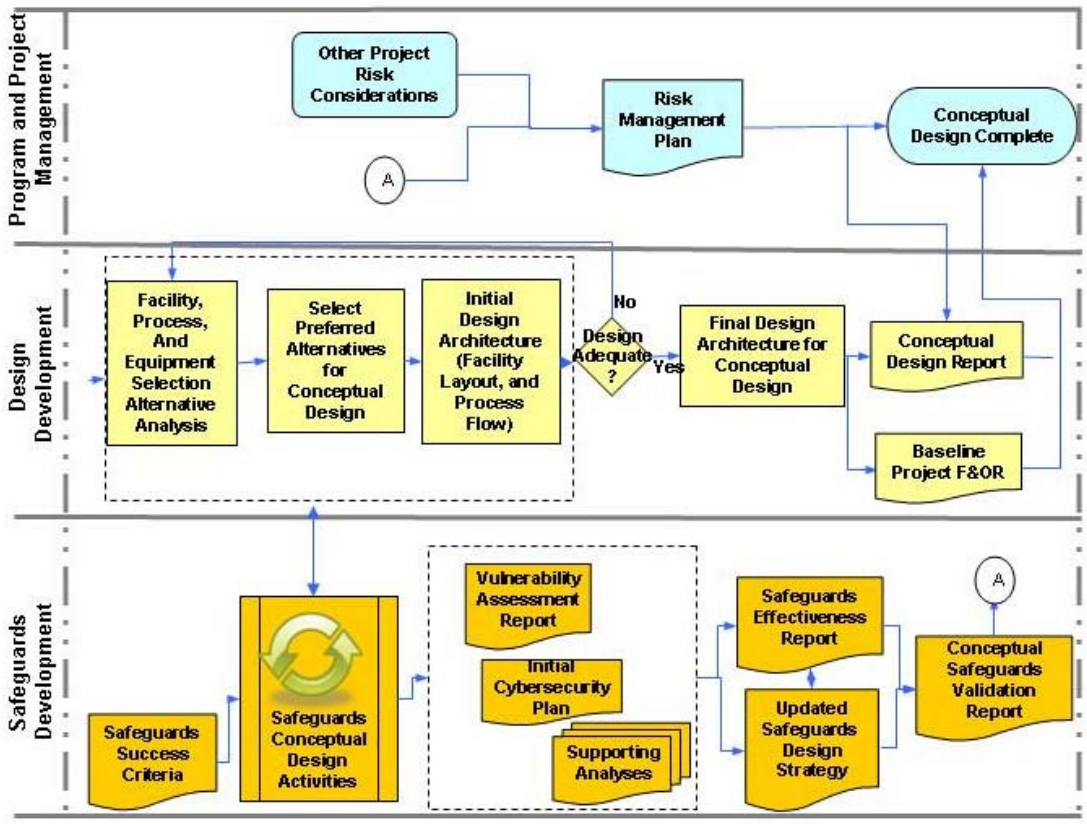

Figure 3. Definition Phase Activities

During the definition phase, the safeguards and security related conceptual design activities are performed and integrated with the conceptual design of the facility. The relevant Design Criteria test the requirements for performing the conceptual design activities. Integration of Safeguards by Design must meet safeguards and security guiding principles, analogous to how integration of safety into the design process must meet the safety design guiding principles provided within DOE-STD-1189-2008. This entails identifying and evaluating alternative facility layout and processing configurations to best meet safeguards and security requirements. Systems engineering is used in this phase, as well as the subsequent preliminary and final design phases of the project. "Systems engineering is a process that progresses through the establishment of functions and requirements, performance of functional analyses, the identification and evaluation of alternatives, the selection of a preferred alternative, and validation of the preferred alternative. The process ends with verification that the need is met, including interfaces, fit, and completeness." [5] Nonproliferation, safeguards (to include international and national considerations), and security requirements and associated functions serve as input to the overall systems that satisfy the project requirements. As the design progresses, changes and updates will be shared with the Safeguards by Design team. The SBD team will then cycle through their design analysis. Facility and system designs or updates to mitigate risks are developed. The outcome is analyzed (Vulnerability Assessments, exercises, etc.) and assessed versus the requirements and

criteria. The SBD team then optimizes the integration of the design, requirements, and criteria. This loop is performed as necessary until the SBD team is satisfied with the outcome, and then the design cycle passes back to the overall project team. Additional work will be required in the future to identify, and develop where necessary, the formal requirements, design criteria, and evaluation tools for incorporating proliferation barriers into the design.

