

HIGHLIGHTS

SECURITY EDUCATION SPECIAL INTEREST GROUP WORKSHOP

Hyatt Regency Crystal City, Arlington, Virginia
April 9-11, 2001

The Training Resources and Data Exchange (TRADE) Security Education Special Interest Group (SE SIG) held its 2001 spring workshop April 9 - 11 in Arlington, Virginia. The SE SIG, established in 1985, is marking 16 years of service to the U.S. Department of Energy (DOE) and continues to be a link to a broad-based security community.

Monday, April 9

Opening Remarks

April Stottler, SE SIG Advisor, Office of Safeguards and Security (SO-21); *Marvin Thompson*, Chair, SE SIG Steering Committee, Pantex Plant; and *Valerie Anderson*, SE SIG Coordinator, ORISE; welcomed the workshop participants. April reaffirmed SE SIG's commitment and assistance to security awareness programs throughout the complex and the program office's support for field initiatives and projects.

Marvin stressed that strong security depends on the conviction and commitment of individuals. "Remember, security is a people business. If we forget that, we fail." He remarked on the good attendance at the workshop and said the D.C. location had allowed an agenda of timely subjects with recognized presenters. "Build it and they will come."

Valerie noted that several people were attending for the first time. She thanked those who have participated over the years for their continuing support of the SE SIG. She emphasized that SE SIG is a year-around resource for security educators.

Keynote Address

Joseph S. Mahaley, Acting Director, Office of Security and Emergency Operations (SO-1), thanked the SE SIG for giving him the opportunity to share his vision and goals for the role of security education and awareness in the department's protection programs. Mr. Mahaley said that DOE needs a new approach to security awareness. To win people over, "we must get rid of complacency" and do a better job of getting people to support the department's security policy, protocols, and procedures. He offered a challenge to "shake yourselves up" and get people to sign up to security. He emphasized the "Security Czar" concept is gone; instead, we must convince people that strong security depends on each person. "Folks need to get on board."

Current security-related policy is being reviewed with the expectation that policy areas will be finalized by the end of July. All policy is being looked at thoroughly. Mr. Mahaley emphasized there are many good programs in DOE. "We're doing a lot of things right." SO-1 has identified three primary areas of organizational focus: policy

formulation, line management formulation, and oversight function. Mr. Mahaley sees a need for a "marriage" of security and information with the Chief Information Officer (CIO). Future policy should reflect some integration of the two. The department will also write policy for Integrated Safeguards and Security Management (ISSM) to be implemented within the NNSA and will change policy when and where necessary. The ISSM is a major initiative and a long overdue step, he said.

Mr. Mahaley believes that Secretary of Energy Abraham is "security conscious." The budget for security has not been cut, and there is good funding especially for material management and inventory systems. No one has taken a "whack" out of security.

The department has been working on several initiatives for cyber security and personnel security. Fixes in cyber security will not be easy or cheap. The department must spend money wisely, Mr. Mahaley said, and move ahead in a well-coordinated fashion that should begin with a careful evaluation.

Personnel security initiatives include a modification of 10 CFR Subpart 710 in response to the requirements of E.O. 12968. The changes will apply to denying or revoking of clearances, with a three-person appeals panel proposed for final decisions. A forthcoming rule will combine the PAP and PSAP programs into a new Human Reliability Program (HRP), managed by SO-21. Explosive safety regulations, currently in Defense Programs, will become part of the department-wide HRP.

Mr. Mahaley said that polygraph testing has been under scrutiny. DOE must build support for the testing in the labs. The polygraphs being given are not full-scope; rather, they have a national security focus. DOE's polygraph program is high functioning with an excellent reputation. Polygraphs require proper adjudication, and DOE has some of the best centers and best examiners.

In closing, Mr. Mahaley stressed the importance of increased security awareness. Commitment begins with the individual. Our awareness challenge is to get people to think about what they're doing. We must change mindsets.

The NNSA Today

John C. Todd, Chief, Office of Defense Nuclear Security (NA-3), said security requires a broad philosophy that begins with basic principles and goes on to address specifics. DOE should work with the Department of Defense on "defined threat."

The NNSA wants to understand what the issues are at the sites and will depend on the sites to identify these. Mr. Todd said security is complex with its many disciplines but we should try to achieve synergism. He asked, "How do we make pieces match so they make sense?" For strong national security, we must apply the fundamental principles, which are:

- Deterrence—based on perception of adversary
- Detection of risk

- Assessment of attack
- Delay of adversary
- Response to attack
- Neutralization of adversary

Mr. Todd believes that security is considered successful if we deter an adversary, and he emphasized "perception is reality." All principles work together. For example, detection without assessment is useless. "And who does the assessment?" he asked. Answer: humans, who must know how and what to assess (such as reporting incidents).

