March 2001

Inside Oversight

Office of Independent Oversight and Performance Assurance
U.S. Department of Energy

Inside this Edition

For More Information: Visit Our Web Site at:
http://tis.eh.doe.gov/iopa

Reviews Focus on DOE Response to Wildland Fires

Major wildland fires during the summer of 2000 focused national attention on Federal fire safety and emergency management. Because of the magnitude of this ongoing threat—wildland fires burn about 3.6 million acres of land in the United States annually—the Secretary of Energy directed a series of reviews to improve the overall response capabilities of the Department of Energy (DOE).

The first of these reviews was conducted in the fall of 2000 by the Offices of Independent Oversight and Performance Assurance (OA), Security and Emergency Operations (SO), and Environment, Safety and Health (EH). Focusing on several higher-risk sites, the review team assessed the sites' ability to prevent and respond to wildland fires and recommended both site-specific and DOE-wide improvements. The sites all had plans, procedures, and resources in place and demonstrated solid basic capabilities. The overall effectiveness of these fire protection programs is reflected in DOE's successful record to date in protecting facilities from wildland fires. The team also identified several opportunities for strengthening these programs.

The details of the initial joint review were reported in *Initial Joint Review of Wildland Fire Safety at DOE Sites* (December 2000), which is available on the OA web site under "Reports."

Cerro Grande Wildland Fire

The conclusions of the wildland fire safety review parallel a series of continuing, DOE-wide weaknesses previously noted by the Office of Emergency Management Oversight (OA-30). In late 1999, OA-30 began a series of follow-up appraisals to assess the progress made since the DOE-wide emergency management review conducted in early 1998. The OA-30 efforts that began in 1999 are reported in *Follow-up Review of Emergency Management Programs in the Department of Energy Complex*, (May 2000), which is also available on the OA-30 web site. One of the most significant continuing weaknesses identified during both reviews was the lack of compre-

(Continued on Page 4)

Three Areas Are Key to Safeguards and Security Improvements for 2001

Recent OA inspections have identified three safeguards and security areas, excluding cyber security and emergency management, that deserve the special attention of DOE field managers, program offices, and policy makers in the upcoming year: material control and accountability (MC&A), the Site Safeguards and Security Planning (SSSP) process, and safeguards and security research and analysis (R&A) issues.

Material Control and Accountability

Irradiated Nuclear Fuel

Forty-one foreign countries have used nuclear fuel from the United States to power their research reactors. Over the next several years, much of this irradiated material will be returned to DOE to be stored. DOE nuclear safeguards policy needs to be developed further in order to deal with the challenges posed by this material. These challenges include identifying points in the material's life cycle where safeguards actions (including measurements) are needed and providing consistency in the protection approach employed by DOE sites to ensure effective protection for this material.

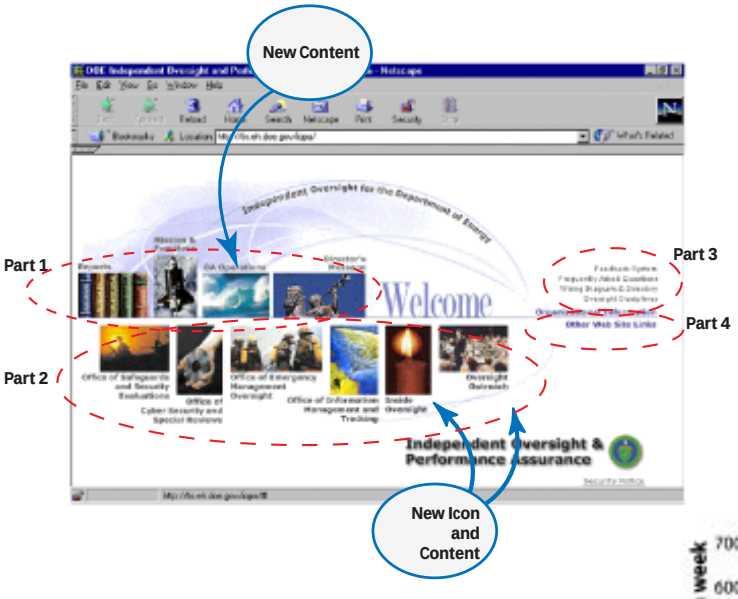
Responding to these challenges will require several specific actions. Steps should be taken to analyze the increased potential for theft or diversion of this material and to devise appropriate, cost-effective responses. Valid measurements should be required. If statistical sampling is permitted, the sampling method should be based on a technically valid sample to ensure that fuel rods cannot be diverted

