February 2004

Inside Oversight

Office of Ind

"Inside Oversight" becomes "Inside SSA"

Inside this Edition

"Inside Oversight" transitions to "Inside SSA" The Office of Security and Safety Performance Assurance

New Office To Coordinate Policy and Oversight Roles

On December 4, 2003, Energy Secretary Spencer Abraham announced the establishment of the new Office of Security and Safety Performance Assurance (SSA), containing the Office of Security (SO) and the Office of Independent Oversight and Performance Assurance (OA), to better coordinate the roles of independent oversight and security policy organizations within the Department. The new office will be responsible for the development and implementation of the Department's safeguards and security policies and will report directly to the Secretary. The merging of SO and OA under one office will provide for better integration and collaboration among the security and oversight communities and will generate a synergy that will facilitate communication and be more responsive to the needs of the Headquarters and field organizations. The new office also will work closely with the National Nuclear Security Administration (NNSA), through the Office of Safeguards and Security Policy, to ensure that NNSA security policies emulate the intent of Departmental security policies, and through OA to continue the independent oversight of NNSA's safeguards and security, cyber security, emergency management, and environment, safety, and health programs.

Glenn Podonsky, formerly Director of the Office of Independent Oversight and Performance Assurance (OA), has been named Director of SSA. Marshall Combs, formerly Deputy Director of the Office of Security (SO), will serve as Director, Office of Security. Michael Kilpatrick, formerly the Deputy Director of OA, will serve as Director of OA. Both organizations report to the new Office of Security and Safety Performance Assurance. The offices will work together to facilitate an increased level of cooperation between SO and OA in support of the Department's protection programs.

As part of this transition, the publication "Inside Oversight" will become "Inside SSA" and will continue to reflect items of interest and common problems and solutions within OA, as well as areas relating to SO (e.g., the development and refinement of clear, effective safeguards and security policy and the development of tools and expertise to assist line managers in implementing effective safeguards and security programs). In this first edition, our theme will include topics that highlight areas of current collaboration between OA and SO, including development of additional guidance and implementation support related to the new design basis threat, the identification of policy and training that better fit the needs of the field, and the collaboration of the OA cyber security laboratories and the SO cyber forensic laboratory.

The creation of the new SSA office places added emphasis and focus on security during this period of uncertainty and our current war on terror, with the ultimate goal of providing unchallengeable levels of protection for the national security assets we hold in trust for our nation.

SSA: A Strategic Response to DOE Security Needs

The DOE, its managers, and its security professionals face the need to implement effective safeguards and security programs in an increasingly challenging threat environment. To address this challenge at the highest levels within DOE, the Secretary of Energy created the Office of Security and Safety Performance Assurance (SSA) to direct and coordinate the efforts of the Offices of Security (SO) and Independent Oversight and Performance Assurance (OA). Joining these two organizations under a single office is expected to improve security oversight activities, policies, training, and technological innovation, which in turn will better support security professionals in the field and improve DOE's safeguards and security programs.

SSA's immediate strategy to meet these expectations is to capitalize on the existing capabilities of both organizations and more closely coordinate their efforts in order to achieve prioritized safeguards and security program goals. Three areas of immediate focus are policy, technology, and professional development.

Policy Initiatives

SSA is coordinating several initiatives to help safeguards and security policy respond to the changing national security environment.

Streamlining Policy. The focus of this effort is to remove ambiguity in roles, responsibilities, and requirements; eliminate conflicting requirements; and incorporate recent updates to safeguards and security policy. The goal is to create sound policy that is responsive to national security needs and enables line management, through Headquarters and field organizations, to implement effective safeguards and security programs in a timely manner.

Coordinating Evaluation Results with Policy Development. SSA's process for coordinating OA field evaluation results with SO policy development efforts will help ensure that the DOE security community has a good understanding of policy and will promote development of clear, specific policy that achieves protection objectives and meets national security responsibilities.

Developing Criteria for Performance Assessment. Developing evaluation criteria for better assessing safeguards and security program performance will help identify deficient programs and poor practices by emphasizing effective performance rather than simply compliance with requirements. SSA expects to issue a revised order and seven manuals this year and to issue evaluation criteria in 2005.

