LA-UR-19-28921
Approved for public release; distribution is unlimited.

Title: EFCOG, IOSC Best Practices Guide

Author(s): Nelson, Wade F.

Intended for: Report

Issued: 2019-09-04

2019

EFCOG, IOSC Best Practices Guide

EFCOG IOSC SUB-WORKING GROUP TEAM
ENERGY FACLITY CONTRACTORS GROUP

Summary

Members of the Energy Facility Contractors Group (EFCOG), Safeguards and Security Working Group, Information Security Sub-Working Group Incidents of Security Concern (IOSC) Team prepared this best practice guide. For the purposes of this guide, "best practices" are "positive examples of work processes, procedures, good ideas, or effective solutions. The team made up of IOSC Subject Matter Experts (SME) identified these best practices as a result of actual operational experience and training.

The guide describes best practices for categorizing incidents and managing inquiries. These practices may serve as guidelines for developing program plans, policy and procedures. These practices are suggestions for Department sites to consider while working in the IOSC subject area. The authors acknowledge that there may be alternatives to the practices identified in this guide. Subject matter Experts from the IOSC program across the Department developed this guide.

Extensive discussion and document reviews were conducted to identify best practices relating to security inquiries. It was not within the scope of this study to assess individual site performance or evaluate compliance.

Department of Energy's (DOE), Order 470.4B, Chg.2, *Safeguards and Security Program*, July-21-2011, Chg 2, January-17-2017, Attachment 5, Incidents *of Security Concern*, contains the requirements for the IOSC program. In accordance with DOE directives and requirements established by DOE/National Nuclear Security Administration (NNSA) oversight, the working group evaluated elements of the IOSC program at each of the working group member's sites such as categorizing events, conducting inquiries, and reporting events. Inconsistencies in categorization across the sites may be due to various factors, including each local field office having different reporting expectations, subjectivity in making determinations, and potential inherent deficiencies in the categorization tables and category descriptions.

Many sites have adopted a sub reportable category for a security anomaly event that it believes does not meet the criteria as a reportable IOSC. The sites typically establish a local standardized process for reporting, analyzing, and trending sub-reportable events. Security incident program managers may need to discuss inconsistent categorization with other Inquiry Officials (IO) and suggest standardized solutions (ie…through policy changes or a forum attended by incident program managers and inquiry officials to discuss standardization solutions.

At least one EFCOG IOSC team member's site is currently using the best practices identified in this guide.

Information Security IOSC Sub-Working Group Team

H. Ray Hubbs, Consolidated Nuclear Security, LLC, (Y12) Team Co- Chair

Terran Robertson, Los Alamos National Laboratory (LANL) Team Co- Chair

Chris Bush, Savannah River Site (SRS)

Carly George, Sandia National Laboratory (SNL)

Seligman, Gregory R Sandia National Laboratory, (SNL)

Dan Frampton, Sandia National Laboratory (SNL)

Mike Colson, Idaho National Laboratory (INL)

Ruben Jimenez, Kansa City Plant (KCP)

John Brown, Oak Ridge National Laboratory (ORNL)

Tonya Stanger, Lawrence Livermore National Laboratory (LLNL)

Mic Daniels, Lawrence Livermore National Laboratory (LLNL)

Andrew Korson, Pacific Northwest National Laboratory (PNNL)

Alan Johnson, Pacific Northwest National Laboratory (PNNL)

Rob Taylor, Kansas City (KCP)

Natasha Wright, U.S. Department of Energy

Wade Nelson, Los Alamos National Laboratory (LANL) EFCOG SSWG Vice Chair

Table of Contents

List of Best Practices

** Best Business Practice #1**

Title: Consistent Categorization of IOSC's

Points of Contact:

H. Ray Hubbs, Y12, Wade Nelson, LANL

Brief Description of Best Practice:

This Best Practice describes steps to promote consistent categorization of incidents of security concern (IOSCs) and avoid isolated decision-making. Each site/facility establishes an IOSC program to ensure that the occurrence of a security incident prompts the appropriate graded response, including an assessment of the potential impacts, appropriate notifications/reporting, extent of condition, and corrective actions. The long-term management of incidents serves as an effective safeguards and security (S&S) program planning and management tool for enhancing site-specific implementation of security policies, as well as preventing the reoccurrence of IOSCs and improving S&S performance.

Under DOE O 470.4B, Safeguards and Security Program, site/facility operators have many alternatives with regard to how their IOSC program is designed, managed, and operated. This Best Practice describes common methods that may be used throughout the U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) to achieve the desired compliance.

Why the Best Practice was used:

This Best Practice was used to achieve multi-perspective and consistent categorization decisions.

What are the benefits of the Best Practice?

The benefits of this Best Practice include:

- increases consistency of categorization determinations across the Enterprise
- assures appropriate graded responses to IOSCs
- serves as lessons learned for other sites participating in determination discussion
- validation of thorough categorization process

What problems/issues were associated with the Best Practice?