Mr. Todd also asked, "How much security is enough?" Answer: enough to send an enemy to another target. He stressed that security must make sense to people. At the sites, we must identify what is important and what is not important. "What does the adversary need? Workers know!" Workers will protect something if they believe it's important to protect it. Workers will implement the security provisions if they know the "why" of requirements. Mr. Todd feels it is important that individuals at the sites have an opportunity to participate in security issues. "No one has all the answers." We must get out of the "us vs. them" way of operating. Security awareness people are the channel for communication at the sites.

DOE will set policy through its orders and directives. These will be implemented by the NNSA according to what is required in the field. It is the NNSA's intention that site implementation will be generated by site federal and contractor employees. The NNSA is also committed to having a chain of command in place and a reporting structure for contractors to do their jobs.

Although the FY 2001 budget is limited, FY 2002 will have more funds available for security education and awareness activity. Mr. Todd encouraged the sharing of security awareness program resources, which is cost effective. Events such as this workshop foster such an exchange. He would like to see improved communication up and down the chain.

Mr. Todd shared his goal that every security professional should take one security course a year for the next five years. If that could be achieved, the department would have people who are trained in various disciplines. Many veteran security professionals are retiring in the near future, and this anticipated loss of talent makes increased training and cross training essential.

The NNSA is working to implement ISSM, a program in which security awareness will play an essential role. Mr. Todd believes that security education and awareness must focus first on the employee. He indicated that ISSM should be operational in 2002.

Counterintelligence (CI) Training

Tod Brown, Director of Training Programs, Office of Counterintelligence (CN-1), discussed foreign intelligence and DOE. He said the office is committed to a multi-channel communication effort so that people can become aware of the foreign

intelligence threat and know how to handle it. The office is also building a comprehensive CI training program.

Threats are real. Awareness programs will not work unless we get real threat information. Threats include: Internet computer intrusions, foreign travel threats, economic espionage, and collection of information by foreign governments through elicitation and solicitation.

Security officers and awareness coordinators should have periodic security briefings on intelligence information. CI staff at the sites are being trained to understand the threat and convey this to the coordinators and others. Human resources personnel need to know the threat to be able to recognize circumstances of potential danger. The National Security Council is requiring foreign intelligence threat briefings to be given to the broader population by 2003.

A communications assessment completed by CN-1 has established a baseline of awareness efforts and needs. Some initiatives completed or planned include:

- CI Training Academy (CITA) for professional development through the Nonproliferation and National Security Institute (NNSI)
- CI module for the Annual Security Awareness Refresher Briefing
- CI tool kit—standard support material for briefings
- Speakers Bureau—experts who speak to the threat
- CI Awareness Guide—a public access Web site (accessed through NNSI)

Mr. Brown stressed that world-class science and security need to co-exist. Security and CI must re-educate a new generation of scientists developing new technologies. The CITA will feature awareness seminars. Mr. Brown noted that when a former KGB general talks to the scientists about security, they listen!

Increasing Risk of IAEA Presence at DOE Sites

Joe Rivers of SO-21's Nonproliferation Support Program discussed on-site inspections by the International Atomic Energy Agency (IAEA). Background: The IAEA supports global controls of fissile materials and works to promote openness in U.S. defense and dismantlement activities. It also encourages other countries (e.g., Russia) to improve nuclear controls.

In 1996, a trilateral initiative was established by the U.S., Russia, and the IAEA allowing the IAEA to verify weapon-origin fissile material. This agreement complements a U.S./Russia bilateral transparency and irreversibility (of nuclear arms reduction) commitment. To ensure "transparency" on the part of both the U.S. and Russia, the IAEA visits nuclear sites to see that each side is reporting accurately the type and quantity of material at the site. IAEA verification follows materials from storage through conversion and disposition. The IAEA must be able to draw independent conclusions, authenticate information, and resolve anomalies. Site security awareness personnel become involved because these visits require briefings and escorting.

Currently, four DOE facilities are visited by the IAEA: the Oak Ridge Y-12 Plant, Rocky Flats, Hanford, and Idaho. Future inspections are planned for the Savannah River Site's K-Reactor and Actinide Packaging and Storage Facility, among others.

Classified Matter Protection and Control (CMPC)

Ray Holmer, Program Manager for Technical and Operations Security, SO-21, said that classified information is difficult to fully protect given that individuals can carry this information in their heads. However, a CMPC program can be successfully carried out when individuals understand why information needs protecting and are given procedures to follow.

According to Mr. Holmer, security awareness is the only way to reach the many people who have a clearance and who must follow CMPC requirements. He says we must "market" CMPC policy and awareness at both the personal and the corporate level.

The forthcoming CMPC manual combines the old manual and guide into a single document. Some CMPC policy changes are:

- Top Secret is accountable.
- Receipts are required for Top Secret (TS) and Secret (S) that are hand-carried outside a facility.
- Inventories of hand-carried TS and S will be conducted upon return to the originating site.
- The period of time for "classified matter in use" has been reduced to 1 hour.
- The "classified matter in use" policy cannot be implemented for use in a vault or vault-type room.
- Combinations and passwords are classified and marked to highest classification level and category of contents of the safe/computer.

