

Defense Nuclear Security Lessons Learned Center



DOE/NNSA Security Workshop Las Vegas, Nevada May 8, 2008

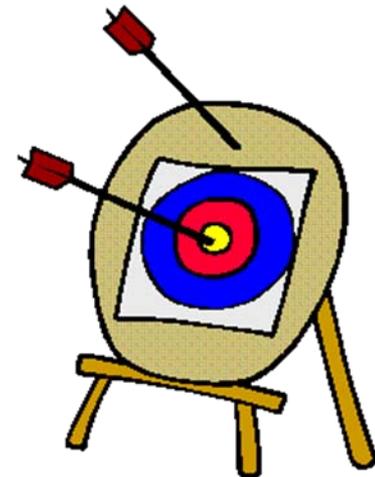
**Presenters: Patty Blount – Center Lead,
David Mullen, and Bethany Redmond**



Defense Nuclear Security Lessons Learned Center

■ Purpose

Provide a centralized infrastructure that will promote the sharing and utilization of security-related lessons learned information gained from operating experiences across the DOE/NNSA Complex.



Slide 2



Defense Nuclear Security Lessons Learned Center

■ Background

- Established/funded by the Office of Defense Nuclear Security (NA-70) in February 2007
- Operational since August 2007
- Developed for security users across DOE/NNSA Complex



Defense Nuclear Security Lessons Learned Center

■ Points of Contact

Defense Nuclear Security Lessons Learned Center

*Sharing Experiences to
Ensure National Security*






Points of Contact

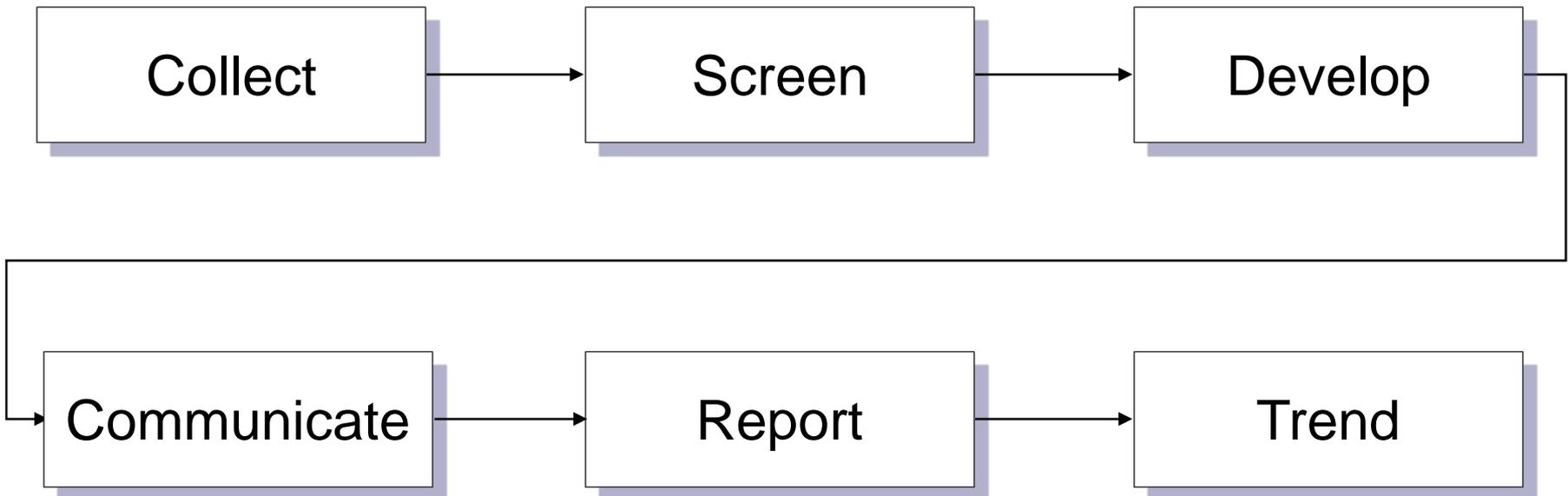
Kathy Sumbry-Wilkins	ksumbry-wilkins@doeal.gov	Albuquerque Service Center
Amber Bullard	adbullar@pantex.com	BWXT Pantex
Kyle Singleton	ksinglet@pantex.com	BWXT Pantex
Anthony George	ageorge@kcp.com	Kansas City Site Office
David Aron	dave.aron@oak.doe.gov	Lawrence Livermore National Laboratory
Diane Menapace	dmenapace@doeal.gov	Los Alamos Site Office
McCloskey, Stan	mccloskeys@nv.doe.gov	Nevada Site Office
John O'Brien	jobrien@pantex.doe.gov	Pantex Site Office
Randy Kubasek	rkubasek@doeal.gov	Sandia National Laboratory
Diane Powell	diane.powell@nnsa.srs.gov	Savannah River Site Office
Lee Prim	lee.prim@srs.gov	Washington Savannah River Company
Debbie Hunter	hunterdl@y12.doe.gov	Y-12



Defense Nuclear Security Lessons Learned Center

■ Operating Procedures

- Serve as the central clearinghouse to:



Defense Nuclear Security Lessons Learned Center

■ Infrastructure

- Database
 - Microsoft Access database maintained by DNS-LLC for archiving, tracking, trending and reporting Operating Experiences
 - Compatible with the Office of Health, Safety and Security (HSS) database (DOE Corporate)
 - DNS-LLC uploads to HSS for posting to DOE Corporate (June 9)
- Webpage
 - Web-based Homepage available on open network – linked to HSS and other DOE/NNSA websites
 - Timely posting and dissemination of security communications
- Help Desk
 - Call-In and E-Mail Resource Center



Defense Nuclear Security Lessons Learned Center

■ Program Drivers and Integration

- Primary Drivers
 - DOE Standard 7501-99 – *The DOE Corporate Lessons Learned Program*
 - DOE O 226.1A – *Implementation of Department of Energy Oversight Policy*
 - DOE Order 210.2 - *DOE Corporate Operating Experience/Lessons Learned Program (OEC)*
 - Memo (20 November 2007 from D'Agostino) – *Expectations for NNSA Regarding DOE O 210.2*
- Coordination and Integration
 - DOE Corporate – Office of Health, Safety and Security (HSS)
 - DOE OEC Coordinator & Operating Experience Working Group
 - Energy Facility Contractors Group (EFCOG)
 - Security Awareness Special Interest Group (SASIG)
 - Training Manager's Working Group (TMWG)
 - DOE National Training Center (NTC)
 - ASIS International



Defense Nuclear Security Lessons Learned Center

• DNS-LLC Process

Inputs

- DOE/NNSA Submittals
 - Lessons Learned
 - Best Practices
 - Success Stories
 - Alerts
- HSS Corporate OEC
- External Data Collection



Defense Nuclear Security Lessons Learned Center

■ Website

- <http://dns-lessons.lanl.gov/>

STAFF

- ▣ Patty Blount
(505) 667-5181
- ▣ Bethany Redmond
(505) 606-1533
- ▣ Antonette Serrano
(505) 667-0233
- ▣ David Mullen
(505) 665-1011

email: dns-lessons@lanl.gov
 Help Desk: (505)665-0196

Defense Nuclear Security Lessons Learned Center

*Sharing Experiences to
Ensure National Security*

**Defense Nuclear Security
Lessons Learned Center**

The Office of Defense Nuclear Security established the Defense Nuclear Security Lessons Learned Center (DNS-LLC) at Los Alamos National Laboratory to encourage and facilitate the sharing of lessons-learned data on physical security-related issues. This center will help users from across the NNSA complex identify and implement effective solutions to various security issues.