Problems/issues associated with the Best Practice include:

- too many perspectives
- can increase consistency, but not result in uniformity
- differences in policy implementation by Field Offices result in compliant categorizations, but lack uniformity across the Complex

How the success of the Best Practice was measured:

This Best Practice was demonstrated by:

- effective utilization by the IOSC Sub-Working group for the past two years
- improved communication and collaboration, resulting in consistent categorization and management of the overall IOSC process

Description of process experience using the Best Practice:

DOE directives govern categorization of incidents but other/site documents can be used as supplemental/complimentary documents. DOE/NNSA uses a graded approach for the identification and categorization of IOSCs. Based on the preliminary inquiry and determination that an IOSC has occurred, DOE O 470.4B should be referred to for the reporting criteria and determination of the significance level category and incident type, with special emphasis on Attachment 5.3.d-g:

- Compromise: Evidence is provided that information was disclosed to an unauthorized person(s) (e.g., published by media, classified information was briefed to uncleared individuals, etc.).
- Suspected Compromise: Evidence is provided that there is a high probability that information was compromised. Although there is no clear indication of compromise (i.e., no direct recipient), the circumstances associated with the incident indicate that there is an obvious possibility that unauthorized disclosure did occur (e.g., classified information is transmitted by email outside of the organization's firewall, classified information is communicated on an unsecure phone line, etc.).
- Likelihood of Compromise is Remote: Although protection and control measures are violated, the circumstances associated with the incident indicate that there is a low possibility that information was disclosed to unauthorized personnel (e.g., classified information is left unsecured and unattended for a limited amount of time in an area accessed only by personnel with the appropriate clearance level, classified information is transmitted by email inside the organization's firewall and is discovered and isolated within a specified period of time.).
- Compromise Did Not Occur: Evidence is provided that there is no possibility that information was compromised.

While not all incidents fit neatly into any one category, it is the responsibility of the reporting organization to determine which level and incident type best describes the incident. Justification for the categorization (i.e., significance level and type) of the incident should be included in the initial notification.

Internal process for categorizing the event:

- local requirements as specified in program plan
- refer to decision trees (e.g., DOE-STD-1210-2012)

- precedence
- if sufficient mitigating factors are not identified within five days, categorize at higher level

Triage with local IOSC team(s)/stakeholders to:

- include local subject matter experts (SMEs)
- reverse engineer (step back through event in reverse order)
- play devil's advocate (multiple, contradictory perspectives)
- get others' perspectives/buy-in regarding the event
    - in the absence of consensus, ensure adequate justification exists to support categorization determination

Consult IOSC sub-working group members) to:

- reverse engineer
- play devil's advocate
- get others' perspectives regarding the event

Advantages of consulting with the EFCOG IOSC sub-working group team members include:

- achieving consistent results in categorization
- greater diversity of experience
- greater diversity of precedence
- unbiased objectivity/feedback
- collaboration to achieve standardization

Consultation with the local site office or DOE-HQ is a viable option for accurately determining the significance level/type of atypical incidents.

** Best Business Practice #2**

Title: Collaborative Categorization

Points of Contact:

Tonya Stanger, LLNL

Brief Description of Best Practice:

The assistance of Subject Matter Experts (SMEs), from such disciplines as Classification, CMPC, and/or Cyber Security when conducting an inquiry into an IOSC is often vital. Although the site-specific Program Plan will serve as the official guide when categorizing IOSCs, collaboration with the SME will assist with the determination. The SME may provide guidance or insights on the specific requirements of processes that are in question or assist in determining the actual level of risk involved in the IOSC. A SME may also provide technical assistance and assurance in the process of ruling out any disclosure of information. All information provided by the SME should be documented appropriately and stored within the case file. The information provided by the SME will not only be helpful in the categorization of the IOSC, but also support the development of interview questions prior to conducting interviews. In the final report, all information obtained by the SME should always be attributed to the SME.

Why the Best Practice was used:

To ensure accuracy regarding subject matter areas outside the IO's expertise.

What are the benefits of the Best Practice?

Significant reduction in the chance for error on the part of the IO.

What problems/issues were associated with the Best Practice?

Delay in classification review and classification challenges.
Forensics reviews were time consuming.

How the success of the Best Practice was measured:

Overall accuracy in determinations regarding the inquiry and accurate conclusions. Overall concurrence by owning organizations with outcome of inquiry (no pushbacks or complaint with outcome).

Description of process experience using the Best Practice:

Increase IO's confidence by using SME input throughout the investigative process.

** Best Business Practice #3 **

Title: Utilization of Published IOSC Reports for Continued Improvement Efforts in Incident Categorization

Points of Contact:

H. Ray Hubbs, Consolidated Nuclear Security, LLC, (Y12) Team Co- Chair

Brief Description of Best Practice:

In accordance with DOE Order 470.4B, Change 2, *Safeguards and Security Program*, July 21, 2011, Change 2, January 17, 2017, Attachment 5, *Incidents of Security Concern*, the sites establish a local standardized process for conducting inquiries. Inconsistencies in categorization across the sites may be due to various factors, including each local field office having different reporting expectations, subjectivity in making determinations, and potential inherent deficiencies in the categorization tables and category descriptions.

In an effort to better standardize IOSC categorization, two tools that might be utilized would be the DOE Incident of Security Monthly Program Report and the NNSA Office of Defense Nuclear Security Monthly Incidents of Security Concern Report that is published and distributed to the DOE /NNSA site federal program offices.