(Continued on Page 3)

Redesigned Home Page Honored in February

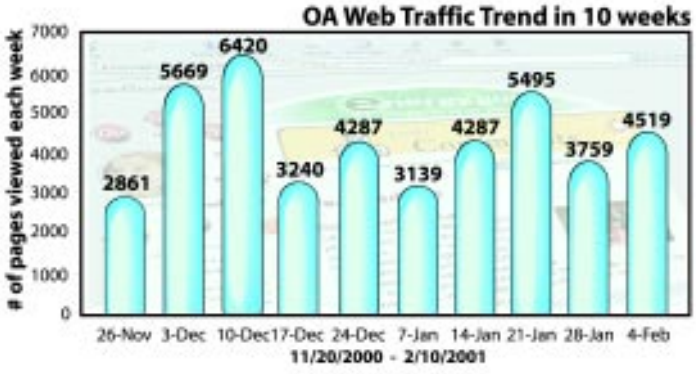
On February 1, OA's newly redesigned and updated home page (http://tis.eh.doe.gov/iopa/index.html) was re-launched and celebrated as the "featured site of the month" for February on the Department's new *energy.gov* web page "Community" section.

Karen Hsing, OA's webmaster, characterizes the new design of the OA home page by noting that it is divided into four principal areas as shown in the figure below. Part 1 provides general OA information, such as OA's missions, weekly highlights, and deliverables. Part 2 links visitors to each OA subordinate office and provides more specific information, such as the program plan and the activities of each office. Part 3 includes the OA organizational chart and feedback system, and Part 4 points to related DOE web sites.



Features of the redesigned page include new icons for the current "Inside Oversight" and for "Oversight Outreach." Also added under the "OA Operations" icon is a current schedule (for the calendar year) of OA inspections activities.

Beyond updating and maintaining OA's web pages, Karen also analyzes web traffic patterns for OA managers, providing relevant insights into the interests of electronic visitors to Independent Oversight information. The figure below depicts the volume of web traffic over the past ten weeks. The most visited area is the Reports section, with the recent OA-30 Wildfire report of particular interest (see article on Page 1).



The Department's new web page, *energy.gov*, which replaced the old DOE site, *doe.gov*, featured the OA home page as "featured site of the month" for February 2001, in recognition of OA's broad-based outreach activities into the Native American community. The Departmental site featuring OA at http://www.energy.gov/community/index.html is shown below.

OA's newest office, OA-40, the Office of Information Management and Tracking, is responsible for providing a complete spectrum of information and knowledge management support to all OA offices. Karen is always looking for comments on how to make our electronic presence more user-friendly and useful to all the communities we serve. She can be reached through the feedback section on the OA home page, at karen.hsing@hq.doe.gov, or at 301-903-1419.

...Security Improvements for 2001 *(continued from Page 1)*

without detection. DOE should measure the material upon receipt and should develop plans to address potential discrepancies. DOE Headquarters approval should be required if timely measurements are not possible (e.g., because of the volume of returns or lack of equipment). Finally, DOE should not accept other countries' statements of continuity of knowledge without formal risk acceptance by senior DOE management and concurrence by other appropriate government agencies (e.g., Department of State and the Central Intelligence Agency).

