

# OIO Panel Discussion 2008 SASIG Workshop

## Site Responses to Questions for OIO Panel

1. How do you develop/conduct a self-assessment of your program? Do you use checklists? Develop and track corrective action plans?	
Fran Armijo Sandia-NM	We have an Assurance Department that works with us on self-assessments. These forms are on the website: A self-assessment report template, a self-assessment finding form, self-assessment scoping guidelines and self-assessment plan template.
Nancy Cross Y-12 National Security Complex	We take the DOE directives to evaluate our compliance with the requirements. We conduct self assessments of the Security Awareness program here at Y-12. We use checklists and have them in an appendix. The self assessments at Y-12 are given a number, and, if there are issues identified, a comprehensive correction plan is developed and tracked. To request an example of one of our self assessments, send an e-mail to crossn@y12.doe.gov.
Scott Colonese LLNL	To conduct an assessment the following occurs: an assessment team assembles, resources and logistics are identified, assessment method (topical, management, etc.) is determined, assessment schedule is created, organization is notified, and a checklist is created. Information is gathered from one/many of the following: a compliance checklist, interviewing individuals, or observation of the work activities (surveillance). All assessments are tracked in our local Issue Tracking System (ITS). If any deficiencies or observations are noted they must be tracked and marked in ITS. All Corrective Action Plans (CAPs) include a measure to correct the deficiency. To close a CAP the issue/deficiency must be resolved. Standard forms are used for each process/step.
Sylvia Lovelett Pantex	Develop Self Assessment: Management Selects the Topical Area/Subject and assigns the self-assessment to an individual or group of people using the "ESTARS" tracking system. The "ESTARS" task will contain: task number (i.e. PANTEX-PER-2008-0021); subject; assigned by; assigned due date; deliverable; task instructions; routing instructions; individual instructions (if required); attachments; and comments.  Conduct Self-Assessment: Individual/group acknowledges the self-assessment task, and a plan is developed to conduct the self-assessment. Once the self-assessment is completed and approved by management, it is closed in "ESTARS." Any findings or corrective actions are assigned and tracked using the "ESTARS" tracking system.
Chet Braswell Flour Hanford	We use an internal audit team to conduct audits. We also conduct self assessments. We use both a checklist and the DOE Inspectors Guide (July 04). If a problem is found we create a corrective action plan with due dates. The corrective action plan is monitored by internal audits.
Kristine Inskeep INL	We were given a checklist from our S&S to review our procedures (MCP & LWP) with the program. We used the DOE M 470.4-1 section K to measure our briefings, activities and storage requirements.

## OIO Panel Discussion 2008 SASIG Workshop

2. What questions are on your required security awareness test/questionnaire?	
Fran Armijo Sandia-NM	<p>Initial: No questions. However, every section of the video starts off with a heading of the content required in DOE 470.4-1. For instance, one section starts off with “Access Control,” and we talk about access control; another “Escort Procedures,” and we talk about escort procedures.</p> <p>Annual: With 12,500 cleared people I have to do something to make them respond on time. We have eliminated test questions at the end of the course. At the beginning of each module, I state the objective of the module. At the end of each module is a question directly related to the objective. Respondents are simply asked to acknowledge that they’ve read the contents and completed the practice questions.</p> <p>Comprehensive: Based on a recent audit of one of our remote sites we found that not all the required contents were being addressed. So, in the 2008 version of the Comprehensive Briefing, we not only made sure we’ve addressed the content, but every question at the end of the booklet is directly tied to that required content. There are a few additional questions. For instance, one question addresses OPSEC, another Protective Force, another Foreign Travel, etc.</p> <p>Termination: No questions. They either view the video and have the “acknowledgement” automatically recorded in our training database or they sign a form acknowledging they understand their responsibilities.</p>
Nancy Cross Y-12 National Security Complex	We do not have a required security awareness test/questionnaire. We have an interactive Initial and Comprehensive Briefings. We ask questions to access awareness knowledge and have used a knowledge questionnaire as an awareness assessment.
Scott Colonese LLNL	Please see attached questionnaire.
Sylvia Lovelett Pantex	Security test questions were created based on information taught in the Initial, Comprehensive or Annual Briefing. The recommended test questions were sent to HQ, and HQ made revisions to test questions. Test questions were sent to 600 randomly selected “Q” cleared employees.
Chet Braswell Flour Hanford	These change each time. Some are from recent lesson plans. During the last OA audit we used questions from our weekly security awareness contest.
Kristine Inskeep INL	I had contacted Oak Ridge, and they sent their questionnaire, which tailored to our facility. Because many of the questions were pertinent to the INL, we only had to develop about 15. We took these questions from our Refresher briefing test. Time frame is critical—we had low participation because we sent out our questionnaire on a week with a holiday weekend. We had to petition for an extension to have employees take it the next week.

