

HIGHLIGHTS

SECURITY AWARENESS SPECIAL INTEREST GROUP WORKSHOP

Hotel InterContinental, New Orleans, LA
April 13-14, 2004

The Security Awareness Special Interest Group (SASIG) held its spring workshop April 13-14, 2005 in New Orleans. The SASIG, established in 1985 as part of Training Resources and Data Exchange (TRADE), is marking 19 years of service to the U.S. Department of Energy (DOE) and continues to be a link to a broad-based security community.

Welcome

Virginia Reams, SASIG Chair, NNSA Oakland, welcomed participants to the workshop and noted that several people were attending for the first time. She introduced the SASIG Steering Committee and encouraged new participants to get to know the Steering Committee and others in the SASIG who are knowledgeable resources for Security Awareness. She thanked Jeff Dugar of the Strategic Petroleum Reserve Office (SPRO) for his efforts in helping to coordinate the workshop. She introduced the workshop theme, "Security Awareness for Changing Times," and said presentations had been prepared by speakers to reflect this theme.

Valerie Anderson, SASIG Coordinator, ORISE, thanked the SASIG Steering Committee for their efforts in planning the workshop over the past several months and their willingness to volunteer for presentations. She also welcomed workshop attendees and noted that the agenda offered topics of interest to old and new participants alike. She thanked Clarice Bruce for coordinating TRADEing POST, an exhibit of Security Awareness materials from many sites. Valerie expressed special thanks to Jeff Dugar for the support he and SPRO provided for this workshop, particularly in the loan of equipment for the meeting room, and she acknowledged the generosity of DynMcDermott Petroleum Company for sponsoring the pre-workshop "ice-breaker."

Rick Shutt, Director of Security and Emergency Operations, Strategic Petroleum Reserve Office, welcomed everyone to Louisiana and provided an overview of the SPRO facility. He explained that SPRO is a critical infrastructure facility with a national security mission. SPRO employs about 750 Federal and contractor personnel. DOE partners with the Department of Interior in protecting the crude oil assets, which are stored in multiple salt caverns at four sites in Louisiana and Texas. The Reserve is the United States' emergency oil stockpile and one of the largest emergency petroleum supplies in the world. SPRO works with the Department of Homeland Security and with FEMA in the protection of the nation's contingency supply.

Keynote Address:

Homeland Security Today

Col. Terry J. Ebbert, Director of Homeland Security for the City of New Orleans, was keynote speaker. In addressing the changing role of Homeland Security, Col. Ebbert described multiple problems the U.S. has been forced to deal with in post-9/11. He said "our enemies truly hate us... and are out to destroy our economy." With 9/11, "we recognized we were a participant in a world war...a war based on survival of our economy." He said some foreign nationals hostile to

us view the U.S. as an open society, driven by a robust economy, and having freedom of speech, travel, women's rights, and education – “freedoms other countries can't co-exist with.”

Fundamentalism cannot operate in an open society, and our very way of life is a target of fundamentalists. Col Ebbert says, “Our enemies dislike us for what we do well.”

He emphasized that these are “changing times,” and that we will never go back to “9/10.” For SE Louisiana, the “Energy Heartland of America,” the new Homeland Security (HS) challenges can be addressed through: 1) Resources, 2) Teamwork, 3) Planning. He described the problems as follows:

- Resources - currently, not enough HS funding is being allocated to the State. Funding is usually based on population and Louisiana does not have a large population. It does, however, provide critical support for national security, and a different formula for dividing limited resources must be devised so these critical national vulnerabilities can be adequately addressed.
- Teamwork – there is little integrated planning among the local governments. Col. Ebbert blames this on a lack of cooperation among the parishes, which all have unique problems and priorities for spending money. The region needs to be prepared to deal with big-picture problems. He asks, if there is a chemical spill, how is response handled? “Who is in charge?” was a perennial question before 9/11, but being able to answer quickly is more crucial now.
- Planning – the Federal mandate is to “fix Homeland Security,” but this fix requires a plan. Even with \$87 billion in HS funds to be distributed, “there is not enough to buy everything for everybody.” There are competing interests that can be adequately addressed only through planning.

Col. Ebbert noted a major change taking place in planning for potential disasters: Prior to 9/11, disaster funding came from FEMA in a “backend” approach. Clean-up for disasters meant “body-bags.” In a post 9/11 environment, “we must focus on prevention.” After-the-fact investigations by the FBI are not enough in doing battle against terrorism. We must identify terrorists and get better at detecting these people at airports and other places. We need a “mission of prevention, not just investigation, arrest, and prosecution.”