Mr. Holmer said that the Office of Defense Programs (DP-43) is working on a Nuclear Weapons Data Order that will change existing Sigma categories and require Sigma markings on new documents. This will also tighten up need-to-know controls.

He also said changes are anticipated for Confidential/Foreign Government Information - Modified Handling Required (C/FGI-MOD).

Incident Reporting

Larry Wilcher, Technical and Operations Security, SO-21, stressed it is important to be aware of what is going on around you and to report an incident. Incidents have been increasing in numbers and complexity and there must be both willingness to report and a means to do so expeditiously and accurately. "We know adversaries are looking for information," Mr. Wilcher states. He goes on to say, "and when an incident occurs, we should always ask, was the action knowingly done, or willingly done? And was the person responsible for the incident aware of the rules?"

Any incident must be reported immediately to the Facility Security Officer (FSO) and the FSO must notify the oversight DOE/NNSA office. Completion of Form 471.1 will initiate an inquiry. If a violation of the law is suspected, this must be noted, along with supportive documentation.

An initial/preliminary inquiry report is due 30 working days after incident categorization; otherwise, a status report must be transmitted to SO-21 through a site's Safeguards and Security Office. The final inquiry report may take the form of a simple DOE F 5639.3 or it may be a comprehensive report with numerous attachments (for significant incidents).

The Incident Tracking and Analysis Center (ITAC) provides security incident data collection and analysis; for example, is there a circumstance that has led to an incident? ITAC also does individual case analysis and provides field feedback and assistance. The center is supported by the NNSI. More than 500 incidents a year are entered into the database. Mr. Wilcher showed several charts that give a trend analysis on types/categories of incidents and closure status of incidents. One chart, the Security Incidents Impact Measurement Index indicates the impact (damage) to national security or DOE security interests. Mr. Wilcher said the majority of incidents reported have been related to physical security.

A new DOE Order for Incident Reporting is pending publication. A Notice, DOE N 471.13, Reporting Incidents of Security Concern, has been signed to cancel an earlier memorandum on Reporting Security Incidents.

Safeguards and Security Inspections and Evaluation

Barry Cooksey, Office of Independent Oversight and Performance Assurance, Office of Safeguards and Security Evaluations (OA-10), talked about the organizational elements and the goals and "mindset" of the inspections program. These goals are:

- Develop relationships by providing meaningful, professional support
- Create value by being part of the solution, not the problem
- Focus on programmatic performance issues, not merely compliance
- Identify areas needing improvement

DOE O 470.2A provides policy for oversight activity. The Appraisal Process Protocols and an Inspector's Guide, among other documents, can be accessed at <http://tis.eh.doe.gov/iopa/index.html>.

Mr. Cooksey believes the inspections and evaluation (I&E) process benefits from openness and "give and take" on the part of the inspector and those being inspected. He said an inspection should have no surprise endings. Through candid and frequent communication, a survey can successfully accomplish its purpose.

During an inspection of a site's Safeguards and Security Awareness Program, the I&E team typically reviews: content of briefings, briefing attendance records, and SF-312's. Inspectors may also interview personnel, observe a briefing, review security incident

information, and give a security knowledge test/questionnaire to a selected group of personnel, often employees in high-risk programs. Mr. Cooksey believes a program's effectiveness can be measured by whether or not people can retain information. The inspections team will also look at local procedures, which if not followed, may result in a site-specific finding.

If program deficiencies are found, correction would require an action plan that includes what will be done and by what date. Mr. Cooksey believes a self-assessment is an important tool and he encourages asking tough questions internally. The team also evaluates how a site is tracking issues and is interested in seeing how lessons learned are tied back into an accountability process.

Mr. Cooksey emphasized that strong programs are proactive. He encouraged use of newsletters, poster campaigns, Web sites, and technology tools such as computer-based training. Most importantly, awareness programs benefit from the involvement of energetic, high-quality people who are dedicated to communicating an awareness message.

Briefings and Badging

Edwin Tippens, Security Administrator for the Badge and Access Office at LLNL, began with the question, "Where do briefings and badging meet?" He went on to talk about their relationship. Briefings are an essential part of the badging process and must be conducted and documented before access is allowed. The briefings and their associated access are:

- Initial—access to the site/facility
- Comprehensive—access to classified matter and information
- Refresher—continuing access

Mr. Tippens explained how continuing access works at LLNL. Employees are given a 14-month period (12 + 2) to complete a refresher briefing; after that time if the briefing has not been completed, the badge "stops" – no access is allowed. The badge access system is tied into a personnel security database. Training records and other data associated with the person may "disappear." As a result, LLNL has found that people pay attention to refresher briefing deadlines! When applicable, electronic access control is very effective in motivating individuals to complete this required briefing.

Technology is being integrated more and more into badging, and "smart card" technology can support security awareness. Under the new ISSM, for example, safety access could be tied to security access.