## OIO Panel Discussion 2008 SASIG Workshop

<b>3. How do you meet time requirements for the Refresher Briefing and ensure compliance from contractors/subcontractors?</b>	
Fran Armijo Sandia-NM	<p>If individuals fail to take their Refresher on the required date, the badge is automatically disabled, and it is not enabled until 24 hours after they've taken the Refresher. We sometimes make exceptions for people on military or medical leave. Very few people at our site are out of compliance. When an individual is more than 14 working days out of compliance, a message is sent to his or her Sandia management stating that after 90 calendar days the individual's clearance will be terminated. Since we implemented this practice and removed test questions at the end of the briefing, response has been great. We have maybe four people out of compliance this month.</p>
Nancy Cross Y-12 National Security Complex	<p>We have an Electronic Briefing Registration System in place that individuals use to sign up for the Initial or Comprehensive Security Briefing. The person attending the briefing fills out the Y-12 Briefing Attendance Form. We enter the pertinent information from that form into the briefing system, and this information downloads into the Y-12 training system (SAP), which tracks when that person is due for the Refresher.</p> <p>If the Refresher Briefing (RB) is not taken within a 12-month period, the person will be deficient. Cleared and uncleared employees and subcontractors are required to complete the RB annually. The RB is a STAR requirement here at Y-12, so if the RB is not taken within that time frame, access is denied to the plant, and the individual will have to go to Visitor Control and take the RB before having access. This works well because access to the plant is denied until the individual is compliant.</p>
Scott Colonese LLNL	<p>We badge all non-employees for one year. When they are issued a badge, they must read and sign the Refresher to get re-badged.</p>
Sylvia Lovelett Pantex	<p>All training, whether contractor/subcontractor, is maintained and tracked by Technical Training using the Plateau Learning Management System. Division Training Coordinators assign curriculum codes based on job requirements. Monthly reports are generated to resolve any training deficiency. Employees are contacted if training deficiencies are identified.</p>
Chet Braswell Flour Hanford	<p>Retraining is conducted via computer and throughout the year. Training is monitored by Site Training Records with a daily feed to the Personnel Security database. We have local agreement with DOE that training is due at approximate 12-month intervals. We do not list anyone as actually past due until 13 months. With the databases tied together, we send auto e-mails to the people who are 12 months and 10 days past due. The e-mail goes to the employee and to his or her manager. If the employee is 12 months and 20 days past due, the Security Awareness Coordinator calls the manager. We have a very high completion rate, typically at 99.8 percent, of taking the training before the thirteenth month. Subcontractors are treated the same as employees on notification, but use the Site Procurement Office to forward the messages and ensure compliance. All subcontractors wear a Site Specific Badge with a 12-month expiration date. We will not re-badge until Site Procurement approves and the person completes the Security Refresher plus all the annual Site Safety Training.</p>
Kristine Inskeep INL	<p>We annually review our briefings 90 days prior to the 12-month due date. Most of the time this works great, but over the course of the eight years I have been in this position, we have slid the date to 6 months different than when I started.</p> <p>We have a Qual that is associated with their access using their badge, and access is denied if they have not completed the ES&amp;H and Security Briefing in the required time. We also flag their badging record so they can not get a new badge until the training is completed.</p>