Col. Ebbert said that weapons of mass destruction continue to be a serious concern. Many foreign countries have nuclear capabilities and it will take a “tremendous coordinated effort” to keep our populations safe. We need “all agencies at the table,” he says, and “the more we work together, the better.”

In terms of potential disasters, Mother Nature poses as much threat as terrorists. He said that a Category IV hurricane could shut down this nation's economy and affect petroleum capability. Disaster planning and recovery must address all eventualities.

In closing, Col. Ebbert believes HS must spend its money judiciously and find ways to incorporate teamwork into planning and spending the resources. Public education will be of

extreme importance. The New Orleans' Office of Homeland Security is developing informational material on Terrorism Awareness for its Web site. For information, go to: www.new-orleans.la.us/home/departmentsAndAgencies/dhs/ti.

What's New at ISOO?

Tina Williams, Senior Program Analyst, Information Oversight Office (ISOO), is ISOO's liaison to DOE and some other Federal agencies. ISOO is part of the National Archives and Records Administration. She presented information on the March 2003 amendment to Executive Order (EO) 12958, emphasizing the changes in marking for declassification. The amendment was issued in response to an impending deadline for automatic declassification of National Security Information (NSI). Full implementation of the EO was completed September 22, 2003. She said the new ISOO Marking Handbook, as modified by ISOO Implementing Directive 1, is available online through the ISOO home page. Go to: <http://www.archives.gov/isoo/index.html>.

ISOO has responsibility for NSI policy and oversight. Tina emphasized whenever NSI has been compromised, DOE has responsibility to report the compromise to ISOO.

Tools of the TRADE

Posters for Security Awareness, and the Video

"Security Ed and the Plight of the Missing Badge"

Chet Braswell, Hanford, discussed the security awareness poster program at Hanford, an initiative that has had much success. Hanford has been willing to share these posters with other sites. Posters are developed around current topics of interest and often tie into time of year (season). For example, in October, Hanford distributed a Halloween poster featuring an owl and "OUO" message. Chet says that posters do much to promote security awareness, and this attention to awareness is still very much needed despite efforts of ISSM. He cited a continuing "us vs. them" culture in which employees tend to see a problem as Security's responsibility, not theirs. The posters Chet has shared by e-mail with the SASIG membership had site-specific information removed. However, these posters can be made site-specific if a site has the software to adapt the information. The posters can be printed in 11" x 17" format using a standard color printer.

Chet also talked about the latest Security Ed video, "Security Ed and the Plight of the Missing Badge," and thanked individuals in the SASIG for taking time to review and comment on the draft script for the video. These comments were considered in developing the final product. The SASIG has seen the evolution of "Ed" – from "somebody else" sitting in an armchair commenting on security issues to a personified security badge that represents "me." Chet said Hanford and Richland Operations plan to continue producing videos that are generic enough so they can be distributed to other sites upon request.

Also, to promote security awareness within Richland Operations, the "Security Ed" challenges continue as a feature of the Hanford newsletter. These "challenge games" have been very popular with employees.

Inspections and Evaluations: A Site Perspective

Kent Oelrich, Lawrence Livermore National Laboratory (LLNL), led a discussion of recent I&E inspection activity at LLNL, Sandia National Laboratories/NM, and NNSA Y-12. Kent shared key points of the SNL report so that we might be aware of what inspection teams look for during an audit of S&S Security Awareness Programs. He said the documentation of briefings is very important; also, inspectors want to know about involvement in ISSM, and even the S&S Awareness Coordinator's participation in the SASIG, which OA notes as an excellent resource and support group. In an LLNL inspection, Kent said that inspectors had individuals complete a questionnaire on S&S awareness and also talked to individuals to gauge their knowledge of the program.

Safeguards and Security Lessons Learned: Contributing to Security Awareness

Gene Marquez, Sandia National Laboratories/NM, talked about how the "electronic era" has changed communications. He said the "masses of information" coming to us are a continuing challenge, and we are in information overload at times. But we must continue our security awareness focus in the midst of this overload.

Gene believes that good communication is needed now more than ever and says we should give people information people they will use. "You don't always have to give a lot of information," he said. Target the information to need. He asks, will people access Lessons Learned? An awareness goal is to enhance security performance. He emphasized a need to drive home the importance of protecting classified and work to prevent security violations, infractions, and incidents. He referred to Col. Ebbert's concern about action taken "after the fact" when an adverse event may have been prevented. In communicating, Gene said that we must eliminate "stove piping" and focus on integration. The Security Awareness & Lessons Learned (SEALL) team at SNL is made up of representatives of various security programs such as CMPC, Cyber, and OPSEC in an integrated effort to promote S&S awareness. (See "SEALL" below for more information.)