The center provides a repository and forum for sharing innovative new tools and practices to address common security issues, improve the efficiency of the security program, and help prevent security incidents. To better develop and implement policies, procedures, and systems that will better manage security risk, the center provides security experts with access to information about real-world security successes.

WHAT'S NEW!

- ▶ **NEW!** Do you know how to avoid copyright infringement? Click [here](#) to read how to avoid prosecution and minimize the risks to your computer by ensuring you have permission to use any copyrighted information and only download authorized files. (4/11/08)

LESSONS LEARNED DATA

- ▶ Search DOE Corporate Database
- ▶ Search DNS-LLC Synopsis
- ▶ Reports
- ▶ Security Communications

[Top of page](#)

MEETINGS & EVENTS

- Advanced High-Risk Dignitary Protection Course
- DOE/NNSA Security Workshop
- Important Dates

DOCUMENTS & TEMPLATES

- How To Create a LL Document
- DNS-LLC Handbook (pdf)
- DNS-LLC User's Guide (pdf)
- DNS-LLC Brochure (pdf)
- DNS-LLC Certificate of Recognition (pub)
- Lessons Learned Template (doc)
- Best Practice Template (doc)
- Success Story Template (doc)

Web Contact

DOE COMPLEX NEWS

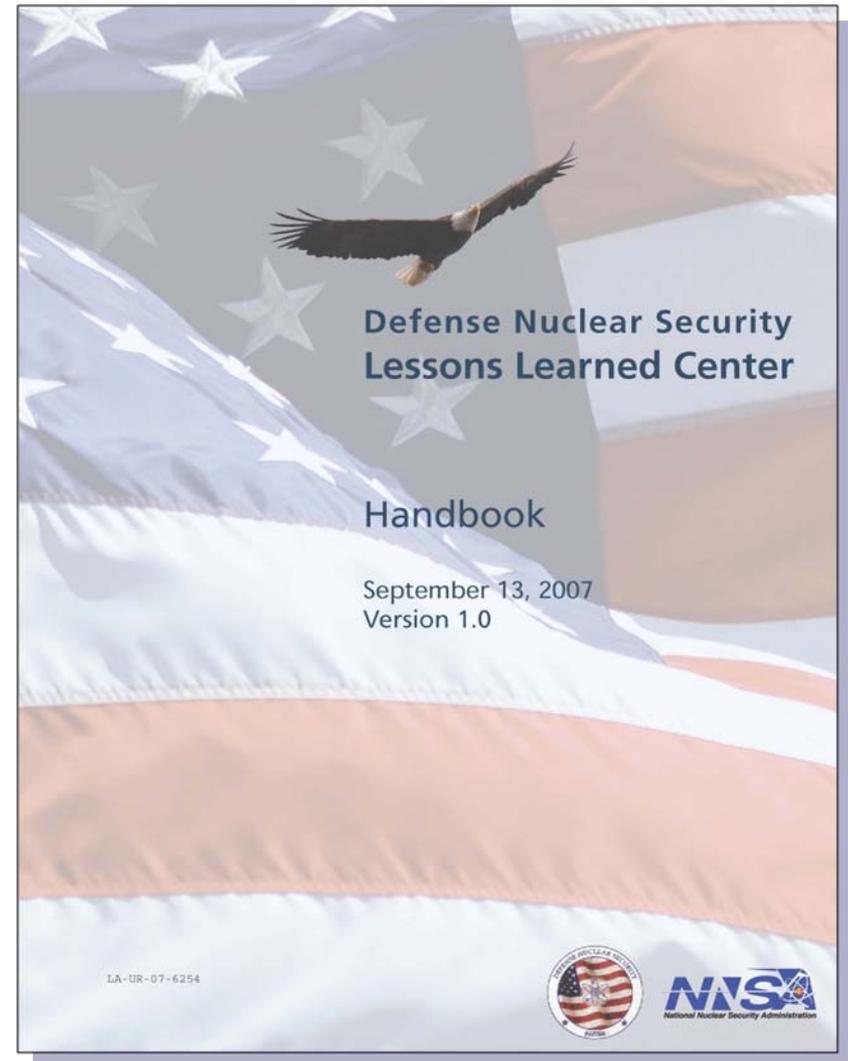
- Sept. 2007 NNSA Newsletter (pdf)
- Security News at DOE sites
- NNSA News Flash about DNS-LLC (pdf)





