

## HIGHLIGHTS

### SECURITY EDUCATION SPECIAL INTEREST GROUP WORKSHOP

Omni Hotel at CNN Center, Atlanta, Georgia  
April 1-2, 2003

The Training Resources and Data Exchange (TRADE) Security Education Special Interest Group (SE SIG) held its spring workshop April 1-2 in Atlanta, Georgia. The SE SIG, established in 1985, is marking 18 years of service to the U.S. Department of Energy (DOE) and continues to be a link to a broad-based security community.

#### **Welcome**

*Valerie Anderson*, SE SIG Coordinator, ORISE, welcomed the workshop participants, noting that several people were attending for the first time. She emphasized the role of the SE SIG in serving as a resource for security awareness coordinators. Valerie introduced representatives from the Nuclear Assurance Corporation International (NAC), the host for the Atlanta workshop, and thanked NAC for providing the continental breakfast on April 1.

*Garland Proco*, Program Director for the Nuclear Materials Management & Safeguards System (NMMSS), welcomed the group on behalf of NAC, which is located in Norcross, GA, just outside of Atlanta. Mr. Proco gave an overview of the services NAC has provided to DOE and the nuclear industry, such as the NRC, since 1968. NAC has operated the NMMSS program since 1995. NMMSS is the data base and information support system for tracking nuclear materials controlled by the U.S. Government.

*Marvin Thompson*, SE SIG Steering Committee Chair, Pantex, thanked SE SIG members for their support during the three years he has served as Chair. He talked about how Safeguards and Security Awareness Programs in years past were some of the first to be cut in a tight budget; however, since “9/11,” he noted that security awareness has come into its own. He said “the door is open” and encouraged us to take advantage of opportunity offered. “Today we’ve been invited.” He emphasized that security awareness ties into every DOE security program.

#### **Keynote Address – Special Agent Gerald Becknell, FBI**

##### **Awareness of National Security Issues and Protection of Proprietary Information**

*Special Agent Gerald (Jerry) Becknell*, Atlanta FBI Field Office, was keynote speaker. Mr. Becknell is the Coordinator of Awareness of National Security Issues and Response (ANSIR) for the Atlanta office. He also serves as the FBI’s InfraGard Coordinator. InfraGard is a network of individuals and groups representing Federal agencies and the private sector. For more information, go to <http://www.infragard.net>.

Mr. Becknell talked about the FBI’s role in law enforcement and the sharing of information with colleagues both domestically and from other countries.

He said that the Patriot Act of October 2001 gave the government new powers in domestic law enforcement and international intelligence. He said we must move quickly to address the threat of foreign intelligence operatives. "We have a security problem in this country...Our borders are wide open." He also noted that the United States is a "Mecca for economic prosperity...Foreigners come to us."

Because one of the biggest threats is the "trusted insider," he believes the protection of proprietary information within corporations remains a challenge, as American businesses have high-tech information the rest of the world would like to have. He described the Economic Espionage Act of 1996 as a "significant piece of legislation" with significant penalties for stealing trade secrets. He said the private sector must practice "counterterrorism awareness" to counteract espionage.

To assist Federal efforts to protect its own agencies and the private sector, the National Infrastructure Protection Center (NIPC) was recently established within the Department of Homeland Security. The NIPC maintains a list of critical infrastructures, one of which is information systems. "Computer fraud is rampant in this country," Mr. Becknell said. Often the computer intruder is an "insider" with access to buildings and areas housing sensitive information. He noted that our nation's university systems are prime targets.

Mr. Becknell believes in addition to corporate responsibilities for protecting information, the government must exercise internal discipline and implement security procedures and practices. He said that today everyone has to assume a role in Homeland Security, and security awareness is the key.

### **Counterintelligence Awareness Briefing**

*Deanna Austin*, CN-1, is a Program Coordinator in the Plans, Policy, Training and Awareness Program, DOE Office of Counterintelligence. Ms. Austin emphasized, "The threat is real" and noted that former KGB officer Oleg Kalugin (a speaker at our 2002 SE SIG Workshop) is teaching us much about how foreign intelligence services and foreign entities operate. She quoted Mr. Kalugin's definition of counterintelligence as "working to counter others' efforts to gather intelligence." "Others" may be foreign operatives or persons within one's own organization.