Open Forum

Virginia Reams, DOE Oakland Operations, and *Sylvia Lovelett*, Pantex Plant, Moderators, opened the session by having workshop participants introduce themselves. Several people said they were attending an SE SIG Workshop for the first time. A short period for questions and discussion followed.

April Stottler called attention to a CD developed by the Naval Criminal Investigative Service entitled, "Do You Know Where Your Children Have Been?" The CD deals with Internet access to child pornography and emphasizes a "safekids" and "parents posse" concept in protecting children from Internet abuses. Copies of the CD, which can be viewed on a computer with PowerPoint, were made available at the TRADEing POST.

Valerie Anderson talked about the new *Safeguards and Security Awareness Handbook*, issued in February 2001. A Special Projects Task Force made up of SE SIG Steering Committee and at-large members met in Albuquerque at the FM&T Honeywell facility in November 2000 to draft the document. The handbook was built on an earlier SE SIG document, *A Guide to Regulatory Requirements*, published in 1990. The handbook offers guidance to awareness coordinators in implementing forthcoming DOE M 470.1-1. An upcoming project for the SE SIG will be to revise an SE SIG Working Paper, *A System for Gaining Management Support for Your Security Education Program*, issued in 1992.

Tuesday, April 10

TSCM Program

Larry Kinsey, SO-21, opened the morning session with a discussion of Technical Surveillance Countermeasures (TSCM). He emphasized TSCM is a counterintelligence program with its origin in the National Security Act of 1947. A national TSCM policy, the U.S. National Security Council Policy on TSCM, was issued in 1998. Director of Central Intelligence (DCI) Procedural Guides 1, 2 and 3 provide operational directions for the TSCM Program. DOE implements the program. A revised DOE O 471.2B is expected to be issued when the HQ policy review ends.

The DOE TSCM Program objectives are:

- Detection—checking for the presence of technical surveillance devices, technical security hazards, and physical security weaknesses.
- Nullification—neutralizing or negating technical surveillance devices and soundproofing sensitive areas such as walls, floors and air ducts.
- Isolation—establishing special areas for the conduct of classified/sensitive activities, which deter the use of surveillance devices.
- Education—making people aware of the technical surveillance threat through briefings, workshops, and staff meetings.

At DOE sites, a TSCM Operations Manager (TSCMOM) manages the program and directs TSCM teams. The Director of Safeguards and Security identifies areas/ facilities for the TSCM services. The TSCMOM develops supplemental directives and is responsible for a TSCM awareness and threat briefing program for the site.

TSCM activities include: surveys, inspections, monitoring, advice and assistance, preconstruction services, and special services. DOE uses a minimum of two people on a team for surveys. Mr. Kinsey said DOE was first to certify TSCM technicians.

Operations Security (OPSEC)

JoAnn Archuleta, Director of the new Foreign Interaction Training Academy (FITA) at the NNSI and senior instructor for information security, talked about the role of OPSEC in the workplace. She emphasized that we would do well to be attentive to detail and watch what is going on around us. And if you are a scientist in a laboratory, or a worker handling classified or unclassified controlled information, it may be that someone is watching you.

Ms. Archuleta describes OPSEC as a process that involves:

1. Identification of critical information at a laboratory or work site. A site's OPSEC Working Group can assist with this.
2. Analysis of threats. OPSEC is threat-driven. Adversaries will want information that is useful to them.
3. Analysis of vulnerabilities. We must always ask, What information do we have of intelligence value that is collectible and observable?
4. Assessment of risks. We must know how much risk is acceptable and the consequences of loss. We are all decision-makers, responsible for protecting the work that we do. An OPSEC Working Group will support us.
5. Application of countermeasures. Practicing good OPSEC can ensure that random bits of information collected by adversaries are of low value. Systematic collection is difficult and costly. OPSEC countermeasures frustrate intelligence collection to the point that it operates slowly and expensively and is not worth the cost.

A high percentage of recommended countermeasures involve OPSEC awareness. In fact, awareness is the Number 1 OPSEC countermeasure. Ms. Archuleta encouraged the use of OPSEC briefings, which are available through the NNSI.

What's New at ISOO?

Emily Hickey, Program Analyst in the Information Security Oversight Office (ISOO), presented an update on ISOO activity. ISOO is part of the National Archives and Records Administration (NARA). NARA receives policy and program guidance from the National Security Council (NSC).

ISOO oversees the security classification programs of both government and industry. The office recently issued a revised *Classified Information Nondisclosure Agreement*, Standard Form 312 (Rev. 1-00). In addition, ISOO reprinted the SF-312 Briefing Booklet in January 2001. Ms. Hickey provided copies of the booklet for the TRADEing POST. The form and the Briefing Booklet are available from ISOO. An electronic copy of the 312 is also available as a pdf file (see Internet address for ISOO below). The old SF-312 will be good only through June 30, 2001.