DOE uses a graded approach for the identification and categorization of IOSCs. This approach provides a framework for the requirements of reporting timelines and the level of detail for inquiries into, and causal analysis of, specific security incidents. By establishing a graded approach, line management can effectively allocate the resources necessary to implement this policy. Categorization is based on the subject policy and any additional criteria as documented in the site IOSC program plan

Why the Best Practice was used:

These monthly reports addresses security incidents, trends, and areas-of-concern for the month by providing a summarized description of both Category A and B security incidents, trending and analysis, and highlighting new changes throughout the DOE/Nuclear Security Enterprise (NSE) as it relates to the IOSC Program. Producing this monthly report coincides with requirements set forth by DOE O 470.4B and allows the DOE and Office of Defense Nuclear Security (DNS) Subject Matter Experts (SME) and management personnel to assess problematic areas or acknowledge good practices across the DOE Complex.

What are the benefits of the Best Practice?

As these reports are shared with the site contractor IOSC offices, the Inquiry Officials would have the opportunity to review inquiries and determine if one would agree with categorization, or find that a respective site might categorize differently. This exercise would spark conversation and could be used as a training aid and tool for consistent categorization.

IOSC SME's at the field level would be able to discuss their rationale for their categorization determinations.

What problems/issues were associated with the Best Practice?

At this time, this report is distributed to DOE/NNSA site Program Managers. It is up to that manager to share the report with the contractor IOSC office. With all stakeholders included in the distribution of the report, the report could be reviewed in a timely manner and shared with program staff.

How the success of the Best Practice was measured:

Success of this practice is measured by the discussions generated among IOSC inquiry officials and the concurrence/non-concurrence of the established categorizations reported.

Description of process experience using the Best Practice:

As there are few Departmental training aids for the incumbent Inquiry Official, these reports will serve as a training aid and enhance the likelihood of a more consistent approach to categorization determinations.

** Best Business Practice #4 **

Title: Utilization of the Equivalency and Exemption Process for IOSC Inquiries Related to the Introduction of Electronic Devices into Security Areas

Points of Contact:

H. Ray Hubbs, Consolidated Nuclear Security, LLC, (Y12) Team Co- Chair, and Wade Nelson., Vice Chair SSWG

Brief Description of Best Practice:

In accordance with DOE Order 473.3A, Change 1, *Protection Program Operations*, dated January 2, 2018, controlled articles such as portable electronic devices, both Government and personally owned, capable of recording information or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in Limited Areas (LA), Protected Areas (PA), and Material Access Areas (MAA), without prior approval.

Historically, incidents involving the introduction of unauthorized cellular phones and personal electronic devices into a LA, PA, or MAA would be considered an incident of security concern (IOSC), which would result in an IOSC inquiry to determine if there was a potential for compromise of classified or controlled unclassified information. In most cases, the incident is self-reported, and /or evidence suggests that the incident did not pose a direct risk of compromise of an asset.

In an effort to better standardize IOSC categorization and reduce the effort and cost associated with this type of incident, one tool that might be utilized would be the Equivalency and Exemption Process as described in DOE O 251.1D, *Departmental Directives Program*, Appendix E.

Use of an Equivalency/Exemption in IOSC reporting of incidents involving the introduction of such devices where evidence suggests the incident did not pose a direct risk of compromise of an asset. It would result in an incident inquiry called a sub-reportable (incidents that reflect non-compliance but do not rise to the level of a reportable IOSC. This incident inquiry would result in time and cost savings, as well as provide a basis for a more standardized reporting of such incidents.

DOE uses a graded approach for the identification and categorization of IOSCs. This approach will provide a framework for reporting incidents involving the introduction of unauthorized cellular phones and personal electronic devices into a LA, PA, or MAA where it is determined that sensitive information was not placed at risk as determined through forensic testing, interviews, and/or other appropriate inquiry methods. Inquiries should be based on the fact that although protection and control measures were violated, the circumstances associated

with the incident indicate there is a low possibility that information was disclosed to unauthorized personnel.

Why the Best Practice was used:

In a Y-12 Safeguards, Security& Emergency Services Management Report on Y-12 Cellular Phone Incidents (July 30, 2009), an evaluation of IOSCs involving the introduction of unauthorized cellular phones and personal electronic devices into security areas was conducted between 2005 and 2008. This evaluation revealed that only 1 out of 127 incidents (0.7%) resulted in reporting the potential for unauthorized disclosure of classified information. This reporting was due to the device being powered on and in the close proximity to a classified discussion. In 2007, of the 70 incidents of device introduction, 42 (61%) were in the security area 30 minutes or less and were not in the proximity of classified discussions or processing. Most of the incidents were self-reported (111 of 127 or 87%) with the remainder being discovered by Security Police Officers or employee supervision.. As this is the only study known the fact remains that assets spent on sub-reportable incidents is not cost affective.

What are the benefits of the Best Practice?

Upon implementing the electronic device Equivalency/Exemption, the time and effort expended will be reduced and a more realistic view of categorization and related metrics will be gained. Several sites have utilized this best practice to include: Los Alamos National Laboratory, Sandia National Laboratory and the Idaho National Laboratory.