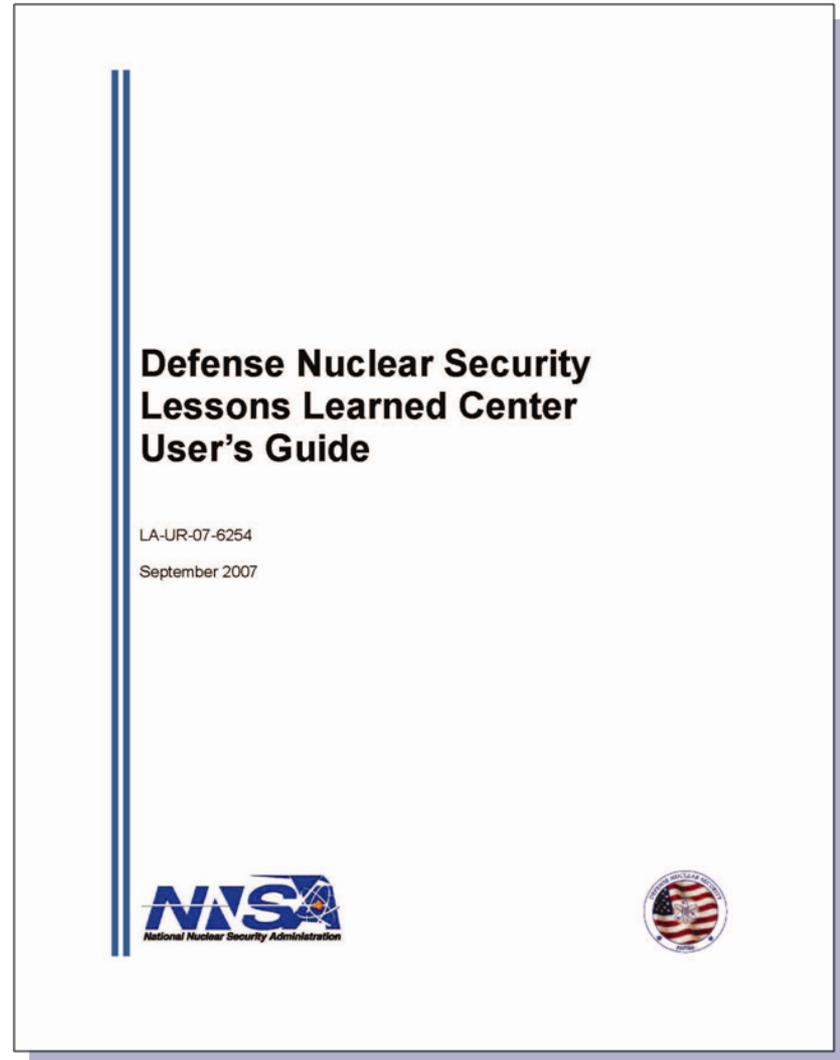

Defense Nuclear Security Lessons Learned Center

- **Handbook**
 - Templates



Defense Nuclear Security Lessons Learned Center

- **User's Guide**

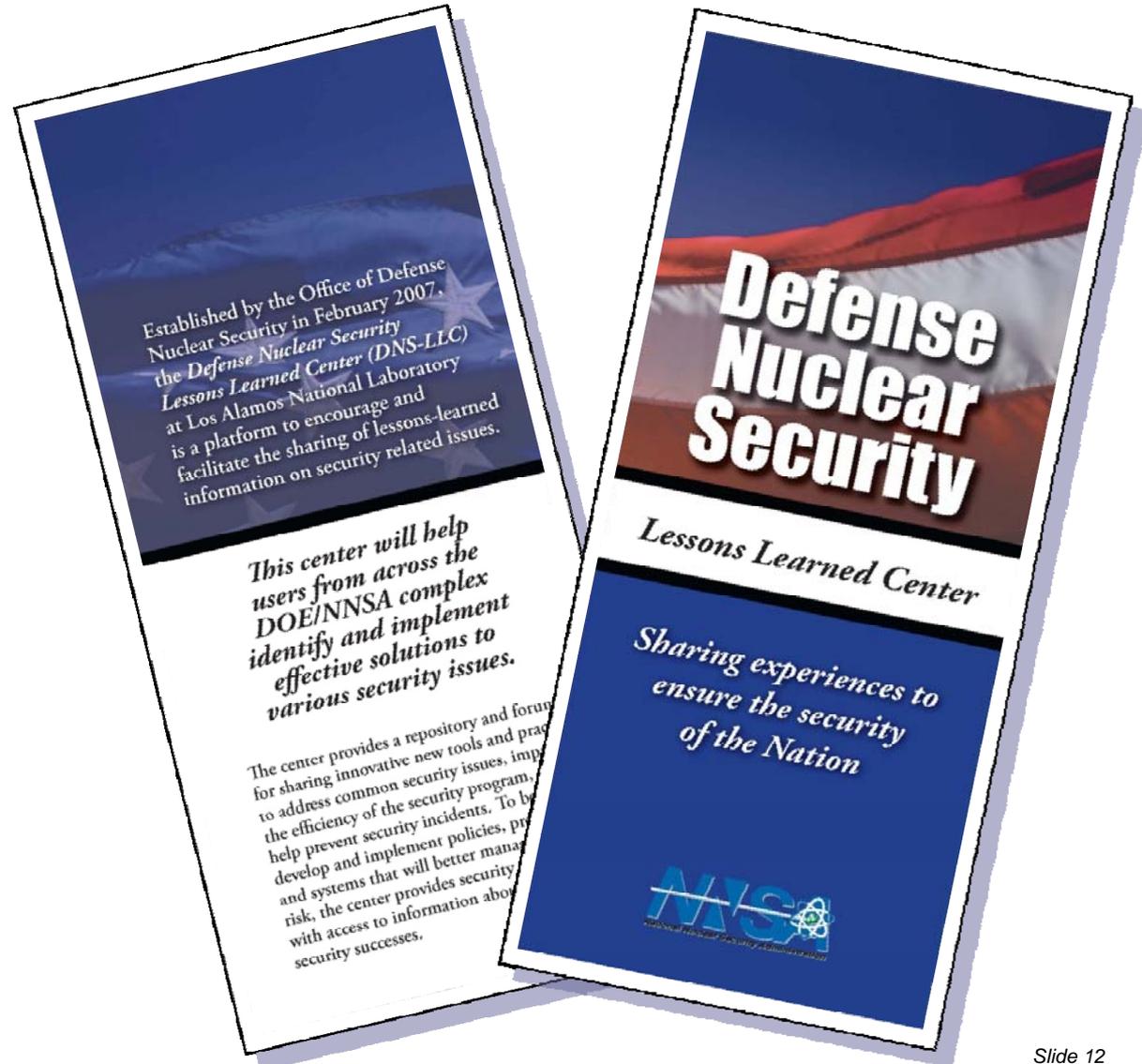


Slide 11



Defense Nuclear Security Lessons Learned Center

■ Brochure



Defense Nuclear Security Lessons Learned Center

Forms & Field Descriptions

- Common to all document types
 - Topical/Sub-Topical Area
 - Date
 - Originator
 - Site
 - Publish Anonymously
 - Title
 - Facility/Site POC
 - Authorized Derivative Classifier
 - Reviewing Official

UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination

LESSONS LEARNED CENTER

**DEFENSE NUCLEAR SECURITY
LESSONS LEARNED CENTER (DNS-LLC)
Success Story Submittal Form**

UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination

LESSONS LEARNED CENTER

**DEFENSE NUCLEAR SECURITY
LESSONS LEARNED CENTER (DNS-LLC)
Best Practice Submittal Form**

UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination

LESSONS LEARNED CENTER

**DEFENSE NUCLEAR SECURITY
LESSONS LEARNED CENTER (DNS-LLC)
Lessons Learned Submittal Form**

Date: _____ ID #: (to be completed by LLC)

Originator: _____

Site: _____

Anonymous Submittal: Yes No

Title: _____

Facility/ Site Point of Contact: _____

Authorized Derivative Classifier: _____

Reviewing Official: _____

Discussion of Activities: _____

Lesson Learned Summary: _____

Analysis: _____

Recommended Actions: _____

Estimated Savings / Cost Avoidance: _____

Keywords: _____

UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination
Page 1 of 1



Defense Nuclear Security Lessons Learned Center

■ Lesson Learned

- Discussion of Activities
- Lesson Learned Summary
- Analysis
- Recommended Actions
- Estimated Savings/Cost Avoidance
- Keywords



UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination

**DEFENSE NUCLEAR SECURITY
LESSONS LEARNED CENTER (DNS-LLC)**
Lessons Learned Submittal Form



Topical/ Sub Topical Area
PROGRAM MANAGEMENT & SUPPORT
<input type="checkbox"/> PROTECTION PROGRAM MANAGEMENT
<input type="checkbox"/> SAS PLANNING & PROCEDURES
<input type="checkbox"/> MANAGEMENT CONTROL
<input type="checkbox"/> PROGRAM WIDE SUPPORT
PROTECTIVE FORCE
<input type="checkbox"/> MANAGEMENT
<input type="checkbox"/> TRAINING
<input type="checkbox"/> DUTIES
<input type="checkbox"/> FACILITIES & EQUIPMENT
PHYSICAL SECURITY
<input type="checkbox"/> ACCESS CONTROLS
<input type="checkbox"/> INTRUSION DETECTION & ASSESSMENT SYSTEMS
<input type="checkbox"/> BARRIERS & DELAY MECHANISMS
<input type="checkbox"/> TESTING & MAINTENANCE
<input type="checkbox"/> COMMUNICATIONS
INFORMATION PROTECTION
<input type="checkbox"/> BASIC REQUIREMENTS
<input type="checkbox"/> TECHNICAL SURVEILLANCE COUNTERMEASURES
<input type="checkbox"/> OPERATIONS SECURITY
<input type="checkbox"/> CLASSIFICATION GUIDANCE
<input type="checkbox"/> CLASSIFIED MATTER PROTECTION & CONTROL
CYBER SECURITY
<input type="checkbox"/> CLASSIFIED CYBER SECURITY
<input type="checkbox"/> TELECOMMUNICATIONS SECURITY
<input type="checkbox"/> UNCLASSIFIED CYBER SECURITY
PERSONNEL SECURITY PROGRAM
<input type="checkbox"/> ACCESS AUTHORIZATION
<input type="checkbox"/> HUMAN RELIABILITY PROGRAM
<input type="checkbox"/> CONTROL OF CLASSIFIED VISITS
<input type="checkbox"/> SAFEGUARDS & SECURITY AWARENESS
UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS
<input type="checkbox"/> SPONSOR PROGRAM MANAGEMENT & ADMIN
<input type="checkbox"/> COUNTERINTELLIGENCE REQUIREMENTS
<input type="checkbox"/> EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS
<input type="checkbox"/> SECURITY REQUIREMENTS
<input type="checkbox"/> APPROVALS & REPORTING
NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY
<input type="checkbox"/> PROGRAM ADMINISTRATION
<input type="checkbox"/> MATERIALS ACCOUNTABILITY
<input type="checkbox"/> MATERIALS CONTROL

Date: _____ **ID #:** (to be completed by LLC)

Originator: _____

Site: _____

Anonymous Submittal: Yes

Title: _____

Facility/ Site Point of Contact: _____

Authorized Derivative Classifier: _____

Reviewing Official: _____

Discussion of Activities:

Lesson Learned Summary:

Analysis:

Recommended Actions:

Estimated Savings / Cost Avoidance:

Keywords:

UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination
Page 1 of 1



Defense Nuclear Security Lessons Learned Center

■ Best Practice

- Brief Description of Best Practice
- Why the Best Practice was used
- What are the benefits of the Best Practice
- What problems/issues were associated with the Best Practice
- Description of the process/activity using the Best Practice
- Estimated Savings/Cost Avoidance
- Keywords



UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination

**DEFENSE NUCLEAR SECURITY
LESSONS LEARNED CENTER (DNS-LLC)**
Best Practice Submittal Form



Topical/ Sub Topical Area
PROGRAM MANAGEMENT & SUPPORT <input type="checkbox"/> PROTECTION PROGRAM MANAGEMENT <input type="checkbox"/> SAFETY TRAINING & PROCEDURES <input type="checkbox"/> MANAGEMENT CONTROL <input type="checkbox"/> PROGRAM WIDE SUPPORT
PROTECTIVE FORCE <input type="checkbox"/> MANAGEMENT <input type="checkbox"/> TRAINING <input type="checkbox"/> DUTIES <input type="checkbox"/> FACILITIES & EQUIPMENT
PHYSICAL SECURITY <input type="checkbox"/> ACCESS CONTROLS <input type="checkbox"/> INTRUSION DETECTION & ASSESSMENT <input type="checkbox"/> SYSTEMS <input type="checkbox"/> BARRIERS & DELAY MECHANISMS <input type="checkbox"/> TESTING & MAINTENANCE <input type="checkbox"/> COMMUNICATIONS
INFORMATION PROTECTION <input type="checkbox"/> BASIC REQUIREMENTS <input type="checkbox"/> TECHNICAL SURVEILLANCE <input type="checkbox"/> COUNTERMEASURES <input type="checkbox"/> OPERATIONS SECURITY <input type="checkbox"/> CLASSIFICATION GUIDANCE <input type="checkbox"/> CLASSIFIED MATTER PROTECTION & <input type="checkbox"/> CONTROL
CYBER SECURITY <input type="checkbox"/> CLASSIFIED CYBER SECURITY <input type="checkbox"/> TELECOMMUNICATIONS SECURITY <input type="checkbox"/> UNCLASSIFIED CYBER SECURITY
PERSONNEL SECURITY PROGRAM <input type="checkbox"/> ACCESS AUTHORIZATION <input type="checkbox"/> HUMAN RELIABILITY PROGRAM <input type="checkbox"/> CONTROL OF CLASSIFIED VISITS <input type="checkbox"/> SAFEGUARDS & SECURITY AWARENESS
UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS <input type="checkbox"/> SPONSOR PROGRAM MANAGEMENT & <input type="checkbox"/> ADMIN <input type="checkbox"/> COUNTERINTELLIGENCE <input type="checkbox"/> REQUIREMENTS <input type="checkbox"/> EXPORT CONTROLS/ TECH TRANSFER <input type="checkbox"/> REQUIREMENTS <input type="checkbox"/> SECURITY REQUIREMENTS <input type="checkbox"/> APPROVALS & REPORTING
NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY <input type="checkbox"/> PROGRAM ADMINISTRATION <input type="checkbox"/> MATERIALS ACCOUNTABILITY <input type="checkbox"/> MATERIALS CONTROL

Date: _____ ID #: (to be completed by LLC)

Originator: _____

Site: _____

Publish Anonymously: Yes

Facility/ Site Point of Contact: _____

Title: _____

Authorized Derivative Classifier: _____

Reviewing Official: _____

Brief Description of Best Practice:

Why the Best Practice was used:

What are the benefits of the Best Practice:

What problems/ issues were associated with the Best Practice:

Description of the process/ activity using the Best Practice:

Estimated Savings/ Cost Avoidance:

Keywords:

UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination
Page 1 of 1



Defense Nuclear Security Lessons Learned Center

■ Success Story

- Overview of Success Story
- Challenge
- Solution
- Results
- Estimated Savings/ Cost Avoidance
- Keywords



UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination

**DEFENSE NUCLEAR SECURITY
LESSONS LEARNED CENTER (DNS-LLC)
Success Story Submittal Form**

**Topical/
Sub Topical Area**

PROGRAM MANAGEMENT & SUPPORT

PROTECTION PROGRAM MANAGEMENT

S&P PLANNING & PROCEDURES

MANAGEMENT CONTROL

PROGRAM WIDE SUPPORT

PROTECTIVE FORCE

MANAGEMENT

TRAINING

DUTIES

FACILITIES & EQUIPMENT

PHYSICAL SECURITY

ACCESS CONTROLS

INTRUSION DETECTION & ASSESSMENT SYSTEMS

BARRIERS & DELAY MECHANISMS

TESTING & MAINTENANCE

COMMUNICATIONS

INFORMATION PROTECTION

BASIC REQUIREMENTS

TECHNICAL SURVEILLANCE COUNTERMEASURES

OPERATIONS SECURITY

CLASSIFICATION GUIDANCE

CLASSIFIED MATTER PROTECTION & CONTROL

CYBER SECURITY

CLASSIFIED CYBER SECURITY

TELECOMMUNICATIONS SECURITY

UNCLASSIFIED CYBER SECURITY

PERSONNEL SECURITY PROGRAM

ACCESS AUTHORIZATION

HUMAN RELIABILITY PROGRAM

CONTROL OF CLASSIFIED VISITS

SAFEGUARDS & SECURITY AWARENESS

UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS

SPONSOR PROGRAM MANAGEMENT & ADMIN

COUNTERINTELLIGENCE REQUIREMENTS

EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS

SECURITY REQUIREMENTS

APPROVALS & REPORTING

NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY

PROGRAM ADMINISTRATION

MATERIALS ACCOUNTABILITY

MATERIALS CONTROL

Date: _____ **ID #:** (to be completed by LLC)

Originator: _____

Site: _____

Publish Anonymously: Yes

Title: _____

Facility/ Site Point of Contact: _____

Authorized Derivative Classifier: _____

Reviewing Official: _____

Overview of Success Story:

Challenge:

Solution:

Results:

Estimated Savings / Cost Avoidance:

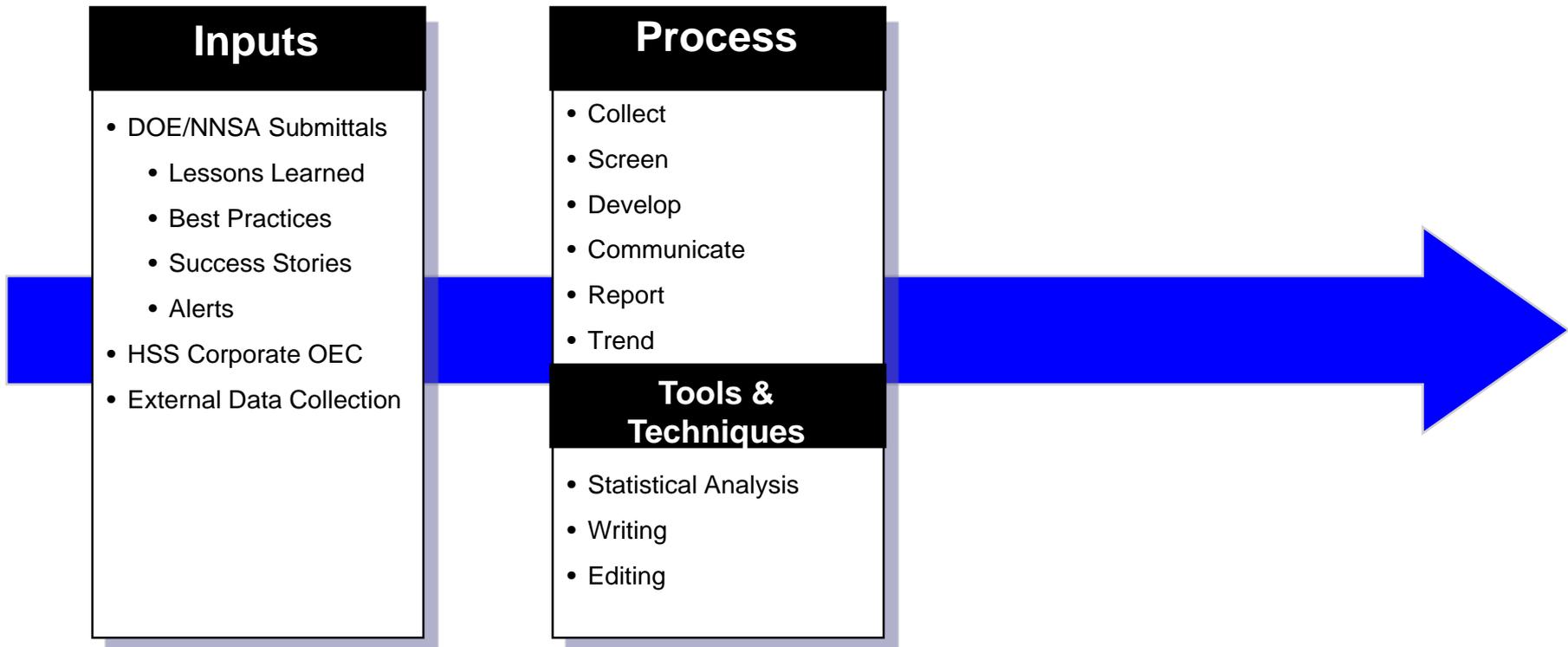
Keywords:

UNCLASSIFIED ONLY
Obtain ADC Review Prior to Dissemination
Page 1 of 1



Defense Nuclear Security Lessons Learned Center

• DNS-LLC Process



Defense Nuclear Security Lessons Learned Center

■ Process

- Verification
- Prioritization
- Evaluation
- Clarification
- Communication



Defense Nuclear Security Lessons Learned Center

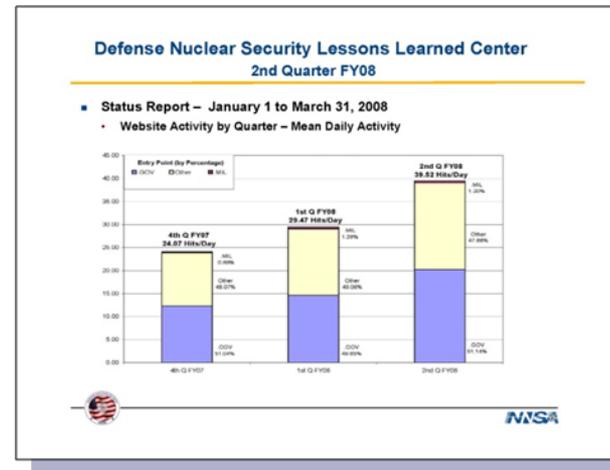
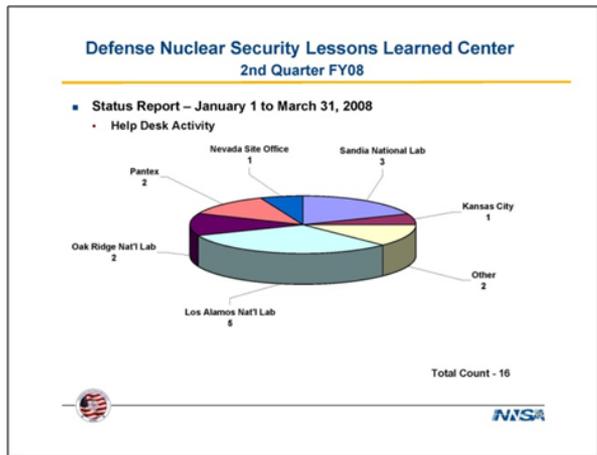
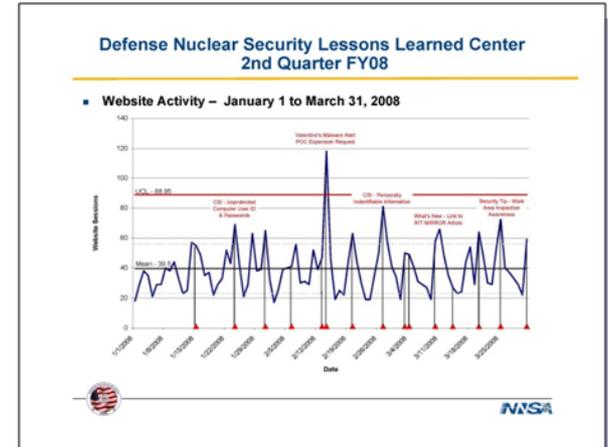
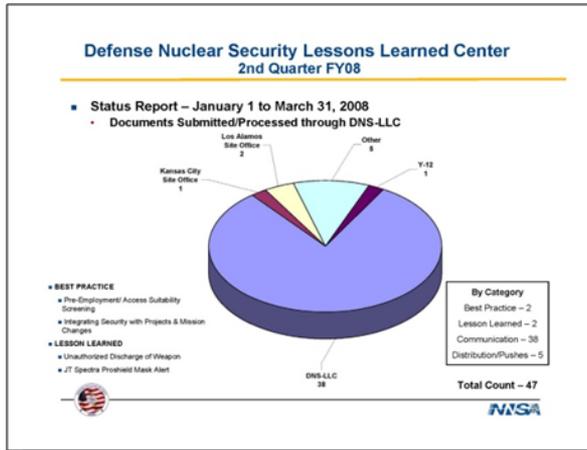
■ Application of Statistical Analysis Techniques

- Control Charts
- Pie Charts
- Bar Charts



Defense Nuclear Security Lessons Learned Center

■ Quarterly Reports



Defense Nuclear Security Lessons Learned Center

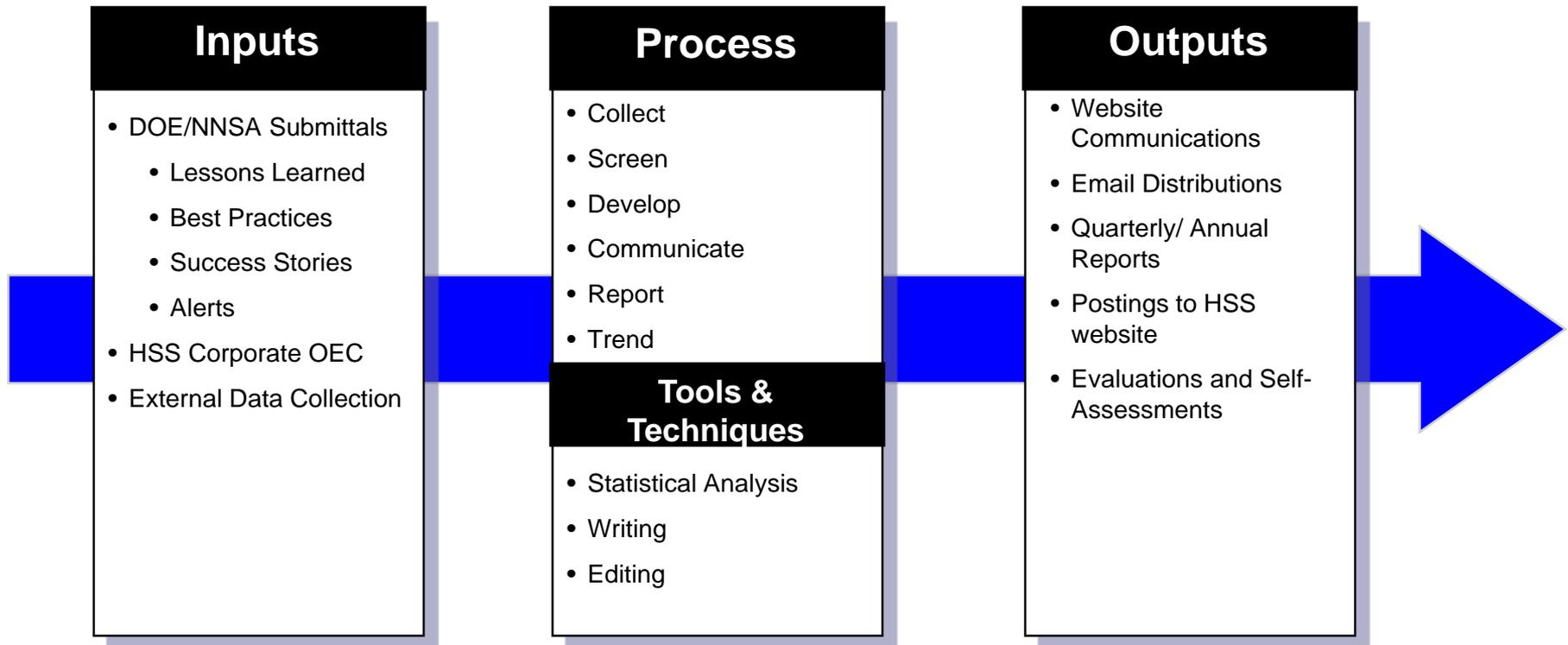
■ Human Performance Improvement

- Incorporate HPI into Lessons Learned via training and communications
- Incidents of Security Concern
 - When is HPI desired? Required?
 - High consequences – Low frequency (IMI 1s)
 - High frequency – Low consequences (IMI 4s)



