Slide 1	

Slide 2	• Sandia's roots can be traced to the Manhattan Project and Los Alamos
	• July 1945
	  • J. Robert Oppenheimer established "Z Division" at Sandia Base
	  • Purpose - perform stockpile development activities and non-nuclear component engineering.

Slide 3	• Sandia's mission areas have increased over the years.
	  • The nuclear weapons component still growing.
	  • And transfer of information to new employees is critical moving forward.
	• Almost 20 years ago Sandia tasked with:
	  • Design and teaching of a class to ensure:
	  • Transfer of information and
	  • Experience to a new generation of nuclear weapons workforce.
	  • Class -11 month, providing in-depth exposure to all aspect of:
	  • nuclear weapon policy,
	  • Research,
	  • Development,
	  • And Production.
	  • While hosted by Sandia, participants are selected from across the Nuclear Security Enterprise and the military. I can almost bet that someone from your site has participated in this class.
	  • Here's where our story starts…

Slide 4	• The individual tasked to author of one of the briefings was knowledgeable and experienced. • The individual used open source and designed a very interesting presentation. • Because the author valued himself as an expert the presentation was never marked or submitted for review. Management trusted the author. • The briefing was presented in a classified environment and every year the individual went back to open source to update the presentation. •

	• On retiring the author was contracted to continue conducting this briefing.
	• Due to popular demand requests were accepted to present the briefing beyond the originally intended audience including:
	  • Sandia employees outside the nuclear weapons program
	  • a Sandia "sister" laboratory
	  • and to an external group of retired non-DOE personnel
	• New program manager joined the team
	  • In search of interesting pictures staff directed him to briefing.
	  • Upon his review the recognition of classified material was discovered.
	  • Immediately reported to Sandia's security incident program.
	• Historical Phase
	• 1997 to 2011
	  • Delivered to internal and external audiences
	  • Presentation existed on numerous media types-personal computer, flash drive, file servers, SharePoint, CDs, and paper copies
	Near-Term Phase
	• 2011 to 2012
	  • Two viewgraphs added to presentation
	  • Delivered only to class participants
	  • No classification review
	  • Presentation existed on organization server with limited access, unauthorized transmission, and paper copies

Slide 5	• Why was it difficult to find a DC about the subject area?
	  • **Because it was not DOE information!!!**
	• The number of slides determined to contain classified information varied between 1 and 22. Ultimately the final determination was 13.
	  • **Without knowledge of the relevant classification issues, none of the hundreds of individuals who viewed this presentation (especially in a dynamic, live presentation format) recognized or even questioned the classification level.**
	  • ***It should be noted that it was not DOE information in the Historical phase.*** **It took a review by the Classification Office to identify the issues from the historic phase of the incident.**

Slide 6	• The author was overly confident in knowledge on the subject matter and classification issues. Management did not question, relying on author as the

	subject matter expert thus leading to an environment where organizational DC review was not viewed as necessary for internal use. • Presentation was considered valuable and in high demand. • Organization assumed an unmarked presentation had been determined to be unclassified by the author or the author's DC. • Human Performance Indicators (HPI) were taken from standardized DOE source, and listed verbatim here. **Root Causes -** • The main root cause was that the author was overly confident in his knowledge of subject matter and related classification issues **Contributing Cause -** • The presentation was not checked for appropriate markings before being posted to the collaborative site, or being printed for handouts **Human Performance Indicator Evaluations -** • Flawed defense in the cultural, organizational expectations • Latent organization weakness in procedure development and use • Flawed defense in the administrative, quality control hold points • Latent organizational weakness in that management failed to recognize the need for or importance of related program • **The second causal analysis** was triggered after additional copies of the presentation were discovered. This discovery caused the inquiry team to re-open the inquiry. • No additional "root causes" were identified in the supplemental causal analysis; however, areas of concern were identified. • Contractors had been allowed to work remotely using a personal computer and personal storage devices.
Slide 7	A thorough DC review was conducted on over 700 presentations located on the organization's servers. • Approximately 20,000 individual slides were DC reviewed. • **Only briefings by this author were classified!!!** • No <u>additional</u> classified information identified. **Enterprise-wide search:** • Searched all systems touching the unclassified Sandia network

	• Searched for briefings authored by department staff members by name • Searched for file name matching original presentation
Slide 8	**This incident created a domino effect beginning with lack of classification review…** **Classification –** • Failed to perform the required classification review of several presentations and apply required classifier markings **Information Protection –** • Failed to protect and control classified information **Classified Cyber Security –** • Failed to ensure that classified information was processed, developed, stored, and disseminated only on approved information systems • Approved servers • And that system media and output were properly classified, marked, controlled, and stored **Causal Analysis and Corrective Actions –** • Failed to conduct a sufficient causal analysis and implement adequate corrective actions designed to prevent recurrence across SNL/NM **Security Incident Inquiry –** • Inquiry failed to establish all of the facts and circumstances surrounding the incident. • Due to the age of the incident and the unreliable memory of the originating author, the inquiry took longer than normal and was unduly complicated; • However, Sandia believes the inquiry established all of the facts and circumstances of this incident. • The initial search by the inquiry official focused on the presentation title **it was not revealed by the author that every variation of the presentation had a unique title.** **Self-Assessments –** • Integrated assessment of the author's organization was not comprehensive and did not thoroughly evaluate the adequacy and effectiveness of its activities related to the protection and control of classified information
Slide 9	Perfect case to challenge severity levels. All sensitive information in the subject presentation obtained from public sources and had been widely disseminated by others