## OIO Panel Discussion 2008 SASIG Workshop

4. How do you ensure that SF-312 requirements are being met (signing, witnessing, storage)?	
Fran Armijo Sandia-NM	The Clearance Office sends us a list of all new, reinstates, extensions, and transfers. We inform the Office about who has to attend the live briefing and who can read the booklet. Persons attending the class receive a certificate. The student takes that certificate and the unsigned SF-312 in the booklet to the badge office where it is witnessed and kept for our Records Management Department to pick up and store, plus a copy is scanned for our Metagroup (quick access). If the individual has to read a booklet, they review it there at the badge office and again sign the SF-312 in front of the clerk in the badge office. Remote sites are a little different and handled on case-by-case basis.
Nancy Cross Y-12 National Security Complex	Regarding SF-312 requirements, we have employees and subcontractors who attend the Comprehensive Security Briefing. After fully understanding their responsibilities regarding the SF-312, they sign the SF-312; the Security Awareness Specialists Witness and Accept the SF-312. This list is updated as needed and is available if auditors request it. We have a list of those who have Authority to Witness and Accept the SF-312, and it is signed by the Assistant Manager for S&S Y-12 Site Office. The active original or legally enforceable facsimile SF-312s are maintained by the Security Awareness Office. When the security clearance is terminated, the SF-312s are sent to the NNSA Y-12 Site Office where they are retained. They can be expeditiously retrieved if the U.S. Government seeks reinforcement or for audit purposes.
Scott Colonese LLNL	Prior to individuals receiving a clearance badge they must sign the SF-312. They are required to sign the SF-312 at the time of their Comprehensive Briefing. Individuals who have authority to witness the SF-312 have been approved by our Local Site Office. Security maintains personnel files where these are kept.
Sylvia Lovelett Pantex	Once an employee has completed the Comprehensive Briefing, the following steps are taken to retain the SF-312s: (1) Employee receives a grant sheet showing an access authorization (clearance) has been granted. (2) A Comprehensive Briefing is scheduled; upon completion of the briefing employee signs the SF-312 which is witnessed by the Security Coordinator. (3) Security Coordinator signs the SF-312 and forwards it to DOE-NNSA Security for acceptance. (4) DOE-NNSA returns the approved SF-312 and it is placed in each employee's security file that is maintained by Access Control. (5) Once an employee terminates, Access Control conducts a termination briefing. (6) Employees re-sign the SF-312 representing acceptance of the debriefing. (7) The signed SF-312 is returned to DOE-NNSA for retention/storage.
Chet Braswell Flour Hanford	The badging office cannot issue a badge with an Access Authorization until the security instructor enters a "Good to Go Button" indicating the SF-312 was completed and the student attended the Comprehensive Security Briefing. Badging does not have the ability to override. Anyone can witness the SF-312, but only the Contractor Security Awareness Coordinator has authority in writing to accept it. We store the SF-312 separate from the personnel files. Random spot audits are performed yearly, and a 100 percent inventory is conducted every five years. Each month all terminated files are forwarded to the DOE office.
Kristine Inskeep INL	I, as SA coordinator, or the badging office have a process of signing the SF-312 prior to picking up the new badge. We can put comments in the badging record to notify the badging personnel that they cannot issue a badge without permission from me or my backup. We have designated personnel who have been given the task of witnessing the signing. This list is sent to DOE-ID and approved to make sure no unauthorized personnel perform the function. Our working process (LWP-11106) explains the steps for notifying, signing, copy for file, and sending original to the DOE-ID office.

## OIO Panel Discussion 2008 SASIG Workshop

5. What is your process for developing and conducting Termination Briefings?	
Fran Armijo Sandia-NM	<p>Based on a self-assessment of the Clearance Office, it hasn't been all good. Good portion—we have a Web-based course for terminations. The individual who has access to our internal website can view the video, get a certificate, and take it to the Clearance Office. If the individual does not have the certificate, the Clearance Office can check the corporate training records for verification. If the person has not seen the video, the clerk will require the person to either view the video or sign the Termination Briefing form. The Clearance Office then forwards that information on to us.</p> <p>The problem—contractors and consultants: The Clearance Office has been very good about forwarding Termination Briefing forms for contractors and consultants when the forms are received through the mail. However, we don't know about those who terminated and never took the briefing. The Clearance Office notifies us when a clearance is terminated—period. If we don't receive a Termination Briefing form or some communication from the contractor/consultant that the briefing has been completed, we will actively pursue it and record that pursuit in our corporate training records.</p>
Nancy Cross Y-12 National Security Complex	<p>The driver for the Termination Briefing is DOE M 470.4-1, Section K. Also we have a Security Awareness Procedure at Y-12 (Y19-131) which addresses Termination Briefings. A Termination Briefing is required whenever an access authorization has been or will be terminated. Termination Briefings must reiterate to the individual the continuing responsibility not to disclose classified information or matter to which they had access, the potential penalties for noncompliance, and the obligation to return all unclassified controlled and classified documents and materials in the individuals possession to the cognizant security authority or to DOE.</p> <p>We use a Termination Checklist for all employees; this is an excellent tool to ensure compliance. Content to be included is the information contained in items 1-6 of the Security Termination Statement form DOE F5631 and information in items 3,4,5,7 and 8 of the SF-312. Also, penalties for unauthorized disclosure of classified information or matter as specified in the Atomic Energy ACT OF 1954 and 18 U.S.C. and penalties for unauthorized disclosure of unclassified controlled nuclear information (UNCI). The termination briefing must be conducted on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information or matter, or SNM, whichever is sooner.</p> <p>The Security Awareness Specialists are accurately documenting the termination briefings through the use of a "sign-in roster" compliance with the content requirements of the DOE470. 4-1 Section K 4(2) d (1) and through the use of a "termination video" to reinforce the information provided to the terminating employee. The Security Awareness Specialists properly document the termination briefings and immediately provide Personnel Security Specialists electronic copies for further processing. DOE badges are collected at the time of the termination briefing and immediately returned to the Y-12 Badge Office.</p>
Scott Colonese LLNL	<p>The Termination Briefing is in the format of a booklet. Individuals who terminate in person receive this booklet along with the Security Termination Statement (STS). If an individual does not terminate in person, a booklet with the STS is mailed to him or her. The booklet covers what the DOE Order requires.</p>
Sylvia Lovelett Pantex	<p>All termination briefings are developed using DOE directives, policies and/or notices and are completed by Access Control.</p>