What problems/issues were associated with the Best Practice?

No problems in the implementation of the Equivalency/Exemption was noted.

The monitoring of sub-reportable (NON IOSC) incidents is essential as it allows management to proactively address reoccurring incidents, thereby minimizing the occurrence of potentially more significant incidents. In addition, sub-reportable monitoring and data collection may assist in identifying repeat offenders, especially in cases where discovery was not reported.

How the success of the Best Practice was measured:

The cost of conducting an inquiry and reporting the incident as a reportable/categorized IOSC during the time of the evaluation was approximately $3,427.46 per incident prior to the Equivalency/Exemption (based on 2008 cost estimates). Utilizing the Equivalency/Exemption, the cost was reduced to $2,644.31 for the actions performed during the inquiry. That equated to an approximate cost savings of $61,085.72 (23%) for the 12-month period. Other time and cost savings may be realized as a result of other negated actions that might be required of a categorized incident, e.g., causal analysis, corrective actions, etc.

Description of process experience using the Best Practice:

There is no additional risk associated with the implementation of this reporting process. Sites will continue to prohibit controlled articles into security areas, thus overall security posture remains the same.

** Best Business Practice #5 **

Title: Consistent and Effective Risk Ranking

Points of Contact:

Mike Colson, INL; Chris Bush, SRS

Brief Description of Best Practice:

This Best Practice outlines specific elements that are evaluated and assessed for risk by assigning a score to certain incidents of security concern occurrences and events. Assessing risk for an incident of security concern is the first step in reducing the likelihood that the incident will recur. Risk ranking also drives a graded approach to causal analysis, corrective actions and follow up effectiveness reviews as well as tracking and trending of incident data (metrics).

It is of the utmost importance that the level of effort and detail for these assessment activities be commensurate with the level of risk associated with the incident being assessed. DOE Order 470.4B, Chg 2 and DOE-STD-1210-2012, dated September 2012 mandates that the risk ranking process be established in the site specific IOSC Program Plan.

Typical elements that are included in risk ranking of an incident of security concern include:

- Classification level and category of material involved
- Location of incident
- Likelihood of compromise
- Intent (i.e., willful, negligence, inadvertent),
- Management involvement
- Mission impact
- External reaction (i.e., publicity)
- Resource loss/damage
- Foreign National access to classified information

Risk ranking is done early in the IOSC inquiry process and before the causal analysis is completed. As more information becomes available during the inquiry and/or causal analysis, the risk ranking could change. If so, a new risk ranking should be performed using the newly acquired information. If a change in risk is determined, the causal analysis, corrective actions, and effectiveness review activities should be modified and documented accordingly.

Why the Best Practice was used:

The key word for why this Best Practice is needed is CONSISTENCY in how risk ranking is to be used.

DOE Order 470.4B, Chg 2 and DOE-STD-1210-2012, dated September 2012 provide guidance for IOSC risk ranking.

Contractor Assurance System provides additional guidance and requirements for managing risks for incidents of security concern. Additional risk assessments for contractor project management, safety audits, and operations risk assessments were being used in place of the approved Risk Ranking process for IOSCs described in the Program Plan.

Contractor personnel felt that to achieve their organizational goals, they had no choice but to use the tools available. This proves to be problematic in that personnel who are not trained Inquiry Officials are making judgement calls on the risks associated with incidents of security concern.

What are the benefits of the Best Practice?

Establishing a Best Practice for Risk Ranking will ensure consistency among the groups as it pertains to integrating risk management into the procedures and processes of the organization. It will also assist in providing a link to determining and communicating where the risks reside and who is responsible for assessing, addressing, and identifying causal factors and corrective actions for them.
Other benefits include:

- Provides security education and awareness program topics for incident lessons learned to share in a proactive and timely manner.
- Consistency in how incidents of security concern are evaluated and assessed risk and which elements are to be included in the risk ranking process.
- Clear guidance in assigning appropriate risk using descriptive criterion that does not elicit private or personal interpretation

What problems/issues were associated with the Best Practice?

Personnel and organizations responsible for incident occurrences are often tasked with analyzing incidents of security concern and developing corrective action to prevent reoccurrence. For those unfamiliar with the IOSC process, the rationale used for incident determinations at times are not understood. Lack of knowledge and awareness of facility personnel working in a non-security environment may not be aware of information protection requirements and treat it differently than what is required. Operations personnel deemed the event to be a Conduct of Operations issue and handled it accordingly. Additionally:

- Facility personnel using other organization risk ranking and causal analysis documents and procedures that are inconsistent with the risk ranking process used for incidents of security concern program plan..
- Use of the IOSC Risk Ranking Score Sheet contained in the DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, dated September 2012 without proper authorization or training leading to inaccurate risk ranking scoring due to personal interpretations.
- The IOSC Risk Ranking Score Sheet contained in the DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, dated September 2012 does not cover all events associated with incidents of security concern. It should be noted that the current Risk Ranking Score Sheet identifies National Security Information (NSI) as a “0” risk. Consideration to modify the risk to a “1” which more accurately assess the risk to

classified during the next revision of the Standard. Sandia National Laboratory has modified their Risk Ranking Score Sheet with approval of their Field Office and added it to their IOSC Program Plan

How the success of the Best Practice was measured:

Program effectiveness is measured by proper incident identification, categorization, and risk assessment so that issues or concerns are timely addressed and corrected to prevent recurrence.