Tools of the TRADE

Self-Assessments

Kaye Hall, Kirtland Operations, talked about self-assessment activity. She coordinates a robust program of self-assessments at Kirtland facilities that has resulted in some inspections being waived. Kaye emphasized that self-assessments are key to strong Safeguards and Security programs. She provided handouts of a Security Self-Assessment Plan that includes methodology, preparation of a survey report, and follow-up corrective action. She also handed out a sample self-assessment form with a checklist of the topical and subtopical requirements for all S&S programs.

SNL's SEALL Program

Ann Marie Griego and *Adele Montoya*, SNL/NM, presented SNL's Security Awareness & Lessons Learned (SEALL) program. In developing this awareness outreach, they worked to involve several security programs. "Organizations need to talk," they said. The goal is to achieve the 4 R's: Provide the **Right** security information, to the **Right** audience, at the **Right** time, through the **Right** mechanism. These translate to What, Who, When, and How.

A Web site for the SEALL program provides management with tools to share at department meetings; for example, streaming videos on security were developed that play for 3 – 5 minutes. Several remote locations have access to this site.

Ann Marie talked about a festive security awareness event being planned for May 5. The “Cinco de Mayo” security fair would feature a Mexican theme and food, a trading post, guest speakers, videos, and games. The fair had been widely advertised at all SNL facilities. A large number of SNL employees are expected to attend. [Post-note: Ann Marie Griego never got to see this event come to fruition. Her death shortly after the SASIG workshop was most untimely. The Cinco de Mayo event was a great success, and we are certain that the S&S programs Ann Marie was involved in will continue to reflect her efforts.]

Create a Menu of Security Briefings

Nancy Cross, ORAU/ORISE, prepared a presentation that featured one of the briefings she is called on to give “on demand.” Often the briefings are in response to a specific need, such as to the “Post-Docs” who are present for finite periods of time at Oak Ridge National Laboratory or the Y-12 Site. Individuals she briefs are both cleared and uncleared, and many are foreign nationals. For this presentation, she focused on briefing the S&S reporting requirements of individuals.

Developing Briefings for Off-Site Personnel

Kaye Hall, Kirtland Operations, coordinated a group activity for the purpose of developing an outline for a generic refresher briefing for often hard-to-reach off-site personnel. A site’s “standard” briefing materials do not always address the special needs of off-site contractors and consultants. The briefing, when developed, should be structured with capability to include site-specific information. Small groups of 6–7 persons worked to identify scope and briefing topics.

Personnel Security Policy Initiatives

Lynn Gebrowsky, Director, Office of Safeguards and Security Policy, SO-10.1, presented a chart showing the proposed re-structuring of the Office of Security (SO), with the expectation that the organizational changes would be finalized shortly.

Lynn also described the draft Safeguards and Security Streamlined Directives to be issued for review and comment. These directives have been drafted to address only high-level DOE program responsibilities. They consist of one DOE Order, six topical Manuals, and one Reference Manual. The intent of streamlining is to avoid multiple Orders, some of which are conflicting. All outstanding policy memoranda have been folded into the directives. With the streamlining policy, DOE’s intent is to focus on “what” rather than on “how” policy will be implemented at DOE/NNSA sites.

Manuals have been developed for the following topical areas: Program Planning and Management, Protective Force, Personnel Security, Physical Protection, Information Security, and Nuclear Materials Control and Accountability. Existing guidance covering these six areas is either incorporated into the Manuals or canceled. New requirements will be formulated only if necessary. Once the Manuals are issued, subsequent changes will be made by page change – not by memoranda. The S&S Awareness Program will be under Program Planning & Management.

Lynn also talked about the new Human Reliability Program (HRP), which is to be implemented by April 22, 2004 in accordance with 10 CFR, Part 712. This regulation merged two former human reliability programs: the Personal Assurance Program (PAP), oriented toward nuclear safety, and the Personnel Security Assurance Program (PSAP), focused on security. Sites affected by the HRP will be given an orientation that details new requirements for the program.

Open Source Information and Intelligence Collection

Wayne Morris, OPSEC Manager at the Nevada Site, is involved in inter-agency OPSEC programs. He shared an entertaining video that was entered into an OPSEC competition. The video, “Arnie Aware: OPSEC Linebacker,” modeled after a TV character, won a national OPSEC award for the Nevada Site.