Other MC&A Program Enhancements

There are a number of other potential MC&A program enhancements that deserve the attention of senior DOE managers. These include:

- Establishing more effective requirements for prompt loss detection
- Establishing a comprehensive scrap control program
- Eliminating the requirement for physical inventory confirmation measurements
- Requiring verification measurement for all non-tamper-indicating items at the time of physical inventory
- Adopting Nuclear Regulatory Commission MC&A definitions (where appropriate)
- Implementing a requirement for item monitoring that provides a quantitative loss detection program
- Requiring a periodic estimation of error variances for bulk measurement systems and sampling techniques
- Requiring a consistent approach to bias correction
- Requiring reconciliation of physical inventories within a specified time.

In the longer term, DOE line management and policy elements should work together to develop an MC&A order with clear performance objectives, a format and content guide for MC&A plans, acceptance criteria for contractor MC&A plans, and a defined MC&A plan approval process. Furthermore, DOE should establish a clear schedule with milestones for this effort.

Calibrating Equipment for Measuring Irradiated Fuel

The Site Safeguards and Security Plan (SSSP) Process

The SSSP concept of analyzing vulnerabilities, prioritizing problems and solutions, implementing those solutions on a realistic schedule, and obtaining management agreement (and acceptance of residual risks) reflects a well-established and time-proven approach to managing risk. Unfortunately, recent practice in DOE has tended to emphasize the process rather than the product, creating a situation where formalisms are fulfilled with insufficient regard for substance. Last year, DOE initiated a new approach to the development of SSSPs designed to ensure that all interested parties are fully involved in the SSSP development process. This new approach has shown sufficient promise to warrant continued support. Additional effort, however, is needed in the area of threat definition, particularly in the development of protocols for the effective simulation of adversary capabilities in computer models and performance tests. For example, although DOE program and policy elements have expended considerable time and resources during the last year to establish a standard adversary capabilities list for the Department, this effort foundered over fundamental disagreements concerning both the weapons that should be included on the list, and the methods through which these weapons would be represented in test and simulations. Since threat characteristics define protection strategies, the lack of a standard adversary capabilities list has the potential to either (1) leave DOE sites unprepared to deal with credible threats, or (2) force DOE sites to needlessly expend resources in responding to unrealistic or exaggerated threats.

Centralizing Safeguards and Security Research and Analysis

To better define threat characteristics identified in DOE's conduct of safeguards and security research and analysis, DOE should strengthen its central clearinghouse capabilities. Currently, some safeguards and security R&A efforts are funded directly by an Office of Security and Emergency Operations' branch, while others are supported by various Headquarters program elements. Field managers sometimes initiate typically smaller-scale R&A efforts, such as the excellent study of radio jamming capabilities conducted by Lawrence Livermore National Laboratory in 1999. Up to a point, this is the logical reflection of the differing needs of these various organizational elements. However, it has become increasingly clear that in some instances this approach has led to unnecessary duplication of effort, and, in other situations, significant R&A requirements have gone unfulfilled. For example, the Department has expended significant resources in recent years to counter a so-called "magic bullet," a heavy rifle round that was reputed to cause instant one shot kills on security response vehicles. This expenditure took place even though comprehensive information to refute this claim existed within the DoD. A central clearinghouse function could assemble information from available sources, support research efforts when necessary information is lacking, and distribute the information to all interested parties. This could be accomplished either by a joint effort on the part of SO and the program offices, or by adding this task to the mission of the existing SO research and development office. ■

Upcoming Oversight Activities

Composite Adversary Team Training
Purpose: Train Composite Adversary Team (CAT) members for their mission of acting as an adversary force during inspection activities.
Date: March 19-23, 2001
Contact: Barbara Stone, 301-903-5895

Lawrence Livermore National Laboratory Cyber Security Review
Purpose: Review cyber security programs and processes; will include external network security assessment.
Date: March 19-29, 2001
Contact: Brad Peterson, 301-903-5781

Strategic Petroleum Reserve Office Program Review
Purpose: Evaluate the integration of safeguards and security, cyber security, and emergency management programs.
Date: April 2-11, 2001
Contact: Chuck Lewis, 301-903-1554