The Risk Ranking Score Sheet contained in the DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, dated September 2012, and provides a foundation on which to build a better Risk Ranking Score Sheet. However, the success of changes recently made in risk ranking have not been evaluated as of this writing. Once approved and incorporated in the Best Practice guidance document, time should be allotted to evaluate and determine its performance effectiveness.

This Best Practice is not intended to take the place of current Risk Management procedures in use or development, to include DOE G 413.3-7A 1-12-2011, or site-specific procedures, but should be vetted through the EFCOG Community and the DOE Office of Enforcement.

Security incidents involve unique considerations that warrant special handling within the corrective action program. Incidents of security concern are ranked as High, Medium or Low risk, determined by scoring a predetermined number of incident elements and adding up the scores. Attachment 1, IOSC Risk Ranking Score Sheet, describes a Best Practice risk ranking process to objectively determine the level of risk caused by an incident of security concern.

Should the final risk ranking score reach High risk, the responsible organization performs an effectiveness review of the incident. It is also recommended that effectiveness reviews be conducted for all actions associated with Medium risk incidents.

Description of process experience using the Best Practice:

This best practice is in the DRAFT stage and once approved will be recommended for inclusion in site specific IOSC Program Plans.

In keeping with DOE Order 470.4B requirements and DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, dated September 2012, properly assessing the risks associated with incidents is imperative as doing no less has the potential to negatively impact national security and the collateral impact with other programs and security interests.

It is recommended that certain definitions and terms contained in EFCOG Guidance Document: Reporting Programmatic and Repetitive Non-compliances in NTS and SSIMS prepared by the EFCOG Safety Working Group Regulatory and Reporting Technical Subgroup, December 2015 be referenced with the Risk Ranking Score Sheet.

** Best Business Practice #6 **

Title: In-house Cyber Forensics Expertise

Points of Contact:

H. Ray Hubbs, Y12; John Brown, ORNL

Brief Description of Best Practice:

Prior to July 2007, sanitization of desktops, laptops and servers was being conducted via on-site visits by cyber-security or subcontract personnel. These personnel were specially trained in order to conduct approved sanitization processes, and had to be Q-cleared in order to perform such tasks. The individual sanitization of one machine could take as much as eleven hours, depending on the size of the hard drive, and the size of the cleanup itself. This added a lot of frustration on the part of the end users, as machines could be confiscated and locked up until someone could visit the area and sanitize the issue. Loss of productivity was a key factor in looking for a more appropriate solution to the sanitization issue.

Why the Best Practice was used:

At the Y-12 National Security Complex and the Oak Ridge national Laboratory, the sanitization process underwent a transformation, as a process for remote sanitization by IOSC personnel was presented to management, subsequently being approved by both management and the NNSA Production Office. Administrative privileges were granted to IOSC Inquiry Officials that would allow for access to all Exchange server accounts (Outlook), desktops, laptops, tablets, and network servers that are on the local domain. This access would allow for connectivity to a user's hard drive, and any network drives associated with their account user id. Access to the login script server was also granted, so that IOSC staff can ensure that all network servers in the login script can be searched for issues.

What are the benefits of the Best Practice?

This remote sanitization effort will save time and money, as time for remote sanitization of one machine could take as little as thirty minutes. Also, end users would not be without the use of their machine during the sanitization process, as had occurred in the past. The IOSC staff can connect remotely to more than thirty machines at a time, scanning and sanitizing as issues are discovered.

What problems/issues were associated with the Best Practice?

The first issue was getting the appropriate permissions to all of the network drives, hard drives, and mobile device servers in the plant. The second issue was getting the appropriate computer equipment to manage multiple open Windows screens in an efficient manner (more memory, processor speed, etc.).

How the success of the Best Practice was measured:

The success was measured by ensuring productivity is minimally impacted without affecting DOE Order compliance. Based on current categorization of IOSCs, rapid sanitization with immediate notification results in the reduction of risk to classified information.

Description of process experience using the Best Practice:

The remote sanitization process is comprised of several different steps. The first step is to ensure that the issue is resolved on the Exchange server as quickly as possible to ensure no further contamination is allowed. After the Exchange server has been sanitized, the IOSC staff will move on to hard drives and network servers, including the personal folders in Outlook (if the option is enabled). Sanitization of these areas is concluded in the timeliest manner possible. Typically, you will see one of the IOSC staff working on the Exchange server exclusively, while the desktops and network drives are being searched by another member of the IOSC staff.

** Best Business Practice #7 **

Title: Conducting Effective Interviews

Points of Contact:

Tonya Stanger, LLNL

Brief Description of Best Practice:

Conducting an effective interview requires a skill set for which, ideally, IOs should be formally trained.