"Who is targeting us?" she asked. With research a high priority in DOE, she said that foreign nations and terrorists groups want our information, particularly classified information, and economic espionage is a growing concern. Ms. Austin noted that "we lose tens of millions of dollars to other countries who can produce products cheaper, using our technology." She believes all DOE and contractor employees are potential targets – the uncleared, who may have access to proprietary information, as well as those with access authorizations. She said, "You may not be aware...People can't believe there's a motive...What do they want from me!"

Ms. Austin says that foreign travelers are specific targets, and she talked about ways in which foreign operatives use elicitation techniques to get information from persons who do not readily recognize they are being hit on. Another tactic by foreign operatives is the

“cultivation” of the insider with the goal of getting the person to give away information unwittingly.

She described various techniques used to gather intelligence and noted cyber concerns. “Access to our systems equals an opportunity to gather intelligence,” she said. “What can we do?” she asked. Ms. Austin said we must put a high priority on proactive reporting. “Reporting is absolutely critical.”

She said that DOE’s Counterintelligence Training Academy (CITA) offers excellent resources to help people become aware of how information is gathered, who is gathering this information, and what and how to report. To find out about training seminars at the CITA, go to <http://www.mnsi.doe.gov>. Also available on the CITA site is a CI Awareness Guide.

In closing, Ms. Austin referenced Marvin Thompson’s remarks about the door being open for security awareness. She said that if Security takes advantage of this open door, “CI will go with you.”

### **Policy Update/Preview of SSAQP**

*Loren Evenson*, Personnel Security Policy, SO-112, presented a “heads up” on new security directives to be issued in the coming weeks and months. He focused his talk on 1) a “streamlining” initiative for all Safeguards and Security directives, and 2) Safeguards and Security directives in process of revision that may be published before the “streamlined” directives.

He noted the impetus for the streamlined directives is DOE P 470.1, *Integrated Safeguards and Security Management Policy*. DOE will focus on “what” and not “how” policy will be implemented at DOE sites. The streamlined directives will be written for high-level DOE program offices and consist of one Order and six topical Manuals, which will replace all existing Safeguards and Security directives.

The rewriting of DOE O 470.1, *Safeguards and Security Program*, is under way, and manuals will be developed for the following topical areas: Protection Program Management, Personnel Security, Physical Security, Information Security, Protective Forces, and Nuclear Materials Control and Accountability. Existing requirements and guidance covering these six areas will be incorporated into the new manuals. New requirements will be formulated only if necessary. [Click](#) here to view the presentation slides on Streamlined Safeguards and Security Policy.

Loren said that several DOE Safeguards and Security directives are in various stages of development or revision, and may be published before the streamlined directives.

Note: Since this presentation, DOE N 251.53, *Extension of DOE Directives on Security*, dated 5/14/03, extends the following directives until 5/14/04:

- DOE O 470.1, *Safeguards and Security Program*, dated 9/28/95

- DOE O 471.2A, *Information Security Program*, dated 4/27/97
- DOE N 142.1, *Unclassified Foreign Visits and Assignments*, dated 7/14/99, was published without an expiration date; it will remain in effect until canceled.

Current and some archived and draft DOE directives are posted on-line at: [directives.doe.gov](http://directives.doe.gov). The SE SIG will also keep its members informed about changes to Safeguards and Security directives through the Listserv.

### **The Changing Role of the Safeguards and Security Awareness Coordinator**

*Dan Valdez* is the Safeguards and Security Awareness Coordinator and member of the Security Integration Team at Los Alamos National Laboratory (LANL). Dan talked about how the role of the Safeguards and Security Awareness Coordinator is changing in light of fluctuating world conditions and security situations at home. He strongly advocates a proactive approach to staying up-to-date on security-related developments, and said that an effective way to get information is through Web sites. Dan showed slides with names and addresses of several organizations that post information relevant to security.

Dan described the *Personal Security Handbook* he developed for LANL's Safeguards and Security Awareness Program that incorporates Department of Homeland Security provisions. He feels DOE should stay abreast of changes in terrorism so that we may be better informed on threats to our national security.