Argonne National Laboratory – West Follow-up Review
Purpose: Follow up on status of previous issues in safeguards and security and in cyber security.
Date: April 30-May 11, 2001
Contact: Barbara Stone, 301-903-5895

Los Alamos National Laboratory Inspection
Purpose: Evaluate safeguards and security and cyber security programs.
Date: June 4-15, 2001
Contact: Barbara Stone, 301-903-5895

Cyber Security Needs a Programmatic Approach

In general, cyber security programs throughout DOE have improved over the last two years. At most sites, cyber security is a management priority. But in the world of cyber security, the question to ask is, "What are you doing today to address the current cyber security threat?" An effective cyber security program has to keep pace with the new vulnerabilities and intruder techniques that emerge every day. To maintain this focus, the Office of Cyber Security and Special Reviews (OA-20) evaluates not only the effectiveness of a site's current cyber security measures, but also the processes the site uses to sustain effective cyber security. These include:

- A risk assessment and management process
- Defense in depth – network configuration management and perimeter-, server-, and host-level security
- A comprehensive intrusion detection strategy
- Automated scanning to routinely identify and eliminate vulnerabilities
- Site policies and procedures consistent with DOE and Federal requirements
- Personnel knowledge of cyber security roles, responsibilities, and authorities.

Weakness in these areas lead to breakdowns in cyber security. Improvements require skillful use of staff, tools, and other limited resources, as well as an aggressive, persistent effort to keep up with new challenges.

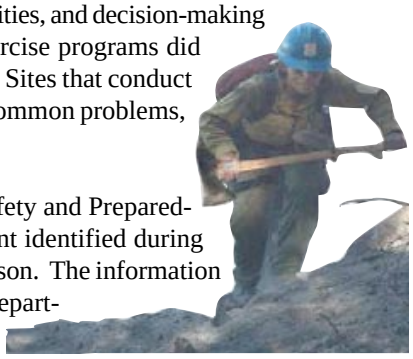
The Office of the Chief Information Officer (SO-30) has taken some significant actions this year to help DOE sites improve their cyber security programs. SO-30 has funded a number of site initiatives, and has also procured complex-wide licenses for commercial vulnerability scanning software and other cyber security tools in order to promote sites' use of these tools.

But having and using the right tools does not always solve the problem—systematic processes are needed to ensure that the tools are implemented effectively. For example, routine scanning for vulnerabilities is useful only if the site uses the results to correct the weaknesses, validate effectiveness, and hold personnel accountable for actions. OA-20 cyber security assessments will continue to focus on these processes, as well as on extensive performance testing. ■

...Wildland Fires *(continued from Page 1)*

hensive hazards assessments that accurately reflect site hazards and operations and the full range of potential initiating events. Sites need this information to establish a technical basis for wildland fire mitigation initiatives, such as prescribed burning, and to formally evaluate all of the potential impacts (e.g., flame, smoke, hazardous material release, fire suppression activities) of a wildland fire. Both reviews also noted that emergency management roles, responsibilities, and decision-making authorities were often unclear, and that training, drill, and exercise programs did not always ensure the proficiency of all emergency responders. Sites that conduct well-designed exercises are also better able to identify and fix common problems, such as communicating with multiple response organizations.

The Secretary of Energy and the DOE Commission on Fire Safety and Preparedness have recommended that the opportunities for improvement identified during the wildland fire review be implemented before the next fire season. The information from the review is also being used to plan a comprehensive, Department-wide fire safety review, which is scheduled for completion by the end of FY 2001. ■



Firefighter Responding to Cerro Grande Fire

Solicitation of Comments, Questions, and Suggestions

OA welcomes your thoughts about our newsletter. Please send or phone comments, questions, or suggestions to:

Glenn S. Podonsky, Director
Office of Independent Oversight and Performance Assurance
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874
301-903-3777

e-mail: Glenn.Podonsky@eh.doe.gov

This newsletter can be found on the OA web site at http://tis.eh.doe.gov/iopa.