August 2000

Inside Oversight

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

Inside this Edition

Front Page

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

Composite Adversary Team Trains to Test Facility Security

Composite Adversary Team Members

For a week last April the sounds of gunfire, explosives, and maneuvering troops could be heard day and night at Area 27 on the Nevada Test Site. A terrorist attack? Well, not really. The military pursuing aliens escaping from Area 51? Nope. It was just the CAT – Independent Oversight's Composite Adversary Team – undergoing annual training to hone the skills its members will use during upcoming safeguards and security inspections of DOE facilities. Each year, specialists from the Office of Safeguards and Security Evaluations (OA-10), sometimes assisted by experts from the Department of Defense, plan and conduct a one-week training program aimed at teaching and improving the particular skills needed to perform the unique "black hat" mission of the CAT. For the third year in a row, the Nevada Operations Office and Nevada Test Site provided support facilities for the training program.

(Continued on Page 3)

Workshops to Share Lessons Learned in the Emergency Management Arena

As the recent fires near Los Alamos and Hanford clearly demonstrate, DOE sites need to be ready to respond to an emergency or natural disaster at any time. The Office of Emergency Management Oversight (OA-30) has an ongoing series of workshops designed to share lessons learned in the emergency management arena. These workshops focus on generic problems identified in the past three years of independent oversight inspections, such as weaknesses in hazard assessments and emergency action levels. They also provide information about OA-30 appraisal techniques, with emphasis on the "table-top exercises" that OA-30 uses to determine whether individuals thoroughly understand their responsibilities and can use their procedures and job aids in a postulated emergency situation.

The OA-30 workshops are a collaborative effort with DOE Headquarters, DOE field elements, and the DOE Office of Emergency Management (SO-40). They are intended to provide a forum, separate from the high-pressure and guarded atmosphere of an appraisal, where OA and the field can discuss problems and potential enhancements in depth with various levels of DOE and contractor management, from the Operations Office Manager to the working level emergency responder. In the past few months, OA-30 has conducted workshops at various DOE sites, including the Nevada Operations Office, the Oak Ridge Reservation, and Lawrence Livermore National Laboratory, as well as special sessions for DOE Headquarters personnel in the Office of Defense Programs and the Office of Environmental Management. Other sessions are scheduled. If you are interested in having OA-30 lead a workshop at your site, please contact the Director of OA-30, Chuck Lewis, at 301-903-1554.

Internet Messaging Systems May Lack Security

Messaging systems such as the ICQ and AOL Instant Messenger (AIM) systems have become a popular means of communicating over the Internet. These tools allow users to send and receive messages in real time over an employer's network connection. Most of these systems also allow e-mail messages to be sent and received, files to be transferred, and users to chat online with other users via their computers.

Messages, e-mails, files, and chat conversations on the messaging systems are all transferred across the Internet "as sent." Few of the systems allow for end-to-end encryption or other means of message protection/security. In addition, because of the nature of these systems and their accepted common usage, many users either forget or are unaware that no secure communication exists and often use the programs to send information that might normally be considered private or sensitive. That information is then vulnerable to capture and/or exploitation by unauthorized recipients.

Exploitable vulnerabilities associated with messaging systems can often increase when other services, such as Web servers, file transfer servers, and mail systems, are installed on a network. For example, there is an increased risk of IP address tracing on a network in which messaging systems are used. Network managers often install firewalls or other devices to conceal organizational address information on their networks. However, many messaging systems allow anyone communicating with a system user to trace and discover the user's true address on a network. Once the addresses are discovered, an intruder can use incoming probes and scans to map and exploit the network. If the various network services, such as file transfer servers, are poorly designed or misconfigured, the network is then subject to attack and exploitation by various viruses or Trojan horses. In some cases, poorly designed controls on file transfer servers can then be exploited to gain remote access to sensitive user files.

Poorly designed controls on file transfers can be exploited.

Message and file encryption can be applied to provide some measure of security for messaging systems. However, encryption cannot facilitate authentication to ensure the identity of authorized users. Many organizations have chosen instead to deploy dedicated internal messaging systems of their own to take advantage of the systems' benefits, while mitigating some of the risks associated with using systems commonly available through the major Internet service providers. These internal systems are protected by the perimeter network security devices, such as firewalls. But, as some organizations are moving forward with internal systems, others have rejected them because of the significant vulnerability of their data to an organization's insider threat.