Preparation is the key to an effective interview. The IO should know prior to the interview exactly what information needs to be elicited from the interview subject and have those questions written down so that nothing is forgotten during the interview. Ideally, the interviewer should already know as much about the incident as possible, including the answers to some of the questions to be asked to determine the truthfulness of the interview subject.

At the onset of the interview, the IO should introduce themselves and clearly explain the purpose of the interview, as well as answer any questions the interview subject may have at that point. IOs are not authorized to detain individuals for interviews or to obtain sworn statements; however, they may conduct interviews with the consent of participants and obtain signed statements.

It is important that the IO remember the purpose of the interview is to find the truth, rather than a "guilty party." Often, IOSCs will involve employees who, through carelessness, inattention, or ignorance, made "honest mistakes" and want to set things right. Here is where an experienced IO will look to "the Golden Rule" and ask themselves how they would like to be treated if they were seated on the other side of the interview table. An interviewer should avoid presenting themselves as an interrogator. Respect and courtesy will go a long way towards an effective interview.

The IO should present the interview process, and the end-product written statement, as the subject's opportunity to present "their side" of the incident. Should the interview subject decide that they do not wish to continue the interview it is their right to do so, however, this action should be documented for the purposes of the written IOSC report.

The end-product of the interview should be a signed statement with which the interview subject is wholly satisfied. This may require multiple edits, but ultimately results in a statement which truly represents the interview subject's input regarding the incident.

Why the Best Practice was used:

This practice is used to elicit accurate and honest input by individuals involved in the IOSC.

What are the benefits of the Best Practice?

Subjects should be put at ease and not felt like they are being “interrogated”. Interview subjects are inclined to share more detailed information and elaborate on statements.

What problems/issues were associated with the Best Practice?

N/A

How the success of the Best Practice was measured:

The attainment of accurate, detailed statements from individuals involved in the IOSC.

Description of process experience using the Best Practice:

Using a more relaxed interview process leads to individuals to open up and share more, those who feel threatened, may close up and end the interview early. These interviews are completely voluntary, and the individuals can leave whenever they determine they are done. It’s in the IO’s best interest to have a relaxed, cooperative interview.

** Best Business Practice #8 **

Title: Managing Offsite Events

Points of Contact:

H. Ray Hubbs, Y12

Brief Description of Best Practice:

The purpose of this Best Practice is to provide the inquiry official a basis for conducting inquiries where the inquiry and/or evidence may lead off-site. The inquiry official must be able to verify statements and evidence relative to the inquiry. Evidence might include procedures that describe a process. The inquiry official must be able to verify that the process, especially one leading off-site, was indeed followed.

DOE O 470.4B, Attachment 5, Section 1, states that Inquiry Officials are responsible for conducting the inquiry and maintaining all documentation associated with the inquiry. Specific actions must at least include:

(1) Collect all information and physical evidence associated with the security incident. Physical evidence collected must be controlled and a chain-of custody must be maintained.

(2) Identify persons associated with the incident and conduct interviews to obtain additional information regarding the incident.

(3) Reconstruct the security incident to the greatest extent possible using collected information and evidence. The reconstruction should include a chronological sequence of events that describes the actions preceding and following the incident.

(4) Identify any collateral effect to other programs or security interests.

Why the Best Practice was used:

Reasonable and relevant inquiries depend upon the unique nature of the incident. If there is question over what is believed to have taken place, it may be reasonable to locate further witnesses or to examine relevant evidence which may have been identified from physical evidence or to determine if policy and procedures were correctly followed.

What are the benefits of the Best Practice?

Positive actions in the period immediately after the report of an incident minimizes the amount of evidence that could be lost to the inquiry, and maximizes the chance of securing evidence that could assist in determining whether a compromise has occurred. In those cases where compromise could not immediately be ruled out, this rapid response could serve to minimize the potential impact on the Department and/or national security.

What problems/issues were associated with the Best Practice?

In those cases where a sub-contract facility may be located at another site, a MOU/MOA might be required between IOSC programs to ensure rapid response to security incidents.

How the success of the Best Practice was measured:

In one instance, information was collected on specific processes and procedures involving interstate shipments of unclassified waste. Although subject matter experts and process representatives indicted that procedures were followed, independent follow-up indicated that the procedures, in this instance, were not followed as prescribed.

Learning from this experience, the practice of "Trust, But Verify" was initiated in another inquiry where the Inquiry Official was dispatched to the evidentiary location immediately after the incident was reported. In this case, there were no sites closer to the location where another Inquiry Official would be logically utilized. This immediate response provided the Inquiry Official with "eyes on" of the evidence and afforded a rapid review of the facility physical security posture and protection capabilities. In addition, the Inquiry Official was able to obtain consensual witness statements and document evidence as required. From this on-site perspective, the Inquiry Official was able to relate relevant information to management for subsequent actions as deemed necessary.

Description of process experience using the Best Practice:

Given the fact that DOE/NNSA interests span the entire country, incidents have the opportunity to affect multiple sites. If a security incident affects more than one site/facility under the purview of a single Program and/or Site Office, that office must assign responsibility to a lead organization. If the sites/facilities fall under the purview of multiple Program Offices, those offices must, by mutual agreement, decide on a lead organization with responsibility for the inquiry. In some instances, evidence associated with the inquiry might lead the Inquiry Official outside the confines of that site, especially where no other site is within proximity to the evidence.