In discussing open source information, Wayne posed the questions, where do adversaries go to get information, and what can we do to limit their collection efforts? He described a five-step OPSEC process we can apply in protecting information (see presentation slides). He noted that intelligence handbooks, such as those developed by al-Quida, People’s Republic of China, and Jihad groups contain information found in open sources. He said at least 80% of information is available through an open source and it may be more like 90%. Bottom line: a wealth of information is available in public places. Wayne said that adversaries will target the Internet, libraries, public media and public records. We need to be aware that these individuals are watching and listening to us. He emphasized the importance of OPSEC awareness as key to deterring and preventing intelligence collection, and he encouraged every employee to be a “foot soldier” for awareness. OPSEC managers, along with S&S Awareness Coordinators, must do their part in promoting awareness initiatives.

Identity theft is also a significant problem today; in fact, according to Wayne, it is “the fastest growing crime in the U.S.” We can and must do more to protect ourselves at home and at work from those who would steal our identity. Our personal information is wanted by others.

Tools of the TRADE

Presentation Options for Required Briefings

Kristine Inskeep, Idaho National Engineering and Environmental Laboratory (INEEL), and *Clarice Bruce*, Rocky Flats Closure Project, talked about presentational options for required briefings. Kristine stressed teaching security awareness through briefings, which can be presented in various forms, such as in-person, through CBT, video, or other means.

Clarice showed her video, *Security Terminations*, produced in preparation for the Rocky Flats Plant for closure activities. She said that Rocky Flats still has 700 access authorizations for individuals who perform classified or sensitive work; however, these are being terminated as the plant undergoes closure. The video has been used successfully to let people know why they will no longer need clearances and to prepare them for loss of their access authorizations.

Tools of the TRADE

Jeanette Lee, Kansas City Plant, shared details of two new security products KCP has in development: one is the Secure Lock Indicator Control, or SLIC, which will be used to monitor

combination locks on vault-type rooms, and the second is the Radio Frequency Identification (RFI) which will be used to track materials.

SLIC allows personnel to see that vault-type rooms have been secured at the end of a work day. Use of this system is expected to reduce security incidents. With fewer infractions, costly follow-up inventorying of a room's contents can be avoided. The KCP is looking for sites to participate in a pilot study.

RFI technology would track materials; in particular, classified items which are important to manufacturing. There are many applications for this technology which would track not only the asset, but associated information.

Jeanette also showed a streaming video with an OPSEC message starring "Fred Hack," social engineer. This video won a national OPSEC award for KCP.

Open Forum

Sylvia Lovelett, Pantex, and *Christina Holbrook*, the Boeing Company, served as Moderators of Open Forum, a group discussion of issues relevant to security awareness.

One participant asked about ways to promote security awareness; in particular, how can we know our program is effective. The group pointed out that with a successful program, there would be fewer security violations, infractions and incidents. Employees who are involved in a strong program will understand their responsibilities for protection of national security assets. An excellent resource for any security awareness program is the S&S Awareness Handbook, available on the SASIG Web site. Also, the 2001 Washington State University study on the effectiveness of DOE S&S Awareness Programs is a worthwhile resource for persons responsible for an awareness program. This study was sponsored by Richland Operations and Hanford with results presented at the 2002 Workshop in Las Vegas (see Highlights for 2002 Workshop). The full report was distributed on CD to DOE Security Awareness Coordinators.

Another topic that generated discussion was the Human Reliability Program (HRP), which has replaced the Personnel Security Assurance Program (PSAP) and the Personal Assurance Program (PAP). PSAP was oriented toward security and PAP toward safety. Dr. Jerry Eisele of ORISE, principal author of the rule-making for HRP (10 CFR, Part 712) and talked about some of the requirements of the new program. The rule was to go into effect April 22, 2004. Those sites participating in the HRP will receive an orientation. In the discussion, it was pointed out that sites may have different ways of implementing this program. For additional information on HRP, see the presentation by Lynn Gebrowsky (above).

Cyber Vulnerabilities: The CI Perspective

Willie Edwards, Instructor at DOE's Counterintelligence Training Academy (CITA), focused his presentation on cyber aspects of CI awareness. He indicated that CI is a part of the cyber world, and we can expect to see more espionage with a cyber connection. The cyber threat is real and cyber terrorists are out to steal information. Willie talked about CITA's Information and Special Technologies Program (ISTP) with its proactive approach of deterring and detecting. ISTP targets foreign intelligence and international elements.