Another means of providing more secure messaging systems is to block communications traffic at the network firewall. Most messaging traffic is transmitted through registered IP ports. Listings of these ports are available at www.iana.net. Once the ports are identified, both TCP and UDP traffic can be blocked at them to deny unauthorized usage of a network's services. Generally, however, it is more secure to create firewall or packet filtering rules that enable only those services required for the users' applications, and deny all others. ■

Cyber Security Inspections Support Ongoing Improvements

Inspections conducted by the Office of Cyber Security and Special Reviews (OA-20) in 1999 and earlier this year showed a generally improving trend across the DOE complex. Until the 1990s, DOE often considered cyber security less important than user convenience or operational efficiency. Additionally, DOE and contractor management sometimes allowed sites to operate computer systems and networks with little attention to DOE policy and effective security.

In 1995, OA-20 began using automated scanning tools to test the effectiveness of cyber security features on DOE systems and networks. OA-20 can test thousands of systems and all of a network within a week, rather than a year or more. Since the mid-1990s, OA-20 has continually expanded its testing capabilities, using such tools as "war dialers," which can test every phone line at a DOE site in a matter of days to identify any unauthorized modems. Hackers could use such modems to bypass a network's firewall and gain access to information or destroy data.

Along with these tools, OA-20 has developed an extensive, dedicated cyber security laboratory that is routinely used for cyber security inspections. During 1999, four of DOE's national laboratories and the Y-12 Plant were inspected in cyber security. Most recently, OA-20 implemented a "Red Team" approach, using a variety of techniques for detailed tests of a site's cyber security features, including network penetration testing by experts who know the latest hacker techniques.

Through its inspections and other activities, OA-20 has helped DOE identify vulnerabilities and improve its cyber security programs.

Current Status

Recent OA-20 inspections showed general improvement in DOE cyber security programs, although a number of areas warranted attention. During an April 2000 DOE Headquarters inspection of unclassified cyber security, several program offices demonstrated the appropriate level of leadership and support for cyber security, with well-defined roles and responsibilities. The DOE Chief Information Officer has strengthened the unclassified cyber security program by improving the Headquarters

(Continued on Page 3)

CAT Training (continued)

The primary mission of the CAT is to serve as the adversary when OA conducts tactical performance tests, but they also assist in testing intrusion detection systems and other elements of a site's protection system. To do this, the CAT members must think like a terrorist or other "real" adversary, reorienting their thinking from traditional defense to using unconventional offensive disciplines. The change to an offensive orientation requires new skills, tactics, and techniques.

In this year's training, CAT members learned techniques for testing (defeating through stealth) many types of perimeter intrusion sensors; they will use these techniques to help OA-10 determine the effectiveness of perimeter intrusion detection systems throughout the complex. The tactical aspects of this year's training focused on assault planning; rapid tactical movement in various environments; and executing operations while wearing protective masks. After three days of instruction and practice, the CAT spent two days planning and conducting "attacks": major force-on-force exercises, using MILES equipment and a full complement of defenders provided by the Nevada Test Site protective force. The protective force's participation benefited both OA and Nevada by increasing the level of realism: the CAT members were able to conduct their assaults against an actual protective force at a real facility, and the protective force received valuable training in defending against realistic assaults and unfamiliar tactics.

The CAT is a critical element of Independent Oversight's tactical performance testing program. The program has proven its value to OA-10 and to the Department many times, in many ways over the years. The program also provides value to the participating facilities, because CAT members take their new skills back to their facilities and use them to improve site protection programs. ■

Cyber Security (continued)

network backbone and main firewall, and by initiating network scanning to identify vulnerabilities. However, several areas requiring strong management attention remain.

The national laboratories inspected in 1999 were Lawrence Livermore, Los Alamos, Sandia-New Mexico, and Sandia-California. Various problems were noted in cyber security that resulted in vulnerabilities in their unclassified computer networks that contained sensitive information. OA-20's return visits to all these locations found that many of these cyber deficiencies had been addressed.

Future Cyber Emphasis

To maintain the current trend in ongoing cyber security improvements, DOE must not only correct the identified problems, but also remain vigilant for emerging threats to its cyber assets. Hackers will continue to come up with new ways to disrupt or damage cyber services, and new or reconfigured network systems will likely contain new vulnerabilities. Thus, DOE will need to develop new and increasingly sophisticated techniques to thwart unauthorized access.