Two recent directives applicable to national security decisions and activities are the Public Interest Declassification Act of 1999 and the National Security Policy Directive (NSPD), signed by President Bush on February 13, 2001. The NSPD governs foreign

affairs and consolidates several policy measures. The Public Interest Declassification Act establishes a Public Interest Declassification Board that includes the ISOO Director as Executive Secretary. This directive, along with other congressional documents, can be read at www.fas.org/sgp/congress/.

Ms. Hickey discussed E.O. 13142, which amends E.O.12958. She emphasized this amendment does NOT end automatic declassification, expand the 25-year rule, change exemption standards, affect approved files series exemptions, or change declassification policy. However, several new requirements are part of this amendment. The amendment may be accessed at www.fas.org/sgp/isoo.

Ms. Hickey said that the current Security Policy Board will be disbanded and the work redistributed among other entities.

National Counterintelligence Center (NACIC)/ Office of the National Counterintelligence Executive (NCIX)

Stephen Argubright presented an overview of NACIC in transition. NACIC has evolved into a new organization with a new name and new seal: the Office of the National Counterintelligence Executive. The office is co-located with the Central Intelligence Agency (CIA) in Langley, Virginia.

NCIX support activities will include regional seminars, a quarterly newsletter, training videos, security awareness material, some of which are travel and business brochures, and posters. NCIX has an Internet site that provides CI Update Advisories and also supports the Extranet for Security Professionals (ESP) Web site: xsp.org. Mr. Argubright encouraged workshop attendees to consider becoming a part of the ESP. This is a private communications Web site that is cleared for For Official Use Only/Official Use Only (FOUO/OUO) communications. NACIC/NCIX also writes an *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Copies of the report for the Year 2000 were provided for the TRADEing POST.

In an effort to move counterintelligence from reactive mode to proactive mode, Presidential Directive Document (PDD)-57 was signed December 28, 2000. A hallmark of the document is a section on "Interaction with the Private Sector." In addition, a CI-21 Task Force was formed to meet 21st Century challenges. The Task Force is made up of a Board of Directors, including a Chair from the FBI; the Deputy Secretary of Defense; the Deputy Director of Central Intelligence; a senior representative from the Department of Justice; the National CI Executive (an individual); and NCIX.

Mr. Argubright showed a new video, "Insider Betrayal," on espionage activity. The video features stories of spies and case studies, such as the Avery Dennison case. Mr. Argubright noted that Robert Hanssen, the FBI agent charged with espionage, has allegedly done extremely grave damage to our national security—far greater than anyone could have imagined. The damage from activities of some of the other convicted spies pales in comparison.

Sources for additional information (videos) on counterintelligence are:
National Reconnaissance Office (NRO)

"In the Public Domain"

"Bad Characters"

Mickey Anderson, POC, 703-808-3750

Defense Intelligence Agency (DIA), <http://www.dia.mil/>

"Expect the Unexpected–Defensive Tactics for a Safe Trip"

Mary Jo Bennett, POC, 703-907-1572

Interagency OPSEC Support Staff (IOSS), <http://www.iooss.gov/>

"Awareness 2001"

Mary Peters, POC, 301-981-0323

Foreign Visits and Assignments Program

Greg Pruitt, Office of Foreign Visits and Assignments (SO-24), cited the June 1999 President's Foreign Intelligence Advisory Board (PFIAB) Report ("Science at its Best; Security at its Worst"), which presents the need to balance science and security. The "balance" theme was reiterated in a National Academy of Sciences workshop, "Scientific Communication and National Security," October 2000, and in a Center for Strategic and International Studies Review (initial review) chaired by John Hamre, January 2001. Mr. Pruitt said DOE is at the "cutting edge" of where the balance needs to be defined.

The Foreign Visits and Assignments Program has two distinct missions: 1) supporting the DOE mission to enhance the "collective science" of the United States within a framework that ensures protection for national security, and 2) supporting the SO-24 mission to enhance science and protect national security in a balanced approach.

Currently, the program operates under DOE P 142.1 (to be replaced by an order) and DOE N 142.1 (to be replaced by a manual). With new policy, a graded approach will be put into place, as "one size does not fit all." The program has a goal to increase communication and awareness at the sites. Older scientists are being recruited at sites to talk to the younger scientists who have little knowledge of Cold War conditions.

Mr. Pruitt discussed the Foreign Access Central Tracking System (FACTS), a centralized knowledge repository to process site access by foreign visitors. Approximately 1300 new records are entered every month and an average of 650 indices checks are done. Sensitive Countries are automatically flagged by FACTS. A new order and manual is forthcoming that will govern FACTS operations. Also, plans are under way to connect FACTS with other agencies, such as State, Commerce, DoD, and NASA. Mr. Pruitt said that DOE is "in the forefront" of accountability for foreign visits.

The newly established Foreign Interaction Training Academy at the NNSI will offer job task analysis training and awareness seminars. Mr. Pruitt anticipates that FITA will begin formal instruction in the Year 2002.