	▪ Information appears in • Numerous Webpages • One webpage alone has ~23K views in 30 days • At least 26 foreign language webpages • Online dissemination • Numerous online sources • University presentations online • Unknown Creator (used a unique nickname) • Has released 71 images to the public domain • 39 are related to nuclear weapons • Many of the 39 appear to be classified • Item of most concern has been widely disseminated since 2005 by other sources • Released to the public domain • Licensed for worldwide use for any purpose without conditions • OSE responded by issuing a FNOV with limited mitigation **What went wrong?** ▪ Sandia leadership change between the time Sandia submitted response to PNOV and the FNOV. ▪ Previous Laboratory President and newly appointed President had differing opinions on resolution ▪ Recent performance review stated Sandia need for transparency with field office. ▪ Priority became rebuilding relationships; Sandia did not follow up a request for hearing accepting FNOV.
Slide 10	Post-event learning has been broad – mostly administrative in nature … working on engineering controls; including ▪ actions identified in the initial causal analysis and supplemental causal analysis, ▪ and other actions taken by the organization, Centers, Division, and Corporation. ▪ This event and its root causes were extensively discussed at the Center level and included in lessons learned discussions. **Division** ▪ focused on lessons learned communications, classification and security refreshers,

	VP ▪ communications to stress importance of security to Sandia Mission **Department** ▪ actions ▪ Developed administrative procedure ▪ All presentations originated internally require DC reviewed AND markings prior to presentation or posting ▪ Contracts changed – work performed on Sandia owned equipment ▪ Review of existing training and/or updated training expectations ▪ Awareness training ▪ Initial and on-going awareness of security topics ▪ Weekly "Security Minute" **Center** ▪ Retrospective view of Center security incidents ▪ Security Awareness Discussion **Lessons Learned** ▪ Division-level actions ▪ Lessons Learned Communication ▪ Security Flashes for every incident ▪ Division validation of corrective action effectiveness ▪ Security Pause - Staff asked for recommendations to improve security (over 500 recommendations received; increase awareness, increase DC, work on class network; Work, Planning and Control for security) ▪ Security Awareness Bulletin to Centers ▪ VP message to MOWs ▪ Operations Improvement Team ▪ Increased number of DCs ▪ Acknowledge those performing DC duties in Performance Evaluation and other monetary awards **Corporate** ▪ Review Corporate termination process by legal o make sure it covered the expectation and obligation of protecting knowledge gained while working at Sandia o consequences for not doing so ▪ Enterprise-wide search & analysis ▪ Updates to Corporate policy and training ▪ Announcements in Sandia Daily News ▪ Security Connection Website Lessons Learned ▪ Security Director LeaderWire message ▪ Security Speaker Bureau ▪ Additional communications by executive leadership and senior management

	▪ Security Director requesting managers to include a "Security & You Learning Minute" in staff meetings. (Review &Approval scenarios). ▪ Updates to Corporate Security Training including warnings related to working from home ▪ Labwide Special Announcement to MOW on Classified Information and DOEs "No Comment Policy" ▪ Corporate Lessons Learned posted to the Security Connection Website related to DOEs "No Comment Policy" on classified information in the public domain Bottom line: Extensive leadership communication to stress critical nature of security. **Other actions being considered/implemented:** o Classified e-mail marking o Classified working groups o Increase number of classified Video Teleconference rooms o Encryption opportunities for external partners o Logging Tool o Increase work on classified network o Modified PEP - moved improved security performance under executive leadership
Slide 11	Review and Approval process is a well-known and well-used process in place for classification reviews For years we have worked diligently to ensure an adequate number of DCs. Subject Matter Related Classification Awareness Briefings Security Incident Program (~3000 hotline calls to SIMP per FY) • 698 DC's • Formally trained & authorized • Adding 5,000 new e-DCs (classified Email-DCs) • An average of 900 requests per month for formal R&A • 10,800 per year • Security Assurance The assurance program encompasses the self-assessment process which includes: • Integrated Assessments with enhanced results documentation • Security Program Assessments • Security Coordinator Assessments • Manager Surveillances • Different approach to causals o ThinkReliability method implemented for cause analysis.

	- Utilizing the Cause Mapping tool has improved the way findings are analyzed, documented, communicated, and solved. - Incorporated risk management principles of DOE O 470.4B in self-assessment processes and scheduling of security topics. The objectives, to: - Prioritize security topics based on graded approach factors - Apply risk management principles - Prioritize and schedule based on risk factors **Security Incident Management Program** To prevent re-occurrence, the Team Lead analyzed the inquiry and developed lessons learned. SIMP Program Improvements: - Evidence collection, preservation & chain-of-custody - High level timeline as attachment in inquiry report - Version identification & sanitization - Over reliance on party involved and not enough research (**trust, but verify**) **Senior Security Manager Outreach** Purpose - help the line understand security is a partner in mission success Senior Managers in the field Meet with Division to - Talk about incidents, assessments, training - Understand security challenges - Provide timely solutions - Security Awareness & Training Most have been administrative in nature. Working toward engineering controls.
Slide 12	Sandia's most pressing security issue
Slide 13	Damage to reputation, loss of knowledge, unallowable cost, penalty