OA-20 will contribute to these improvements not only through its inspection methods, but also through the new field partner program. In this program, **OA-20 invites cyber security professionals from DOE facilities to participate in its inspections**. By accompanying the OA-20 inspection team, each field partner can see first-hand how the cyber security inspection process works and gain a better understanding of the performance testing protocols and software tools that OA-20 uses to identify vulnerabilities.

With the continuing strong support of the Energy Secretary, significant enhancements in cyber security programs throughout the DOE complex are expected. ■

For further information on the OA-20 field partner program, contact the OA front office at (301) 903-3777.

Understand the Relationship Between Hazards Assessments and Hazard Analyses

The Office of Emergency Management Oversight (OA-30) has found that some weaknesses in hazards assessment can be linked to a misunderstanding of the relationship between hazards assessments and hazard analyses.

A misunderstanding may occur because hazards assessments and hazard analyses have similar attributes. However, the purpose of hazard analysis is to establish the basis of a facility's safety basis (which is documented in the facility's safety analysis report), while the purpose of the hazards assessments is to establish the basis for a site's hazardous material emergency management program. Outputs from hazard analyses include design parameters for release barriers and mitigative systems, instrumentation needs and specifications, and operating limits. Outputs from hazards assessments include the size of the emergency planning zone, indications of failed barriers (for use in developing emergency action levels), and predetermined protective actions.

Both hazards assessments and hazard analysis evaluate accident scenarios and typically use similar analytical techniques. However, the scope of the evaluations differs in several manners. Two specific examples are discussed below.

Malevolent acts are not considered as accident initiators in hazard analyses for plant operating design purposes; they are considered as part of vulnerability analyses for security purposes. However,

(Continued on Page 4)

Upcoming Oversight Activities

Sandia/TSD Emergency Management Lessons Learned Forums
Purpose: Communicate lessons learned from OA-30 reviews and solicit feedback on emergency management issues from DOE and contractor line management.
Date: To Be Determined
Contact: Chuck Lewis, 301-903-1554

Cyber Security Review of Argonne National Laboratory
Purpose: Review cyber security at ANL-East and ANL-West; will include external network security assessment.
Location: ANL-East and ANL-West
Date: August 7-16, 2000
Contact: Brad Peterson, 301-903-5781

Lawrence Livermore National Laboratory Follow-up Review
Purpose: Review status of efforts to resolve safeguards and security findings.
Date: August 21-30, 2000
Contact: Barbara Stone, 301-903-5895

Pantex Emergency Response Exercise Evaluation
Purpose: Review the capabilities of DOE and contractors responding to accidents involving hazardous materials.
Date: August 28 - September 1, 2000
Contact: Chuck Lewis, 301-903-1554

Revised Inspectors Guides Update DOE Inspection Process

The Office of Safeguards and Security Evaluations (OA-10) is updating and releasing its latest series of inspectors guides. Originally developed to describe the inspection process for the OA-10 inspection staff, the guides have been updated to reflect new inspection techniques and changes in security policy and technology. Although designed for OA, site self-assessment programs and field element safeguards and security staffs can benefit from these guides.

Inspectors guides being updated include:

- Classified matter protection and control
- Protective force
- Personnel security
- Physical security systems
- Material control and accountability.

Currently, the inspectors guides for the protective force and classified matter protection and control topics have been updated. These guides are available in PDF form on OA's Web site at http://tis.eh.doe.gov/iopa/reports/guide_docs/guide.html. OA-10 expects to complete the remaining guides within this calendar year.

Hazards Assessments (continued)

malevolent acts are considered as part of the hazards assessment and need to be evaluated in order to establish emergency action levels and protective actions for these events if the potential consequences warrant these actions.

Beyond-design-basis events are considered in hazard analyses to estimate the residual risk of operating the facility and to seek ways to minimize these risks. However, they are not considered in establishing the plant safety design.

On the other hand, hazards assessments consider such events as an integral part of establishing important aspects of the emergency management program, including the size of the emergency planning zone, emergency action levels, and predetermined protective actions. Consideration of beyond-design-basis events is important because it provides an addition level of safety (i.e., defense-in-depth) if the plant design fails in a manner that was not anticipated or that was considered to be "beyond extremely unlikely."

OA-30 is working with the Office of Emergency Management (SO-40) to ensure that DOE facilities receive a consistent message on developing hazards assessments by participating in emergency management lessons learned workshops (see article on page 1), participating in a special review of a set of hazards assessments, and communicating with each other on hazards assessments issues.

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**.