Personnel Security Activities

Lynn Gebrowsky, Program Manager for Personnel Security Policy, SO-21, gave an update on personnel security directives—orders, notices, and guides that are undergoing a security policy review. Rulemaking is not affected by the policy hiatus. Notices for Rulemaking can be found on the NARA Web site. A summary status follows:

- DOE O 470.1, Chapter IV, S&S Awareness Program, is currently in draft. When the security policy hiatus ends, the order can be finalized and submitted to RevCom.
- DOE M 470.1-X is in the comment resolution process. Once the order is issued, the manual can follow.
- DOE O 472.1B is undergoing revision with a formal draft not yet published.
- DOE M 472.1-1A is ready for issuance once policy review ends. NNSA applicability has been added.
- DOE M 472.1-1X is in process of being written. The new manual will address how interim access authorizations can be used. Also, it will reflect changes in FBI investigations due to the National Defense Authorization Act of 2001.
- 10 CFR 710, Subpart A, "...Determining Eligibility for Access..." has been revised and is moving forward for publication as a final rule. Changes applicable to the denying or revoking of clearances have been made to respond to E.O. 12968.

The Clearance Verification System (CVS) is used to process visitors to the DOE sites. Information in the Joint Personnel Adjudication System—also used for DoD and other agencies—is made available to CVS. The Security/Suitability Investigations Index is linked, as well, to the CVS, which serves as a central database for verifying and clearing visitors.

The department holds 110,000 Q and L clearances, 80 percent of which are for contractors. Although an effort remains to hold clearances to a minimum, the office has seen an increase in clearance activity because area access authorization requirements are being supported by Congress. Reinvestigations, which are measurable, are proceeding according to schedule.

Linda Repass, Program Manager for the Personnel Security Assurance Program (PSAP), discussed the new Human Reliability Program (HRP), which will replace/unify the Personnel Assurance Program (PAP) and PSAP. New policy under 10 CFR 712 is going forward with a Notice of Proposed Rulemaking to be published in the Federal Register. Public hearings will be held at selected sites.

Ms. Repass described the current PAP and PSAP programs. Historically, PAP has been mostly a safety program and PSAP a security program. Parts of each program will be incorporated into the new HRP.

Requirements common to both PAP and PSAP that will carry over to the HRP:

- Drug testing. A random unannounced drug test is administered at least once every 12 months. Also, drugs tests are conducted for reasonable suspicion and following an occurrence.
- Counterintelligence scope polygraph examination. Individuals are requested to submit to a counterintelligence polygraph in accordance with the Polygraph Examination Regulation, 10 CFR Part 709.

PAP requirements that will carry over to the HRP:

- Eight-hour abstinence rule for alcohol. Individuals who are scheduled for nuclear explosive duties and individuals in specific (designated) positions are prohibited from drinking alcohol in the eight hours before a work assignment.
- Psychological evaluations. Individuals are given a psychological test the first year and every third year. A semi-structured interview will be conducted annually as part of the medical assessment.

PSAP requirement that will carry over to the HRP:

- Annual submission of the Questionnaire for National Security Positions (QNSP), Part 2. This yearly requirement will assist in assuring that HRP-certified individuals are reliable and trustworthy.

New requirement for the HRP:

- Random alcohol testing for all. A random unannounced alcohol test will be administered at least once every 12 months.

Training will be an integral part of the new program and will be developed and conducted for employees, supervisors, managers, and administrators. Once the new policy is issued, there will be a 9-month implementation period for the program.

Classification and Security, a Partnership?

Cathy Maus, Office of Nuclear and National Security Information (SO-22), makes the case that classification and security are indeed a partnership. By definition, classification is the process of identifying the information to be protected in the interest of national security.

Ms. Maus stressed, "If you can't identify it, you can't protect it." But it seems as though classification and security remain separate, with separate orders and sometimes no obvious organizational linkage. Historically, the two have been under different organizations; however, since 1955, the HQ Security and Classification policy organizations have been co-located, and these two organizations are co-located at several sites. Functionally, the two need to be linked, she said.

Ms. Maus talked about classification-rooted security problems that result in infractions. One group of infractions stems from a misunderstanding of the GEN-16, DOE's No Comment Policy, and another from publication of papers with classified information that did not receive proper review by an authorized derivative classifier (ADC) before

publication. Persons generating information need to be aware of classification by compilation/association and that information found in the public domain is not automatically declassified. Also, different sections of a paper can have multiple authors and not receive complete and consistent ADC review. Careful and systematic review of all information is necessary when documents are to be released to the public or disseminated internally, as well.

An awareness program will reach people who generate classified material. Classification information is included in the comprehensive security briefing and is often a part of the annual security refresher briefing. A site's Classification Officer can provide input to the briefings, perhaps with a dedicated block of briefing time, or, at a minimum, provide classification material for the awareness coordinators.