Willie explained the difference between cyber terrorism, which is overt, and cyber espionage, which is covert. In an overt act, we can know when the “threat is hot.” However, with covert espionage, we “may not have a clue what’s going on.” For example, power grids can go down before we are aware of what’s happening. He cited major vulnerabilities of the cyber world: e-mail, including attachments; Web sites with business-sensitive information, including information on personnel; and personal information. Computer systems should have router and firewall support for anti-viruses. He cautioned never to use business e-mail for personal use. Also, if people work from home and access a work computer, this access may spread viruses.

S&S Awareness Coordinators Training

Rob Ambrose, Instructor at DOE’s Central Training Academy (CTA), announced that the former Nonproliferation and National Security Institute (NNSI), which has responsibility for managing the CTA, has been renamed the National Training Center (NTC). Rob reported on upcoming training courses that may be of interest to SASIG members, including the S&S Awareness Training scheduled for the week of July 12, 2004. For more information, contact Rob at: 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 SASIG Special Task Group assisted with review of lesson plans and slides for the 2003 Safeguards and Security Awareness Coordinators Training.

Incidents of Security Concern

Debbie Larabay, Headquarters Team Lead for Incident Reporting and Management, Office of Field Assistance, SO-20.1, discussed criteria for security incidents reported by sites. The criteria are designated according to the severity of the incident using an Impact Management Index (IMI). Designations are IMI 1 – 4, with 1 the most serious.

The Incident Tracking and Analysis Center (ITAC) is operated by Pacific Northwest National Laboratory to track security incidents throughout DOE. Incidents occurring at sites are reported to PNNL and entered into the ITAC database. Reports can be run that provide various types of information. Site Facility Security Officers can request information specific to their site, and Headquarters program managers may also request reports. PNNL is currently sponsoring ITAC pilot programs at DOE HQ, KCP, Pantex, INEEL, and SRS. In the pilots, sites enter incident information directly into ITAC; and through classified channels, the information can be transferred to the Safeguards and Security Information Management System (SSIMS). Direct use of ITAC by sites is expected to result in a more efficient and expedient reporting and tracking process.

Integrated Safeguards and Security Management (ISSM) Implementation

Peggy Finney, Program Project Manager, BWXT, Pantex, talked about ISSM implementation at the Pantex Site. She said that ISSM is being implemented plant-wide and is linked to the site’s Strategic Plan. The site has begun developing new operating documents to reduce the kinds and amount of operating procedures. The Safety, Security, and Quality Assurance Process (SSQA) functions as a tool to implement security requirements and consists of four business process documents, replacing all operating documents. A matrix links roles and responsibilities and work instructions, etc. Peggy said the site is also working on matrices for measurement to show how

line management is meeting the ISSM requirements. She is encouraged with site progress; however, she acknowledges that the “cultural change is slow.”

Workplace Violence in Post-9/11: How Our Responses Have Changed

Todd Conklin, Deputy Group Leader, Nuclear Material Information Management, LANL, talked about the challenges of managing violence in the workplace, particularly in a post-9/11 environment. He described three cases of potential violence that he was involved with that called for de-escalation. One case involved holding a hostage at gunpoint. Todd was able to successfully diffuse each situation successfully, but not without some tense moments. He emphasized that people’s coping mechanisms can break down when faced with changes (such as loss of a job). “We must give them a mechanism to de-escalate,” he said. Also, domestic violence “plays big at sites.” We are often front-line information links between the worker and the workplace. When employees are impaired, workplace safety and security is in jeopardy. Todd emphasized that it’s the responsibility of an employer to provide and maintain a safe work environment for employees.

However, when people leave a workplace with anger and disgruntlement due to loss of their job, there are often consequences that can include: 1) theft, 2) vandalism, 3) graffiti, and 4) sabotage. How do we deal with the violent acts? When confronted with potential violence, Todd said you have to “solve for drama first and solve for process later.” He suggested that “being nice” helps and says we need to respond to people in a way they feel they are being listened to. We can indeed be “little beacons of light” for people on the brink of committing a violent act. We must convey in serious, no-nonsense terms what we accept and don’t accept in behavior. Help them de-escalate.

In this uncertain world, outbursts of violence can happen at any time. When someone threatens, we must make a quick assessment of the threat, asking, “Does he/she have the means and mode to carry out the threat? “Gut” feelings are important, and the best indicator of future behavior is the person’s past behavior. If someone has a gun, don’t try to deal with the situation yourself. Call Security.

In closing, Todd emphasized that we must try to control and diffuse a tense situation before it turns into a violent act. It is important for us to recognize symptoms of employee stress and report observations to management. Detection and prevention are the keys to dealing with potential workplace violence.