Defense Nuclear Security Lessons Learned Center

• DNS-LLC Process



Defense Nuclear Security Lessons Learned Center

■ Communication

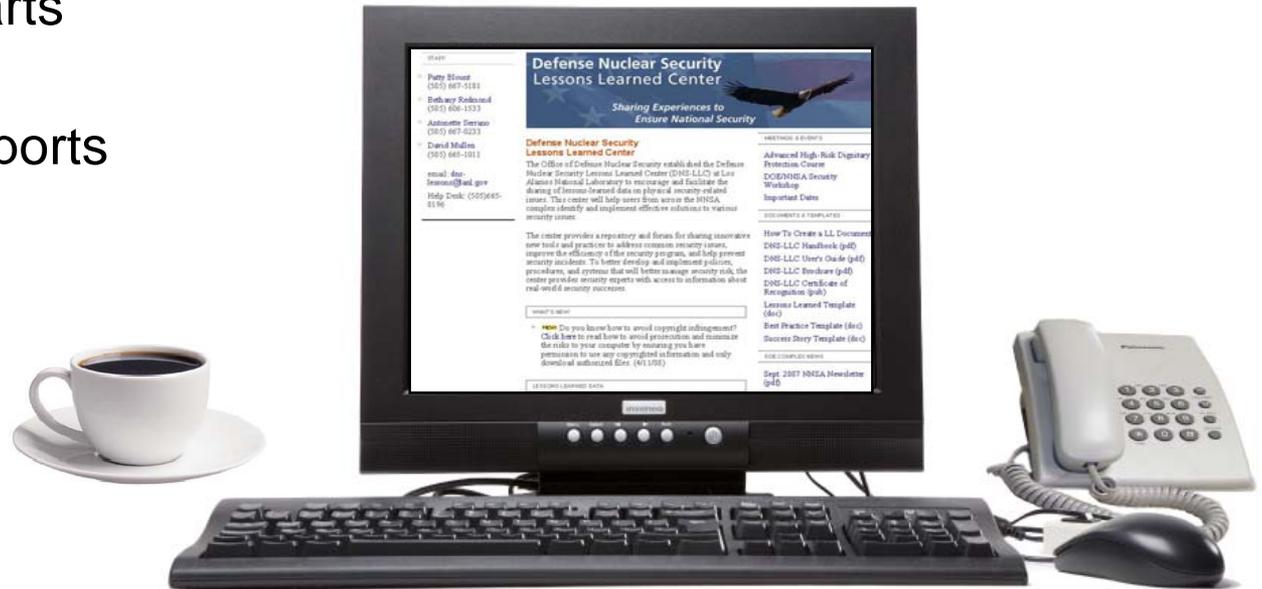
- Provide information to the right audience in a timely manner
- Utilize a structured approach to push/pull information
 - Information must be able to flow in multiple directions
 - Cannot just rely upon a top-down approach, must also encourage a bottom-up approach
- How is information communicated /collected at other sites



Defense Nuclear Security Lessons Learned Center

■ Communication Products

- Website
- What's New
- CSI
- Tips
- Security Smarts
- Synopsis
- Quarterly Reports



Defense Nuclear Security Lessons Learned Center

Website

- <http://dns-lessons.lanl.gov/>

STAFF

- Patty Blount (505) 667-5181
- Bethany Redmond (505) 606-1533
- Antonette Serrano (505) 667-0233
- David Mullen

Defense Nuclear Security Lessons Learned Center

Sharing Experiences to Ensure National Security



About Us Contacts Site Map FAQ's Links

Defense Nuclear Security Lessons Learned Center

Security Communications

- Security Smarts
- CSI: Contemplating Security Incidents
- Security Tips
- Other Security Communications

Defense Nuclear Security Lessons Learned Center

The Office of Defense Nuclear Security established the Defense Nuclear Security Lessons Learned Center (DNS-LLC) at Los Alamos National Laboratory to encourage and facilitate the sharing of lessons-learned data on physical security-related issues. This center will help users from across the NNSA complex identify and implement effective solutions to various security issues.

The center provides a repository and forum for sharing innovative new tools and practices to address common security issues, improve the efficiency of the security program, and help prevent security incidents. To better develop and implement policies, procedures, and systems that will better manage security risk, the center provides security experts with access to information about real-world security successes.

WHAT'S NEW!

- ▶ **NEW!** Do you know how to avoid copyright infringement? Click here to read how to avoid prosecution and minimize the risks to your computer by ensuring you have permission to use any copyrighted information and only download authorized files. (4/11/08)

LESSONS LEARNED DATA

- ▶ Search DOE Corporate Database
- ▶ Search DNS-LLC Synopsis
- ▶ Reports
- ▶ Security Communications

MEETINGS & EVENTS

- Advanced High-Risk Dignitary Protection Course
- DOE/NNSA Security Workshop
- Important Dates

DOCUMENTS & TEMPLATES

- How To Create a LL Document
- DNS-LLC Handbook (pdf)
- DNS-LLC User's Guide (pdf)
- DNS-LLC Brochure (pdf)
- DNS-LLC Certificate of Recognition (pub)
- Lessons Learned Template (doc)
- Best Practice Template (doc)
- Success Story Template (doc)

DOE COMPLEX NEWS

- Sept. 2007 NNSA Newsletter (pdf)
- Security News at DOE sites
- NNSA News Flash about DNS-LLC (pdf)





Top of page

Web Contact



Defense Nuclear Security Lessons Learned Center

■ What's New

WHAT'S NEW!

- ▶ **NEW!** Do you know how to avoid copyright infringement? Click here to read how to avoid prosecution and minimize the risks to your computer by ensuring you have permission to use any copyrighted information and only download authorized files. (4/11/08)

STAFF

- ▣ Patty Blount
(505) 667-5181
- ▣ Bethany Redmond
(505) 606-1533
- ▣ Antonette Serrano
(505) 667-0233
- ▣ David Mullen
(505) 665-1011

email: dns-lessons@anl.gov

Help Desk: (505)665-0196

Defense Nuclear Security Lessons Learned Center

Sharing Experiences to Ensure National Security



Defense Nuclear Security Lessons Learned Center

The Office of Defense Nuclear Security established the Defense Nuclear Security Lessons Learned Center (DNS-LLC) at Los Alamos National Laboratory to encourage and facilitate the sharing of lessons-learned data on physical security-related issues. This center will help users from across the NNSA complex identify and implement effective solutions to various security issues.

The center provides a repository and forum for sharing innovative new tools and practices to address common security issues, improve the efficiency of the security program, and help prevent security incidents. To better develop and implement policies, procedures, and systems that will better manage security risk, the center provides security experts with access to information about real-world security successes.

WHAT'S NEW!