He believes that Safeguards and Security Awareness Coordinators have a part to play in Homeland Security and that we now have opportunity to become involved and active in the broader security arena. We should not necessarily limit ourselves to a set role. Dan's message reinforces the "open door."

### **Safeguards and Security Evaluations (I&E) Inspection Trends and Perspectives**

*Arnold Guevara* and *Mike Stalcup*, Office of Independent Oversight and Performance Assurance, Safeguards and Security Evaluations, OA-10, talked about inspection trends and perspectives. Mr. Guevara is Acting Director of the Office of Safeguards and Security Evaluations and Mr. Stalcup has responsibility for the Personnel Security Program, including audits of the Safeguards and Security Awareness Program.

Mr. Guevara said as a result of 9/11, their organization began taking some different approaches to inspections in providing independent feedback on protection for special nuclear materials (SNM), classified matter, and sensitive unclassified information. He said they are doing more performance testing and force-on-force exercises. They are also including audits of cyber security as part of a joint effort with the Cyber Security Office. Mr. Guevara said they have noticed that DOE sites have expanded security measures to increase protection. As a result, there is heightened awareness. The teams have also seen a strong response to the Homeland Security Threat Conditions.

Mr. Guevara cited the following “positives” during audits of sites: knowledgeable S&S staffs, ISSM implementation to make line managers responsible and encourage people to take more ownership for security, and progress with unclassified cyber security. Some concerns are: excessive Protective Force overtime, and reduced emphasis on training and performance testing. He also cited physical problems, such as aging alarm systems, old facilities in need of an upgrade, and internal network security failures.

For a stronger security program, Mr. Guevara feels that DOE’s design basis threat should take into account different characteristics of what terrorists can do, and sites should update their S&S plans to address vulnerability assessments. Research and development funds would be needed for such efforts, however. Currently, there is uncertainty about funding levels.

Mr. Guevara said root cause analysis is basic to a survey and self-assessment program, and he encouraged self-identification of problems. He believes any assessment of risk should include cyber risks. He also said that the best people to identify the weakness of a site are those who work there. When an I&E team does an inspection, he said the team looks at corrective action plans. He strongly encouraged that sites’ corrective action plans be revised to conform with DOE O 470.2B, *Independent Oversight and Performance Assurance Program*, dated October 31, 2002, which includes some changes in the corrective action plan requirements.

Mike Stalcup said Personnel Security inspections are conducted in four main areas: access authorizations, human reliability, foreign visits and assignments (FV&A), and safeguards and security awareness. He said that the insider threat remains a concern, and DOE is working to address employee access to SNM and sensitive unclassified information. Mr. Stalcup said the FV&A Program continues to make progress, but has a way to go. In looking at FV&A, the team reviews INS and Passport data. For PSAP/PAP (future Human Reliability Program [HRP]), he said reviews are done using objective selection of files, rather than totally random sampling. He said HRP candidates must not be allowed to work in HRP positions before certification. Access control is being looked at closely, and the CPCI database is compared to employment data.

Addressing the Safeguards and Security Awareness briefings, Mr. Stalcup said the team looks to see that the briefing topics cover requirements and that briefings are given on time and to the right people. Records must be organized and accessible. He encouraged sites to get feedback from the site population between briefings.

In closing, Mr. Guevara invited security personnel from the field to apply to be part of the HQ audit team in OA-10’s Augmentee Program. A field perspective would enhance the I&E effort, he said. OA would pay travel expenses.

### **S&S Awareness Coordinators Training/Security Refresher Briefing**

*Rob Ambrose*, Instructor at DOE’s Central Training Academy, began his presentation with information on the Nonproliferation and National Security Institute (NNSI). He said

the NNSI would soon have a new name, the National Security College, and would be granting a 2-year degree.

Rob said the CTA is assisting with the Accelerated Access Authorization Program (AAAP) used for granting some interim Q clearances. With a backlog of investigations, DOE is encouraging this process for selected cases. Security Police Officer (SPO) candidates who must become certified for PSAP/PAP may now use the AAAP to obtain a Q access authorization.