## OIO Panel Discussion 2008 SASIG Workshop

5. What is your process for developing and conducting Termination Briefings?	
Chet Braswell Flour Hanford	Exiting employees cannot obtain a paycheck until signed off by security that their badge was returned and a termination briefing (if needed) was accomplished. The staff uses a structured lesson plan, and the briefing is one-on-one. Most termination briefings are conducted by the Security Awareness Coordinator. If the coordinator is unavailable, the Personnel Security Clearance Coordinator conducts the termination briefing. If that person is unavailable, the staff at Central Badging can conduct a briefing. During layoffs, staff are placed in a central location, and all actions are conducted in one building (term briefing, badge collection, dosimeter collection, HR exit interviews, and payroll.)
Kristine Inskeep INL	Our Termination briefing is conducted by Personnel Security on the individual's exit visit to turn in the badge. For circumstances (death, illness, termination for cause, etc.) that do not allow someone to turn in a badge, we do a termination briefing by mail.

## OIO Panel Discussion 2008 SASIG Workshop

6. What is your report format for training verification (e.g., Excel)?	
Fran Armijo Sandia-NM	Again, we have 12,500 cleared people. We have a corporate training database called TEDS. Normally, we have “Training Coordinators” responsible for inputting training requirements, extending them, or removing them from a person’s training records. For security, we prohibit anyone but Awareness from doing so, which helps a lot.
Nancy Cross Y-12 National Security Complex	<p>Y-12’s training department maintains the training verification of the briefing records that are entered into our electronic briefing registration system for the Initial and Comprehensive Briefings conducted. The training department also tracks the Refresher Briefing to ensure individuals have taken it within the 12-month timeframe, and, if they have not, access to the site will be denied.</p> <p>The Security Awareness Specialists maintain sign-in rosters and hard copies of the Briefing Attendance Records are entered into the Electronic Briefing Registration System. Y-12 has a Requirements Compliance Assurance Matrix that is a living database in which all company contractual requirements and related implementing documentation are captured and tracked. Importantly, it helps meet DOE requirements for a contractor assurance system that says we know what our requirements are and how we are managing them. Basically, it provides software that allows subject matter experts to list in one place all applicable requirements for Y-12, including DOE directives, rules, regulations, and standard; federal, state, and local laws; and corporate guidance. These requirements are recorded on an Excel spreadsheet template and uploaded to the database. Once there, they must be reviewed at least semiannually and validated annually by the appropriate managers and subject matter experts. Another great tool for ensuring compliance.</p>
Scott Colonese LLNL	Ltrain (Livermore Training Records and Information Network) has been used at our facility for about 17 years. Due to the limitations, we are in the process of moving to PLATEAU.
Sylvia Lovelett Pantex	Employees complete a PX-3864 “Training Completion Form” after completing training. The form is forwarded to Technical Training and the data is entered in to the Plateau LMS. Training records can be retrieved electronically, and the hard copies are kept using normal GSA Record Retention periods.
Chet Braswell Flour Hanford	Customized software developed and used by the Site Training Records organization.
Kristine Inskeep INL	<p>Our reports are done in Crystal Report software. Our TRAIN system that keeps the records of our training comes from the database.</p> <p>During the OIO, we were asked to submit the reports in EXCEL and had a hard time converting the information. We accomplished this, but it was very time consuming for our security and training computer people.</p>

## OIO Panel Discussion 2008 SASIG Workshop

### 7. What security awareness activities do you use to promote your program (e.g., posters, flyers, website notices)?

Fran Armijo  
Sandia-NM

We use self-made posters, self-made videos; new manager briefings (twice a year); contractor briefings (three to four times a year); line-requested, organization-specific briefings; annual FSO Conference; FSO website (6000+ hits so far), quarterly FSO newsletter; monthly internal newsletter; and Info Sessions—basically, we bring in speakers. Unfortunately, these aren't well attended, so we've decided to cut them back from four to two a year.