** Best Business Practice #9 **

Title: Managing IOSC Case Files

Points of Contact:

Andrew Korson, PNNL

Brief Description of Best Practice:

IOSC case management encompasses the processes and techniques used to move the inquiry from one stage to another, such as the initial response and notifications, conducting interviews, and evidence reviews, analysis, report writing and final documentation in case files. This Best Practice encompasses a process for making sure all case files are complete, well organized and of sufficient quality to meet DOE requirements for documenting results of inquiries. The practice includes development of a local checklist that specifies in detail all of the information that should be included in the case file, such as evidence collected, cyber records, results of interviews, statements, report results, cause analyses, corrective actions, and other information. The checklist also covers proper categorization and marking of the record, and is used in the final step to close out every incident.

Why the Best Practice was used:

DOE Order 470.4B describes the minimum documentation requirements for an IOSC. Without specificity and consistency that aligned with the Laboratory's processes, this led to variations in quality of IOSC case files. PNNL adopted a more detailed case file management process that includes the minimum requirements but also provides enough specificity for Inquiry Officials so that all case files meet our quality standard and were consistent.

What are the benefits of the Best Practice?

The biggest benefit is that management has a very high degree of confidence that IOSC case files not only meet minimum DOE requirements, but also our own standards for high quality and consistency. This makes it much easier to review previous files when looking for repetitive and recurring events, or when analyzing for tracking and trending purposes.

Additionally, when case information is needed to support external requests for information, such as during assessments, audits or other similar activities, it can be provided quickly and completely.

What problems/issues were associated with the Best Practice?

There were no significant issues or problems associated with implementing this best practice. The most likely issue to arise is failure to follow the practice for all cases, such that a review determines that one or more cases does not comport with the checklist requirements. Attention to

detail by the IOSC Program Manager in reviewing all closed files to verify that Inquiry Officials are complying with the checklist is needed to keep quality level high.

How the success of the Best Practice was measured:

The measure of success for this best practice is improvement in quality and completeness of documentation, which translates directly into higher quality inquiries, and improved performance during internal and external reviews.

Description of process experience using the Best Practice:

Our experience with this best practice has been very positive. Since implementing this checklist approach to managing case files, we have received consistent positive reviews from auditors during assessments, not only on the organization of the files, but also in the quality of information contained therein. This includes a site assist visit from the Office of Enforcement, who specifically mentioned this best practice as a significant positive program element to Laboratory management during the site assist visit out brief.

** Best Business Practice #10 **

Title: Inquiry Official Field Kit

Points of Contact:

Mike Colson, INL; Ruben Jimenez, KCP; John Brown, ORNL

Brief Description of Best Practice:

Development of an Inquiry Official (IO) field kit to ensure that IO's have the necessary documents, tools, and equipment staged, ready to respond to reported incidents. Field kits can contain such items as witness statements, screwdrivers, cameras, gloves, etc. that may be needed for inquiry into a reported event. Consistent field kits allow IO's to "grab and go" and have the knowledge that what they require for an incident response is always ready.

Why the Best Practice was used:

Field kits were developed to ensure Inquiry Official had necessary documents, tools, and equipment when responding to incidents in the field where access to such items may be necessary for timely response.

What are the benefits of the Best Practice?

The best practice ensures timely and consistent response to reported incidents. It allows Inquiry Officials to effectively respond to incidents in the field with the knowledge that the pre-developed field kit has the necessary items they need to conduct an inquiry.

What problems/issues were associated with the Best Practice?

Responding to reported incidents without the appropriate documents, tools, or equipment sometimes leads to an inconvenient time loss response to events while trying to locate needed resources. Additionally, certain key steps may be missed due to not having appropriate documents or tools available, ie. Sanitization of media.

How the success of the Best Practice was measured:

Effectiveness was measured by determining how and when the kit was used amongst staff members in the organization. Success stories were shared and available to validate having a Field Kit being useful to the Inquiry process.

Description of process experience using the Best Practice:

Tool kits that have been developed pre-incident reporting ensure that documents, tools, and equipment needed have been readily accessible to responding IO's. This has prevented IO's

from having to stop preliminary investigations to locate items needed. Field kits have allowed necessary steps to be performed when needed for rapid containment.

Elements of a Field Kit:

Field Kits should contain the following items:

- Property Receipts
- Witness Statement Documents
- Risk Ranking Worksheet
- Notebook
- Nylon or Rubber Gloves
- Evidence Bags (clear plastic and paper bags)
- Evidence Seal Tape
- Tape Measure
- Flashlight
- Mini-Tool Kit for removing computer hard drives and other items
- Electro-static Free Hard Drive Evidence Bags
- Copies of procedures for sanitization and clean-up of electronic media
- Phone lists of cyber security support personnel
- Phone lists of Security Contacts to include Mgmt. notifications
- IOSC Field Handbook (in development – step by step guide to handle incidents)
- Copy of the DOE IOSC Technical Standard to assist with categorization

** Best Business Practice #11 **

Title: Use of Credentials for Inquiry Officials

Points of Contact:

Chris Bush, Savannah River Site (SRS)

Brief Description of Best Practice:

As a Best Practice, the Inquiry Official Certification Process supports the foundation of a trained Inquiry Official. This Best Practice utilizes a DOE issued badge type credential to identify the bearer as having authority to perform assigned official duties as an Incident of Security Concern (IOSC) Inquiry Official (IO).