Technology Initiatives

SSA will continue to champion the effective use of technology by field organizations to increase protection program efficiency. DOE's history of developing innovative security technologies, for use both internally by the Department and by other governmental and international agencies, has led to a well documented return on investment. SSA is committed to improving the deployment and use of security technologies within DOE and sharing technology development information throughout the DOE complex. Working with the national laboratories that do much of the developmental work, SSA will move aggressively to build on SO's technology development program to promote the most promising and most urgently needed technologies. SSA will emphasize technologies that foster a transition from administrative controls to engineered controls, thus diminishing the Department's reliance on increased manpower levels as the primary means to strengthen security. Also, through revitalized partnerships with line management, SSA will provide greater opportunities to effectively deploy emerging technology in security programs.

The new communication opportunities resulting from the SSA organization will allow the staff of OA to leverage the knowledge base of the SO technology development program to keep current with the latest security technology. In addition, SSA will explore ways to improve the lessons-learned program within the security community and, as a start, will ensure that innovative technologies and techniques that resolve common security problems are quickly shared.

Professional Development Initiatives

Because policies and technologies are only as effective as the people who implement them, SSA is committed to advancing the professional development of DOE security personnel. Increased pressures on field security staff's time and limited travel budgets have reduced their opportunities to take advantage of available training, and SSA is already taking steps to assist in this area. Further, SSA has resolved to continue to improve the Nonproliferation and National Security Institute (NNSI) to ensure that training is responsive to the needs of the DOE community while maintaining its reputation as a national training center. For example, SSA is accelerating the development of new vulnerability assessment courses based on evolving policy, threat, technology, and evaluation tools, in order to increase line management's assurance that protection systems and strategies meet the design basis threat. Additionally, the NNSI is emphasizing distance learning programs and mobile training teams to make training in evolving security policy, strategies, and technologies more accessible to its customers in the field.

SSA will also improve training opportunities by expanding the OA augmentee inspector program, which allows qualified DOE field staff and managers to participate in inspections of other DOE sites. By participating, augmentees can gain insights into OA inspection protocols, site self-assessment and continuous improvement processes, and effective security solutions. This program can be a cost-effective training opportunity for sites, because SSA will continue to pay augmentees' travel costs and there is no charge for participation.

(Continued on Page 3)

Meeting the Threat

SSA's initial efforts are focusing first on addressing the most immediate security challenge – effectively and efficiently implementing protection programs that fully respond to the May 2003 design basis threat policy (see related article on page 4). To meet DOE's goal of fully implementing this policy by the end of 2006, SSA is helping DOE address programmatic and technical uncertainties and establish cooperation and useful dialog between managers and security professionals at all levels.

SSA, through the initiatives described above and through its organizational focus, will be able to meet the Secretary's expectations by directing and coordinating the efforts of SO and OA in evolving security oversight, policy, technology development, and training programs. The partnership of SSA and other DOE line management elements will assist the Department in continuing to proactively address changing threats and national security needs in its evolving security programs.

Coordination Across SSA To Improve Cyber Security

An important priority for the new Office of Security and Safety Performance Assurance (SSA) is to strengthen cyber security across the Department. SSA has two organizations focused on this important task, one within the Office of Independent Oversight and Performance Assurance (OA) and one within the Office of Security (SO). The Office of Cyber Security and Special Reviews (OA-20) conducts assessments of classified and unclassified cyber security programs and provides independent feedback to line management on the effectiveness of implementation. The Office of Safeguards and Security Policy (SO-11) provides forensics support for the Department's unauthorized-disclosure program and supports requests for technical assistance from DOE sites on cyber security issues. While these two offices support different missions, the formation of SSA will allow them to leverage each other's expertise to improve the protection of information within the Department.

SO-11 carries out its missions through the Cyber Forensic Laboratory (CFL). Over the past few years, CFL activities have expanded beyond cyber forensics due to a growing number of requests to take full advantage of their technical expertise. In their technical assistance role, CFL specialists have conducted in-depth analyses of software tools to ensure that they perform as intended. In addition, the CFL has assisted various DOE facilities that needed confidential, independent assessments of how specific technologies would affect cyber security within their network environments. The CFL also can train onsite incident response teams to help them assure proper data handling in support of cyber forensics investigations.