The next Safeguards and Security Coordinators Training course will be held the week of July 18, 2003. It will be a 4 ½ day course. For more information, contact Rob at: [rambrose@nnsi.doe.gov](mailto:rambrose@nnsi.doe.gov), or go to the CTA Web site at <http://www.nnsi.doe.gov> and click on S&S CTA to see courses offered. An SE SIG Special Task Group is helping to review lesson plans and slides for the Safeguards and Security Awareness Coordinators Training.

For the 2003 Security Refresher Briefing, the CTA Web site offers a briefing resource page with several topics available for downloading. The PowerPoint files were developed by subject matter experts at NNSI and can be integrated into a local refresher briefing. Rob said he would welcome additional submissions for 2004.

#### **Tools of the TRADE - INEEL**

*Kristine Inskip*, Idaho National Engineering and Environmental Laboratory, showed how the S&S Awareness Program complements her site's Total Integrated Management System. She said that with a safety culture well established, security was able to "piggy-back" onto this culture. She showed a segmented "wheel" marked with five programs. Kristine said that ISSM is being incorporated into all of these. Together, the programs comprise an integrated management structure for the site.

Within the Safeguards and Security Awareness Program, Kristine plans and carries out ISSM activities that include an ISSM video, puzzles, challenges and giveaways oriented toward ISSM awareness, and a Security Education presentation at a staff or safety meeting. Kristine handed out copies of a recent issue of "INEEL Talk" telling how security goals are being incorporated into the annual performance review process.

#### **Integrated Safeguards and Security Management (ISSM)**

*Terry Owens*, Director of Safeguards and Security in the Laboratory Administration Office, University of California, has responsibility for implementation of ISSM at Lawrence Livermore National Laboratory (LLNL) and LANL and has assisted with implementation at NNSA's Y-12 Plant in Oak Ridge and at Argonne National Laboratory. Mr. Owens has been involved with ISSM since its inception and has served on the ISSM Executive Council and the Safeguards and Security Management Implementation Team (SSMIT). He presented a brief history of ISSM, and cited its ongoing effort, driven in part by the Hamre Report of 2001. He emphasized the ISSM goal of performing work securely. He said that leadership support from senior level security managers is the key to successful implementation, along with "ownership" for security on the part of employees.

He said that ISSM was set up to mirror the Integrated Safety Management (ISM) guiding principles and core functions; however, the process is moving toward Integrated Management or IM. He emphasized ISSM is also a collaborative process. He noted DOE's directive on ISSM - DOE P 470.1. The philosophy inherent in this policy is that DOE would outline the "what" and sites would determine the "how."

Mr. Owens encouraged sites to share Lessons Learned and best practices, and he suggested that DOE write directives that are not overly prescriptive. Sites need to think about optimizing security dollars and take a risk-based approach to security. He said that the management contract for the University of California has an ISSM component and ISSM "guiding principles" are reflected in laboratory operations. Workers are asked to get involved and identify security issues. He emphasized that the importance of "grass roots" responsibility. The ISSM Web site can be accessed at: <http://www.issm.doe.gov>.

*Kent Oelrich*, Security Awareness Coordinator at LLNL, talked about how LLNL is continuing to incorporate ISSM into the Safeguards and Security Awareness Program. At the 2002 SE SIG Workshop, Kent described what was being done in "Phase I." He reported Phase I is now complete, with the site having reviewed the information. The team especially looked at questions and issues coming out of a "gap analysis" of ISSM, and one of the findings was that "non-security people were driving the train."

Note: From last year's workshop, we learned that a "gap analysis" involves such activity as reviewing security practices to identify policies and requirements that are fragmented, line responsibilities that are not always defined, and the integration of S&S programs.

Kent said that Phase II is expected to be completed by end of CY2003. The site has identified 27 specific taskings in 6 categories. Kent believes that a feedback and accountability system is particularly important to achieving their performance goals.

#### **Tools of the TRADE – Nevada Site Office**

Cindy Farinholt and Wayne Morris, Nevada Site Office, provided a video being used in Nevada's current Safeguards and Security Awareness and OPSEC programs. According to Wayne, the video "demonstrates collection activities of our adversaries and how employees can mitigate this collection threat through OPSEC awareness." Wayne and Cindy play central characters in this entertaining video, *Looking at It from a Different Angle*. For more information, you may contact Cindy or Wayne.