We also place articles in the *Sandia Daily News* (no more than a paragraph), Sandia's homepage (again no more than a paragraph long), the secretarial "Wednesday" newsletter, and the *Porcelain Press*—a monthly newsletter published by our ES&H people and placed in bathroom stalls.

This year, we're providing a handout with security-related quiz/questions for our visiting children on "Take Your Child to Work Day." We're also joining forces with ES&H on a Safety/Security Fair to be held on June 5. We hope to have 18 security groups participate in this event.

We're putting together a handbook for our Center and Division S&S Coordinators. These are people (approximately 50) assigned to help the line with various security-associated tasks. We are also working on a managers' tool cart.

When referring to "we," it is basically "me," with some great help from the people in my department—editors/writers, photos/videos, web-talent. I couldn't do it without them. Margret Tibbetts is responsible for all the training records and is my side-kick for all event planning. She pretty much coordinates the yearly FSO Conference. We do have what is called a "Security Education & Awareness Liaison Team" composed of SMEs and S&S Coordinators that is supposed to work with Awareness to get the message out. Mostly, I get suggestions but very little "I can do it!" help.

## OIO Panel Discussion 2008 SASIG Workshop

7. What security awareness activities do you use to promote your program (e.g., posters, flyers, website notices)?	
Nancy Cross Y-12 National Security Complex	<p>We do Security Awareness Bulletins monthly on various security subjects and topics. Security Awareness maintains the monthly schedule which has a different Security group responsible for the bulletin that month. Example: Personnel Security one month, Cyber Security the next. If Security subjects or topics need additional reinforcement, we add more bulletins for that month. We recently added ones for OPSEC.</p> <p>We also have awareness campaigns and had an Information Campaign in which we addressed our Cell Phone Policy. As reminders, billboards, signs, and posters are placed around the plant. We also had a contest for employees and subs to submit ideas on how to remember not to bring cell phones into unauthorized areas, and the winner received a prize. Everyone that entered was recognized.</p> <p>We have various websites on YSource (Y-12 intraweb) that includes Security Awareness, OPSEC, Counterintelligence, Computer Security, Classified Matter Protection and Control. All Security Departments have websites that are updated and well maintained. "Security Matters," which lists frequently asked questions and answers, is posted every day on our intraweb. An example of a posting is: "What are my Personal Security Reporting requirements?" In answer, the reporting requirements for cleared individuals are listed, along with the name of the subject matter expert in Personnel Security who can help with additional guidance. In addition to this, we also make announcements on the Ysource Intraweb to share Security reminders on procedure or order changes.</p> <p>We use posters and conduct adhoc security briefings—most recent was on Personally Identifiable Information. Integrated Security awareness is promoted.</p> <p>The Security Awareness Special Interest Group has been an excellent tool that provides valuable input and many excellent resources. The handbook is a great example. Also, the recent Refresher is very good.</p>
Scott Colonese LLNL	<p>We use posters, "NewsOnLine" (lab website), Security Bulletins, Security Website, TV ads on the Lab television, Security Reminders, and "What Would You Do?" (column in the daily online news).</p>
Chet Braswell Flour Hanford	<p>We use live briefings, computer Refresher briefings, web advertising, staff briefings, posters, contests, giveaways, employee recognition, and news articles.</p>

## OIO Panel Discussion 2008 SASIG Workshop

### 7. What security awareness activities do you use to promote your program (e.g., posters, flyers, website notices)?

Kristine Inskeep  
INL

We have an annual event that is usually shared with the Safety Program to promote safety and security awareness. These events have been held in the past:

- Security cubicle—identify what it wrong with this
- Card board figures displaying security sayings at main facilities
- Fairs with exhibits, displays, and presentations
- OPSEC/Security Awareness have several different presentations on security subjects that we present to employees at staff meetings, all hand meetings, and special topical briefings when requested. We do two or three a month.
- Posters—when they came from DOE HQ—we have not put up too many and still use the ones we have had in the past and rotate them.
- Annual security calendar with a yearly theme. This has become a standard and employees will start calling two months before it expires to make sure another one is coming.
- We sent out iNotes to our employees when needed, but they have become fewer due to the amount of information that comes out on iNotes. We find that the employees don't pay attention when they are being inundated by continual safety, security, company information.
- We have a quarterly newsletter that goes out under the OPSEC program, and I put a Security Awareness message, puzzle, or other activity in it.
- We have had a quarterly coaster with thought provoking statements and graphic that CI, Information Security, Cyber Security, OPSEC, Personnel Security, etc. takes turns sending out. These are usually placed on employees' desks to put their beverage on and seem to be a constant reminder of our particular focus.