In the same time period, OA-20 has been conducting more in-depth technical assessments in conjunction with classified and unclassified cyber security reviews. The OA Cyber Security Testing Network (CSTN), established to support these assessments, includes two remote penetration testing locations, go-kits for onsite assessments, and a cadre of technical experts. These resources provide for thorough technical assessments that give an accurate picture of the effectiveness of the site's current protection posture for information systems. As examples of advances being made, CSTN personnel have recently developed improvements for wireless testing and new remote testing techniques for evaluating automated blockers used by DOE sites.

As the SSA organization matures, OA and SO will be identifying specific areas where the CFL and CSTN can provide complementary services to the Department, while maintaining their different functions and their current relationships within the DOE complex. For example, during assessments OA-20 routinely identifies significant cyber security issues that DOE sites need to address. OA-20's recommendations on how sites may approach such issues can now be greatly enhanced through targeted referrals to the CFL for in-depth technical assistance. Additionally, OA-20 can provide feedback to the CFL on Departmental cyber security issues so that field personnel can get the help they need. Alternatively, the CFL can greatly assist OA-20 by providing input on the latest cyber security vulnerabilities that OA needs to consider during their technical assessments and by answering specific technical questions whenever necessary. The CFL and OA-20 will also collaborate on general cyber security issues to identify trends and the underlying root causes of cyber security weaknesses, in order to improve feedback and lessons learned to DOE sites and, ultimately, to improve protection of classified and unclassified networks.

These are some of the areas that SSA will be exploring over the next couple of months. SSA will continue to partner with the Office of the Chief Information Officer to ensure that the Department's cyber security program is the best in the government. Enhanced coordination between the CFL and CSTN will allow SSA to significantly benefit cyber security programs across the Department.

Upcoming Activities

Protective Force Special Review
Multiple Sites

Classified Program/SCIF Assessment
Multiple Sites

ES&H Review
Kansas City

Emergency Management Review
Brookhaven

Combined ES&H and Emergency Management Inspection
Hanford

DOE-SSA Safeguards and Security Seminar
March 10-11, 2004

U.S. - IAEA Additional Protocol Exercise
Los Alamos
Lawrence Livermore

DOE Safeguards and Security Special Interest Group Meeting

DOE Publishes New Design Basis Threat

The design basis threat (DBT) establishes a performance standard for protection system designs across the Department. On May 20, 2003, DOE published the first revision to the Department's DBT policy since 1999. The new DBT is based on the intelligence community's assessments of adversary characteristics, including the attacks inside the United States on September 11, 2001, and subsequent activities worldwide. The DBT describes adversaries, such as terrorists, criminals, and foreign intelligence agents, in terms of their tactics, equipment, level of training, level of motivation, and other characteristics to assist DOE analysts in evaluating specific threats. Even though the DBT is a DOE internal standard, it has been coordinated with the Department of Defense and the Nuclear Regulatory Commission to ensure that similar national security assets are provided equivalent protection, regardless of what agency has primary custody of an asset.

The 2003 DBT represents a departure from earlier DBTs in its basic structure. Previous DBTs specified a fixed number of adversaries for each adversary type, such as terrorists or criminals, regardless of the site's mission or assets. Graded protection was achieved by combining the results of an analysis of protection effectiveness with consequence values reflecting the degree of damage to the Department's interests that would result from adversary success. The new DBT, on the other hand, provides for a varying number of adversaries within each type, and the assets present at each site or facility determine the number of adversaries to be defended against. By including the consequence values implicitly within the size of the adversary group, protection effectiveness becomes the final basis of comparison among sites and the primary basis for evaluating sites' success in implementing DOE protection requirements.

At the same time, DOE has modified the formula for determining protection effectiveness. The previous formula, dating to the 1980s and reflecting the limitations of computer systems at that time, assumed that the protective force was dispatched at the last possible moment to intercept an adversary. Since today's analysts use personal computers that often exceed the capabilities of the mainframes of the mid-1980s, a new methodology has been developed that allows sites to take credit for the detection, assessment, and response functions that normally occur long before the "last minute" response previously assumed.

Together, these changes will allow DOE analysts to make more accurate assessments of site protection systems against the threats that have emerged over the past two years. As a result, sites will be able to design more cost-effective protection systems that provide better protection while minimizing the additional costs associated with the more modern threat.

Solicitation of Comments, Questions, and Suggestions

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

Glenn S. Podonsky, Director
Office of Security and Safety Performance Assurance
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1290
301-903-3777 or 202-586-4399

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

This newsletter can be found on the SSA web site at **http://www.ssa.doe.gov**