#### **Tools of the TRADE - Richland Operations**

*Ann Czebotar*, PNNL, and *Bonnie Harris*, Richland, presented an update on "Security Ed," the cartoon character in Richland's Safeguards and Security Awareness Program. *Chet Braswell*, Hanford, is also a member of the security team working to reinvent "Ed."

Background: Ed was introduced at the 2001 SE SIG Workshop. At that time he was depicted as invisibly "seated" in a chair in front of a computer, commenting on security issues of the day. Since then, Ed has continued to evolve, becoming a friendly, amorphous person with a hard hat, and in the latest incarnation, a badge, representing

“every employee,” because, as Ann and Bonnie explained, “Everyone wears a badge.” Ann and Bonnie also played a video showing “co-worker to co-worker” involvement in getting people to think about security; particularly, about who should have access to areas where classified information is located. “Security Ed” has a starring role. Richland also offers weekly “Security Ed” challenges through its newsletter, *The Hanford Reach*. To see these challenges, go to: <http://www.hanford.gov/reach> and click on “Security Ed Challenge.”

### **Identifying and Protecting Official Use Only Information**

*Linda Brightwell*, SO-121, is a Security Specialist in Information Classification and Control Policy, Policy and Quality Management Group. She talked about the new Official Use Only (OUO) directives, which, at the time of the workshop, were undergoing final review.

In developing these directives, Ms. Brightwell said the Freedom of Information Act (FOIA) exemptions are the basis for the OUO program. Unlike classified information, an OUO determination is less “authoritative.” However, the Hamre Report of 2001 identified a need to develop clear standards for identifying and protecting sensitive controlled information. DOE’s Office of Security took the challenge and began a directives package consisting of an Order that would give requirements and responsibilities, a Manual that would have detailed instructions for implementing requirements, and a Guide to provide information to assist with whether information falls under one of the FOIA exemptions.

Ms. Brightwell said that although anyone can determine OUO, people must know and understand the OUO objectives that are driven by the FOIA exemptions in Title 5, U.S. Code, Section 552(b)(1) to (9). One goal of the new directive is to offer commonality and consistency for determining whether something should be marked “OUO.” Previously, several program offices had their own guidance documents for OUO and the new directive is drawing from some of those. Ms. Brightwell said there are “no OUO police.” Whether information is OUO is determined by those who have responsibility for the information. She said, “If you don’t think you can protect it [information], don’t mark it. It’s up to you!”

If a document is requested under the FOIA, an OUO marking does not automatically exempt the information. A formal review is required. Ms. Brightwell cautioned that we must remember that an OUO marking is just a notice. A legal decision is needed for release of information.

Ms. Brightwell also talked about the importance of marking e-mail and transmittals. For sending OUO over telecommunication circuits, she said to use encryption.

Note: Since the workshop, the following OUO directives have been published:

- DOE O 471.3, *Identifying and Protecting Official Use Only Information*, 4/09/03

- DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, 4/09/03
- DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, 4/09/03

### **Unclassified Cyber Security**

*Melna Jones*, Program Manager for Unclassified Cyber Security for NNSA Oakland, said when she first started at Oakland, the work force was largely unaware of responsibilities for computer security. She began addressing various aspects of cyber security, such as network engines, and she assisted in writing comprehensive policy, procedures, and guides. She educated employees about policy and security. The Security Department soon became the information technology (IT) “support team” for the Oakland Office.

In developing computer security, the IT team focused on assessment, perimeter control, risk management to close vulnerabilities, and monitoring. The team found as people learned more about computer security, they became interested in knowing risks and threats. Ms. Jones believes that the more employees understand, the more they are willing to become involved in risk management and disaster recovery. As a result, the culture changed – from the top down – and Security reported fewer cyber security incidents.