- ▶ **NEW!** Do you know how to avoid copyright infringement? Click here to read how to avoid prosecution and minimize the risks to your computer by ensuring you have permission to use any copyrighted information and only download authorized files. (4/11/08)

LESSONS LEARNED DATA

- ▶ Search DOE Corporate Database
- ▶ Search DNS-LLC Synopsis
- ▶ Reports
- ▶ Security Communications

Top of page

Web Contact

MEETINGS & EVENTS

- Advanced High-Risk Dignitary Protection Course
- DOE/NNSA Security Workshop
- Important Dates

DOCUMENTS & TEMPLATES

- How To Create a LL Document
- DNS-LLC Handbook (pdf)
- DNS-LLC User's Guide (pdf)
- DNS-LLC Brochure (pdf)
- DNS-LLC Certificate of Recognition (pub)
- Lessons Learned Template (doc)
- Best Practice Template (doc)
- Success Story Template (doc)

DOE COMPLEX NEWS

- Sept. 2007 NNSA Newsletter (pdf)
- Security News at DOE sites
- NNSA News Flash about DNS-LLC (pdf)



Defense Nuclear Security Lessons Learned Center

■ CSI: Contemplating Security Incidents

Defense Nuclear Security Lessons Learned Center
Sharing Experiences to Ensure National Security

February 2008

Theft or Loss of Personally Identifiable Information (PII)

In September 2007, the National Nuclear Security Administration (NNSA) mandated that the loss of PII under the Control of NNSA be considered an Incident of Security Concern (IOSC).

Case

While Jim was on travel, the laptop was bagged and his unclassified government laptop was stolen along with some personal valuables. Upon discovering the bag was Jim's wife called the police department and contacted Jim. He immediately notified his group leader who reported the incident and in the organization's security forum. The group leader told Jim the group leader also advised that there could be classified information on the laptop. Jim's wife was on the laptop in case for when he was very tired and his wife's name was on the laptop. However, Jim advised that he and his wife had recently moved to a new home. The security representative was not aware of this. The security representative was not aware of this. The security representative was not aware of this.

Security Concern

The compromise of an individual's PII can be PII. Someone with identification throughout the person's lifetime. DOE had a policy that all PII on government computers shall be encrypted. The loss of PII for 20 or more individuals is an IOSC. Loss of PII for 20 or more individuals is an IOSC.

Causal Analysis

Jim had a legitimate need to take the government laptop at home. However, he did not need the PII that was on the laptop to conduct his work. He had previously protected the PII on the computer with a password. The password was not strong enough. The password was not strong enough. The password was not strong enough.

BE SECURITY SMART!

Defense Nuclear Security Lessons Learned Center
Sharing Experiences to Ensure National Security

January 2008

Unprotected Computer User ID and Password

Your password allows access to many computing and information resources. The password, along with a user identification (user ID), authenticates your identity to an online (web) computer user or to a computer system or network. Your user identification is then used to control your activities within the system or network, and to determine your identity. In order to avoid unauthorized users, it is important to know:

Case

Diane was authorized by her group leader to take a work laptop so she could work from home. Since Diane eventually started to have difficulty logging on to the laptop, she requested and was approved to send the laptop for a condition report for home use. The group leader authorized security representative contact on account of the desktop computer for Diane but he failed to check for sensitive information left by the previous owner. Diane returned the laptop and took the desktop computer for home use. A few weeks later, one of Diane's children noticed it was possible to log on to the computer for her father since the family did not own a computer. Diane logged in and allowed him unauthorized and unapproved access to the network. Shortly thereafter, she was also using the computer for her work. Diane knew she was not supposed to give her user ID and password to anyone, but she gave them to her children so they could log in without bothering her. The children began to use the computer and Diane's work user ID and password at will. They routinely accessed Internet sites and used unauthorized peer-to-peer software.

Security Concern

The loss of DOE and local policies by giving her children her work user ID and password. Doing so put sensitive information at risk. Diane's children could easily have downloaded viruses, worms, Trojans, and other malicious software that could have affected almost every computer system on the site. A review of the computer's hard drive revealed a sensitive file that had been left by its former owner. The child could have had a sensitive document that he or she made it vulnerable to access by others. A forensic review of the hard drive revealed that the file had not been deleted and the computer was issued to Diane.

Analysis

The process for approval and management of use of government property allowed Diane to use the laptop for work. The process for approval and management of use of government property allowed Diane to use the laptop for work. The process for approval and management of use of government property allowed Diane to use the laptop for work.

BE SECURITY SMART!

Defense Nuclear Security Lessons Learned Center
Sharing Experiences to Ensure National Security

November 2007

EVER WONDER WHAT EVENTS LEAD UP TO A SECURITY INCIDENT? CSI CAN UNRAVEL THE CLUES.

IMPROPERLY SECURED CLASSIFIED SLIDES

Work environment, human nature, task demands, and individual capabilities are the four general categories of pressures (task demands) and stress (human nature) contributed to an error that fortunately did not result in a serious security incident.

Case

Anne was tasked to develop and deliver a classified briefing about a project on which she was working. The briefing was previously assigned to another worker, but Anne's supervisor had her to take responsibility for the presentation, which was to be delivered later that day. Anne was able to rearrange her schedule so she could deliver the briefing at the afternoon of a prearranged presentation consisting of 23 viewgraphs, of which were classified. Later, as she was preparing her classified slides she had created. Anne set aside the slides when she was running late for her appointment. Anne realized she was running late for her appointment. Anne realized she was running late for her appointment.

Analysis

The process for approval and management of use of government property allowed Anne to use the laptop for work. The process for approval and management of use of government property allowed Anne to use the laptop for work. The process for approval and management of use of government property allowed Anne to use the laptop for work.

BE SECURITY SMART!



Defense Nuclear Security Lessons Learned Center

■ Other Security Communications

Defective Ammunition Alert

Sensitive Media Awareness

Human Performance Philosophy

FBI Issues Valentine's Day Email Warning

Integrating Security With
Projects & Mission Changes



Defense Nuclear Security Lessons Learned Center

■ System Evaluations

- HPI Feedback
- Program Effectiveness
- Continuous Improvement



Defense Nuclear Security Lessons Learned Center

■ Successes

- Integration and Participation with existing Operating Experience Programs
- HSS Compatible – Corporate
- 11 Operating Experiences Received/Processed
- 7904 hits on website
- 1191% Increase in Email Distribution List contacts
- Targeted distributions



Defense Nuclear Security Lessons Learned Center

■ Challenges

- Integration of DOE O 210.2 into site specific programs
- Utilize DOE/NNSA Security Operating Experiences as part of the Work Planning process
- Build into management/employee training



Defense Nuclear Security Lessons Learned Center

■ Opportunity

- Worker Recognition
- Integration With New Organizations
- Integrated Working Groups
- Customer Driven Data Collection and Reporting



Defense Nuclear Security Lessons Learned Center

■ Workshop Feedback

Defense Nuclear Security Lessons Learned Center <i>Sharing Experiences to Ensure National Security</i>	
	
DOE/NNSA Security Workshop Evaluation	
What was the most valuable aspect of this year's Security Workshop	
If the Security Workshop is held again next year, what are your suggestions for the following:	
Venue:	
Duration of Workshop:	
Guest Speakers:	
Topical Areas:	
Additional comments and feedback:	



Defense Nuclear Security Lessons Learned Center

- **Questions**