It is during this SBD design activity and the earlier examination of alternative facility layout and process configurations, where the greatest opportunities for identifying and incorporating intrinsic features for safeguardability, protectability and proliferation barriers into the facility design exist. Life cycle cost analysis should be utilized to balance tradeoffs between early (intrinsic) capital costs and later (extrinsic) operating costs, which are incurred by both the operator and the regulatory agencies. The following reports are developed during this definition phase of the project and are updated as necessary as the project design is performed:

- Vulnerability Assessment Report,
- Cybersecurity Plan,
- Safeguards Effectiveness Report,
- Updated Safeguards Design Strategy, and
- Conceptual Safeguards Validation Report

The Safeguards Validation Reports are prepared by DOE at key decision points including completion of conceptual, preliminary, and final design activities. They document the DOE reviews of the Safeguards Effectiveness Reports and are prerequisites for moving from the definition phase to and through the execution phase. The DOE reviews the Safeguards Effectiveness Reports against the Safeguards Design Strategy and documents the reviews in the validation report to confirm that the Safeguards positions adopted during conceptual, preliminary, and final design will meet the defined requirements and success criteria, and constitute appropriately conservative bases to proceed.

The primary activities performed in the definition phase, as highlighted in Figure 3, are repeated in the execution phase in order to proceed from the development of the preliminary design to the completion of the final design. The SBD design team cycles through their design analysis as the design progresses. Changes and updates are shared by the SBD team and the design is updated to ensure the requirements contained in the Safeguards Design Criteria are being met. In addition to the Final Design Report, the Final Safeguards Validation report is developed to document that the final design meets the requirements of the Safeguards Design Criteria.

Figure 4 highlights the high level activities and documentation created to complete the Construction, Transition, Start-up, and Closeout of the project.

INTERACTION WITH THE INTERNATIONAL ATOMIC ENERGY AGENCY

In developing the SBD process, the potential for future application of International Atomic Energy Agency (IAEA) safeguards was reviewed. Intrinsic features that are necessary to allow proper IAEA verification must be considered and included, as necessary, early in the design process to avoid costly redesign and retrofit efforts. Early notification to the IAEA to initiate the international process is crucial. Additionally, for Nuclear Weapons States, such as the United States, determination of whether to place the facility on the Eligible Facilities List must occur early to permit the rest of the processes to proceed in a timely fashion.