Executive Order 12958, the implementing directive, identifies specific classification areas that must be included in a comprehensive briefing. These are:

- What classified information is and why it's important to protect it.
- Responsibilities of individuals who create classified information.
- Levels of classified information and the damage criteria associated with each level.
- General requirements for declassifying information.
- Procedures for challenging the classification status of information.

In addition, a comprehensive briefing should cover the three categories of classified information along with their definitions. Ms. Maus also suggests talking about DOE's No Comment Policy, classification review requirements, and compilations/associations.

In closing, Ms. Maus emphasized that if a partnership between classification and security exists at a site, "work to strengthen it; and if the partnership doesn't exist, pursue it. We're all in the business of protecting national security."

De-Mystifying "Sigma" Information

Marvin Thompson, Classification Officer, Pantex Plant, and *Thomas Cousins*, Office of Defense Programs (DP-43), briefed the group on DOE's Sigma Program that concerns proper access to nuclear weapon data. This data is always Restricted Data (RD) or Formerly Restricted Data (FRD). Sigma markings are not classification categories or levels; rather, they are designations that restrict access, much like other caveats (e.g., FGI, NoForn, SAP). The markings serve to limit access and dissemination of specific types of data to persons with an established need-to-know and the required clearance level for the information.

Currently, there are 12 Sigma categories, although historically as many as 18 existed. The draft of a revision of the Nuclear Weapon Data Order adds one new Sigma and consolidates the existing 12 into 8 for a total of 9 Sigma categories.

For Sigma access, DOE F 5631.20 will continue to be used for federal employees and contractors. Any visit/access is recorded in the Weapon Data Access Control System. Weapon data can be transmitted via a classified mail channel registered in the Safeguards and Security Information Management System (SSIMS). A new process is being established whereby a Statement of Security Assurance (form) must be completed before information can be authorized for transmittal in SSIMS.

Tools of the TRADE

This segment of the workshop offered opportunity for sites to talk about and demonstrate their awareness programs. Representatives from three DOE sites gave presentations that showed how varied approaches can be used successfully in getting across a security message. Security educators have many types of audiences to reach.

Sylvia Lovelett, Pantex Plant, showed a video of past refresher briefings from Pantex. In preparing a briefing, she emphasized that the question should always be asked, what information can people retain? The content of an annual refresher should address any immediate security needs of the site as well as remind individuals of their ongoing security responsibilities. The Pantex Plant documents briefings using a tracking system tied into access control. The 2001 refresher briefing has the theme, "Who Wants to Be Security Conscious," based on "Who Wants to Be a Millionaire." Feedback has shown the game to be both entertaining and informative. A study guide was handed out prior to the briefing covering questions that would be asked.

Chet Braswell, Hanford, *Ann Czebotar*, PNNL, and *Bonnie Harris*, Richland Operations, introduced "Security Ed," a cartoon character who finds himself involved with security problems and resolutions. Ed is an evolving character (he could be any site employee). He sits in a chair in front of a computer and has access to the site's latest security "concerns," which he feels free to comment on. Ed is becoming a regular feature of Hanford's security newsletter, also available to Richland Operations and some parts of PNNL. "Security Ed" is the product of the Hanford Security Awareness Council, which meets once a month and decides what issues Ed should deal with next. A "Security Ed" video is in progress.

Clarice Bruce, and *Courtney Lebya*, Rocky Flats, talked about their site's awareness program and demonstrated a game they developed for the 2001 refresher briefing. Security Awareness Trivia uses software featuring the character, "Al Morale." Al is a game show presenter. For the Trivia game briefing, site employees are given handouts of information to read to prepare for the game with questions taken from the handouts. Using Game Show Presenter software, questions for the briefing can be changed as required. Feedback has been very positive and shows that security messages can reach people effectively through the use of cartoon characters. Information on the software is available from the Rocky Flats Safeguards and Security organization.

Wednesday, April 11
"Identity Theft"

Cindy Farinholt and *Wayne Morris*, Nevada Operations, shared a security video that was developed in-house by the Safeguards and Security organization. This video on the subject of stolen identity brings to light how important it is to protect personal information, such as credit cards, a driver's license, bank account numbers, and even a car registration number. In recent years there has been alarming loss of people's "identity" because of the ease by which an unknown person can take and use someone else's personal information.

The message is clear. We must know what to protect and become conscious of who might have access to personal data. Missing credit cards should be reported immediately and a police report filed. When using fax machines, cellular and cordless phones, email, etc., we must recognize these are susceptible to interception.

Become OPSEC Aware! OPSEC is a five-step process that:

1. Identifies critical information to be protected.
2. Analyzes the threats. OPSEC is threat-driven. Know who might want the information.
3. Analyzes vulnerabilities. What information has intelligence value that is collectible and observable?
4. Assesses the risks. Know how much risk is acceptable and the consequences of loss.
5. Applies countermeasures. Practice good OPSEC, which can help ensure any information collected is of low value. Systematic collection is difficult and costly. OPSEC countermeasures slow things down to the point that collecting information is not worth the cost.