Ms. Jones presented a video showing how employees can be monitored at their company computers. When sending e-mail, she advised us to think about three things: “Be careful of what you say, who you say it to, and who may be tuning in!” A workplace computer is fair game for monitoring to prevent fraud and abuse and misuse of network connections. She said that companies have a legal right to investigate use of Web sites. The video showed scenarios on the abuse of employee time spent on the Internet and the resulting termination of employment based on evidence. Ms. Jones said, “When you go online at work, it’s not a private line.” Ms. Jones furnished a list of computer security Internet resources.

### **What’s New at ISOO?**

*Emily Hickey*, Senior Program Analyst in the Policy Directorate, Information Oversight Office (ISOO), presented information on ISOO’s new organizational structure and mission. ISOO is part of the National Archives and Records Administration. For Web site information, go to: <http://www.archives.gov/isoo/index.html>. ISOO supports Federal agencies with security education and training. Materials ISOO has developed for government and industry include a Marking Booklet and the SF 312 Briefing Booklet.

Ms. Hickey spoke about the new amendment to Executive Order 12958. This further amendment was signed on March 15, 2003, and has been designated E.O.13292. The amendment was issued in response to an impending deadline for automatic declassification of National Security Information. (This deadline had been extended in 1999 to April 17, 2003.) Ms. Hickey talked about what parts of current policy did and did not change. Some changes went into effect immediately; however, others, such as marking of documents, are pending full implementation of the E.O. through an interagency process to be completed by September 22, 2003.

Emily Hickey has been the ISOO liaison to DOE for a number of years. She announced she is assuming new responsibilities in the Policy Directorate and that Bernard Boyd, a Policy Analyst in the Operations Directorate, will replace her as the DOE liaison.

### **CDC Bioterrorism Preparedness and Response**

*Dr. Joanne Cono*, Centers for Disease Control (CDC) in Atlanta, is a Senior Medical Epidemiologist in the Bioterrorism Preparedness and Response Program. Dr. Cono presented an overview of how the CDC prepares for and responds to potential attacks using biological agents. Since terrorism can manifest in various forms, becoming aware of potential events is key to acting quickly to mitigate consequences. Dr. Cono described how the CDC is on the alert constantly, both nationally and internationally. She said the agency depends on medical personnel in the field to identify and report, much as we depend on “front line” individuals to report our security incidents.

Dr. Cono specializes in smallpox response planning and vaccination and is consulted nationally and internationally on these issues. She presented several slides on smallpox, some of which, although quite graphic, give a sobering reminder of how deadly the disease can be. She talked about the virus being particularly virulent (30% of persons infected with smallpox will die) and there is no cure. Vaccination, however, is an extremely effective preventative measure, although it carries some risk with the live virus. She emphasized how important it is to quickly identify symptoms and put into place containment measures if an outbreak should occur. Education, awareness, and a well developed preparation and response plan are crucial in addressing biological threat. [Click here](#) to see the CDC presentation slides.

### **MC&A Awareness Project in Russia**

*Paul Thurmond*, a security consultant to DOE, reported on NNSA’s efforts to establish a Nuclear Materials Control and Accountability (MC&A) Culture Project in Russia. He is a member of a team that is working to establish a security awareness program at nuclear production facilities and power plants at former Soviet Union facilities and sites. He noted that there are many challenges ahead to successfully accomplish this mission.

Paul said the NNSA team will be visiting large facilities on-site for 2½ weeks to identify protection needs and to put into place a pilot self-assessment program. The program would be enacted on an interim basis. He said there is much social and economic upheaval right now in Russia and the “human factor” is so critical in all operations. He noted that the facilities do not have strict controls, and said, “There is not much in way of incident reporting.” At the Russian facilities, managers don’t tend to recognize the insider threat.

Paul would like to see an exchange program with some of our site Safeguards and Security Awareness Coordinators involved, but is not sure how that might be accomplished. In establishing a new security culture, the NNSA team will conduct surveys of management. Also, awareness training courses are being planned for security managers and workers. The team will work to develop standardized training plans, he said, and a goal during their short stay on-site is to gain familiarity with facility

operations assess available support for the program from the Russians. The team will work exclusively with security personnel in each facility. Later trips will involve talking to other facility personnel.

Paul asked, "How will we [the team] measure success?" He said they are looking for some metric to establish a baseline. He invited our comments/input into how best to establish an effective security awareness program at these nuclear sites that all have potential for global nuclear proliferation.