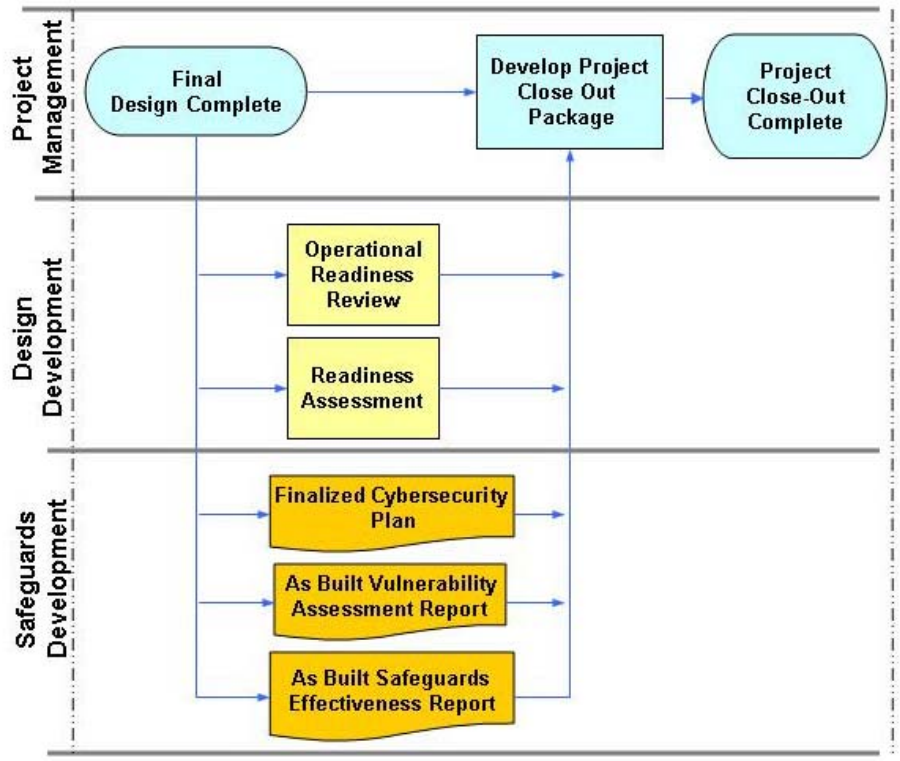

Figure 4. Transition/Closeout Phase

The IAEA involvement currently begins in earnest with the preparation and submittal of the Design Information Questionnaire (DIQ). Preparation of the DIQ requires that a minimal amount of design has been completed; thus, this action is required immediately after the completion of the conceptual design phase. Transmittal of the DIQ to the IAEA requires coordination among the design team, national regulatory agencies, (e.g. DOE) and state level organizations (e.g. U.S. State Department). The Facility Attachment is a negotiated document between the IAEA and the state regarding the features (intrinsic and extrinsic) that will be incorporated into the facility design to accommodate the IAEA verification activities during construction and operation. It is vital that the impact of the facility attachment on the physical plant (lab space, conduits, footprint of hot cells, etc.) be agreed upon in a timely fashion to allow the detailed design efforts to proceed. As the design effort progresses to the final details, so also does the input from the IAEA facility attachment. As the facility design is optimized and reviewed for final approval, the IAEA input is finalized and incorporated into the overall design.

As construction begins, Design Information Verification activities will be performed by the IAEA through all stages of construction and will continue as required during operation. As the facility is built and prepared for operation, the equipment will be delivered and installed (including testing, tamper-proofing, initial calibrations, etc.).

CONCLUSION

The reemergence of nuclear power and subsequent growth in all facets of the nuclear fuel cycle requires that safeguards be applied in a most effective and efficient manner. Therefore, it can readily be seen that a significant need exists to develop an institutional approach for incorporating Safeguards by Design into the design of nuclear facilities. The development of an SBD process that requires the establishment of the SBD team by the project manager is a key ingredient of the institutional approach discussed in this paper. This early, integrated design focus can produce more robust facilities and systems, while reducing the life-cycle operating costs to both the operator and the regulatory agencies. Doing so is therefore warranted and should be enthusiastically embraced by project teams. Additionally, the SBD process adds consideration of proliferation barriers into the design process, including the application of international safeguards.

Many of the individual elements of the SBD process are already formalized and have been utilized in past and current projects. However, this paper proposes a process for their tight integration into a single comprehensive framework, with the addition of some new elements and activities to meet new needs. The new process has a major objective to fully exploit the efficacy and cost savings potential of the early introduction of beneficial intrinsic design features. The greatest potential to capitalize on intrinsic features occurs early in the design process, during the conceptual design phase. This is when the objectives are to identify design candidates and their risk and cost ranges, recommend a preferred design approach, and establish the general facility layout. This places the greatest burden for successful execution in the earliest stages of the project. For success, the SBD project team must be involved from day one of the project.

The SBD process discussed in this paper directly supports goals of the Next Generation Safeguards Initiative, as well as goals and objectives of the IAEA. This process supports the development of a "Safeguards Design Basis" similar to the "Safety Design Basis" utilized at nuclear facilities in the United States. The primary objective is the design of nuclear facilities with high safeguardability. Potential obstacles to successful SBD are recognized; however, as we proceed to formalize and institutionalize the SBD process, we will remove or mitigate the obstacles. All relevant parties should work together to develop a process that ensures the early involvement of the SBD team in the design of facilities in order to maximize efficiency and effectiveness throughout the lifecycle of the facility.

REFERENCES

1. Bjornard, T. and Pasamehmetoglu, K. SESAME - Advanced Modeling and Simulation Applied to Nuclear Nonproliferation and Safeguards. Institute of Nuclear Materials Management 47th Annual Meeting, Nashville, Tennessee, June 2006.
2. International Safeguards: Challenges and Opportunities for the 21st Century. United States Department of Energy, Nuclear Security Administration, NA-24, October 2007
3. Program and Project Management for the Acquisition of Capital Projects, DOE O 413.3A. United States Department of Energy, July 27, 2006.
4. Integration of Safety into the Design Process, DOE-STD-1189-2008. United States Department of Energy, March, 2008
5. Program and Project Management, Systems Engineering and Interface Management. United States Department of Energy Office of Management, Budget, and Evaluation, June 2003.