A short video based on the movie, "Home Alone," showed how would-be thieves can be foiled through the practice of good OPSEC. Nevada Operations, Office of Safeguards and Security, also produced this entertaining video.

Cyber Security Program Activities

John Przynucha, Acting Associate CIO for Cyber Security (SO-33), discussed DOE computer security policy, which, he said, is evolving. The Cyber Security Action Plan II, "Achieving Success Through Risk Management," will address: policy, planning, and performance; training, education, and awareness; engineering and assessments; and research and development. The Office of Cyber Security has issued 20 policy-related documents since 1999. Eighty-seven cyber security program plans have been reviewed. The office is gearing up for a complete remake of cyber security policy.

A new order will incorporate roles and responsibilities for the HQ program office and will be focused on high-level accountability for cyber security. The requirements will flow down to operations offices and sites.

Mr. Przysucha believes that policy and procedures fall short today on management accountability in accepting risk and making decisions involving risk. New policy will need to address risk assessments and appropriate countermeasures, he said. The policy to be developed will also cover personal electronic devices (PED) such as cell phones with Internet access and laptops with infrared transmission capabilities. Mr. Przysucha believes that PEDs must be restricted in some way, but not necessarily prohibited. Development of a national policy for PED regulation should be undertaken.

Headquarters would also like to bring classified and unclassified security together in one plan, each addressed in a separate section, to include commonality of terms.

Training goals include awareness training for systems administrators, senior management, and line management. Measuring the effectiveness of the training and reassessment will be important components of this training. Mr. Przysucha says there is a need to develop training for Help Desk personnel. A DOE-wide training conference to be held in Cincinnati will address training needs for cyber security. A number of courses have already been identified and are available.

In the near-term, the program office plans to work toward reestablishing credibility of the Computer Incident Advisory Center (CIAC). Penetration tests show much progress has been made in protecting classified information, and CIAC will be part of the new defensive policy.

Mr. Przysucha says that oversight and audit activity is increasing. Providing rapid and responsive training programs will be the key to success in maintaining computer security.

Security Videos

Trent Olaveson, Sandia - Livermore, showed a video produced by the National Reconnaissance Office on "infrastructure security" that includes the protection of computer networks and wireless phone systems. The video carries a strong message that a company's management system is vulnerable, and access to sensitive information is often facilitated by file sharing, reprogramming phones, etc. Careless use of infrared and wireless devices leads to stealing of files. People using the system are the problem—not simply the technology.

Kelvin May, Kansas City Plant, talked about how the plant's Safeguards and Security organization promotes awareness. A series of security videos produced in-house features the character, "Jim Leak," an engineer who works in a classified area. Kelvin showed a video that had clips of Security Awareness Week activities and an interview with the actor who played the role of "Jim Leak." Kansas City was notified it has received an OPSEC National Award in the multimedia category for the "Jim Leak" video series. Winners of the award are selected from sites throughout DOE, DoD, and private industry. The award will be presented at the national conference in Tampa, Florida in June 2001.

Chet Braswell, Hanford, showed a video that was developed by students as an awareness tool to help prevent school shootings and other violence. The video has ramifications for

workplace violence and disgruntled employees. An organization called Student Crime Stoppers produced this video, "Choose to Trust," which dramatizes the story of two troubled teens. Endorsed by students and teachers, the video portrays a realistic approach to helping persons recognize and consider the consequences of remaining silent.

Security Awareness Coordinators Training/CTA

Rob Ambrose, NNSI, presented an overview of the CTA and upcoming training opportunities. The Safeguards and Security Training Academy offers a Security Awareness Coordinators course in addition to several security-related courses, such as Incident Reporting and CMPC. The Coordinators course is scheduled for the week of July 16, 2001. Persons can register on the Web or with their site's CTA point of contact.

New CTA initiatives include:

Establishment of the Foreign Interaction Training Academy and a Department of State Antiterrorism Assistance Program, offering specialized training for foreign police who protect embassies.

Mr. Ambrose talked about Personnel Security Awareness, stressing four points to be included in briefings:

1. Understand why clearances are required for certain access.
2. Know reporting requirements. (Different reporting procedures may be in place for DOE vs. corporate reporting and individual vs. supervisor/contractor reporting.)
3. Know what constitutes a security risk (e.g., susceptibility to blackmail as reflected by financial irresponsibility).
4. Know how to avoid security risk.

The 2001 Safeguards and Security Awareness Refresher Briefing is being offered on the Web with an option for sites to download the briefing and make it site-specific. A different approach will be explored for the 2002 annual refresher, perhaps developing stand-alone modules on various security topics that sites can use "as is" or adapt.

SSAQP/SE SIG Steering Committee Meeting

The Safeguards and Security Awareness Quality Panel and the SE SIG Steering Committee held a joint meeting following the workshop. Minutes of the meeting will be available on the NNSI Web site.