### **Posters and Appropriations**

*Ceil Rogers*, Security Education and Training, SO-61, said that the DOE poster program is continuing; however, new posters have been on hold pending a change in contractor personnel. The person who will be reviewing and providing designs will be on board shortly, and Ceil expects the posters to be issued in a timely manner. She also said she would welcome ideas from people.

On the topic of Federal appropriations, Ceil had attended a seminar on appropriate use of funding and wanted to share information on what might be appropriately spent for items considered as "promotional." She said that any expenditure must involve application of the "necessary expense doctrine," and that monies need to be used for purposes "for which the funds were obtained." For our group, promotional items should remind people of their security responsibilities, and ideally the promotional items should be something used in the workplace, such as pencils. Safeguards and Security Awareness Program "awards" can be purchased and given out if they are part of an awareness activity.

### **Open Forum**

*Sylvia Lovelett*, Pantex, and *Virginia Reams*, NNSA Oakland, served as moderators of Open Forum, a group discussion of issues relevant to Safeguards and Security Awareness Coordinators.

Virginia began by giving an update on the re-structuring of the NNSA; specifically on one of its four major offices, the Office of Federal Services. Virginia reported that the Acting Administrator of NNSA approved a functional alignment on December 19, 2002, that "would better enable NNSA to meet varied missions and changing operational requirements." Virginia said the realignment affects her position in Personnel Security at the Oakland Office, as this function will move from Oakland to an NNSA Service Center in Albuquerque.

The new Office of Federal Services includes the following "departments": Security Support (including the Personnel Security Division), Information Technology, Human Resources, and Training and Development. The NNSA realignment is to be completed by December 2004.

Another topic for discussion was concern over the excessive processing times for DOE access authorizations. It was noted that one of our OA-10 speakers the previous day had said funding resources for reinvestigations are limited, particularly since the FBI began

reinvestigating persons tapped for the high-security positions, such as PSAP. The timeliness issue has been elevated to DOE HQ and OPM and FBI liaisons, but all Federal agencies have backlogs. DOE continues to work with OPM and FBI to reduce current backlogged timeframes; however, ultimately, the U.S. Congress may have to get involved.

JoAnn Archuleta, who directs the CTA's Foreign Interaction Training Academy, said that the FV&A directive is undergoing revision, and current policy is to be followed.

#### **Tools of the TRADE – Sandia/AL**

*Adele Montoya* and *Ann Marie Griego*, SNL/AL, presented a video on access controls developed for Sandia's Safeguards and Security Awareness Program. Its title, *The Sandia Kid*, hints at the video's humorous portrayal of a "bandit" trying to force his way into security areas. The bandit is thwarted by a Security "good-guy." SNL provided CDs of this video for TRADEing Post.

Ann Marie talked about how ISSM is becoming integrated into the SNL Safeguards and Security Awareness Program. The site is working toward getting people to think about security in a different way, she said. A mindset that integrates ISSM and Security should help cut down on security incidents.

#### **Threat Management – Violence in the Workplace**

*Christina Holbrook*, Security Operations Specialist at the Boeing Company, Seattle, talked about managing violence within a corporate setting. In this uncertain world, we all could be subject to outbursts of violence at any time on the part of a disgruntled employee. However, it's the responsibility of an employer to maintain a safe work environment for employees. An employer must not allow aberrant behavior to persist. Christina talked about early intervention to prevent a person's "snapping." And she said it is important for all of us to recognize symptoms of employee stress and report observations according to site policy.

She presented slides defining workplace violence and describing why a company needs a threat management program with several key elements. She talked about the impact of workplace violence, the myths surrounding workplace violence, and why violence is not being reported. She emphasized that "violence is a process." And "the best indicator of future behavior is past behavior."

Christina favorably cited two DOE documents on *Security in the Workplace*: "Supervisor's Guide to Preventing and Dealing with Violence in the Workplace" and "Employee's Guide to Preventing and Dealing with Violence in the Workplace." These documents are available from SO-211 by e-mailing a request (include your mailing address) to [kim.alson-akers@hq.doe.gov](mailto:kim.alson-akers@hq.doe.gov).