Possessing valid credentials verify that the IOSC member has fulfilled all training and qualification requirements for the position or duties and is empowered through the issuance and use of DOE credentials during IOSC inquiries and investigations.

Why the Best Practice was used:

Credentials are issued to contractor employees whose official duties include conducting employee interviews related to an incident of security concern, safeguards & security investigations, inquiries, and/or assessments. In lieu or in addition to an appointment letter from the authorizing Officially Designated Federal Security Authority (ODFSA), credentials can also be used as an official form of identification during company IOSC inquiry investigations. Dependent upon the employee's access authorization, the credential may include authorization to transport Restricted Data and/or other classified information.

What are the benefits of the Best Practice?

Credentials are issued only to those who have successfully met the training requirements set forth by the organization's Qualification/Certification Program Requirements. In addition, credentials allow ready identification as an inquiry official and is easier to maintain than a paper copy of the appointment letter.

Other benefits of credentials include:

- Enables trust between the IOSC Program and other facility and site programs
- Provides identification and credence for greater interoperability between departments and federal facilities on the same site DOE, EM, PF, OIG.
- Fosters credibility when presented during inquiry interviews
- Establishes authority in performance of roles and responsibilities
- Paves the way for a smoother investigation when evidence collection and reconstruction is required

- Provides authority for physical and logical access (IT systems) to site and organization premises during the conduct of the inquiry

What problems/issues were associated with the Best Practice?

- Federal authorities throughout the DOE complex may or may not approve of the use of issuing credentials to Inquiry Officials.
- There are a few sites that issue credentials to the manager of the IOSC Program and not to Inquiry Officials.
- Failing to maintain training qualification or proficiency as an Inquiry Official can lead to revocation of the credential.
- Retrieving credentials from previously trained Inquiry Officials who are no longer in that role.
- Credentials can be easily lost, stolen or misplaced.

How the success of the Best Practice was measured:

Measuring the effectiveness of the use of credentials by an Inquiry Official was conducted by using said credentials during several preliminary inquiry investigations. Alternatively, in other inquiry investigations, the Inquiry Official presented the letter from the ODFSA to those responsible and/or involved in the inquiry investigation process. (see below)

- Workplace Violence
- Information Spillage
- Unsecured Repository
- Unauthorized CUI Transmission
- Unattended CUI
- Introduction of Personal Smartphone into a Limited Area
- Onsite Interaction with Other Onsite Agencies (DOE, OIG, OCI, Protective Force, Human Resources, General Counsel, etc.,)

Description of process experience using the Best Practice:

It is postulated that the contrast in the response received is merely how one perceives the seriousness of the incident in terms of whether they were the person responsible, involved, or the person who discovered the incident.

There are sites where Inquiry Officials have already been issued IOSC credentials. It is important to have consistency in how IOSC conducts business. Credentials not only establishes Inquiry Officials as authorities, but subject matter experts in the IO investigative process.

In conclusion, When an Inquiry Official possess credentials, it is evidence of authority, status, entitlement, privileges and the rights to conduct an effective and thorough IOSC inquiry investigation that ensures risk to national or facility security interests have been properly evaluated.

** Best Business Practice #12 **

Title: Inquiry Official Certification Process

Points of Contact:

Lisa Kaneshiro, SNL

Brief Description of Best Practice:

The purpose of this Best Practice is to provide the appointing designated Federal entity, CSO, and Incident of Security Concern Program Manager, a consistent process for training and certifying new Inquiry Officials (IOs), ensuring consistency throughout DOE by outlining methodology to:

- Identify a potentially qualified IO candidate;
- Enterprise-wide and site-specific classroom and online training;
- Outline formalized On the Job Training (OJT) and
- Identify tools to adequately document and maintain training records.

Why the Best Practice was used:

DOE O 470.4b, Chg. 2, Safeguards and Security Program, Section 5, "Safeguards and Security Training Program," requires that site/facility management "establish programs that ensure personnel are trained to a level of proficiency and competence that ensures they are qualified to perform assigned safeguards and security (S&S) tasks and/or responsibilities."

What are the benefits of the Best Practice?

The best business practice will enable the IOSC program manager to hire, train, and certify the most qualified personnel to process Incidents of Security Concern (IOSCs). The methodology ensures timely, consistent, and adequate response to IOSCs, ensuring protection of national security information and will prepare a new IO for success and long term sustainability in their career.

What problems/issues were associated with the Best Practice?

Inconsistencies in how Inquiry Officials are trained throughout the complex led to variations in categorization of IOSCs and quality of reports. Inadequate training ultimately sets the IO up for failure and could result in the loss of Classified Information.

How the success of the Best Practice was measured:

Effectiveness of the methodology was measured using performance results, surveys, peer reviews and semi-annual review of the program to ensure all aspects still applied and new ones were added when necessary.

- After OJT, how did the new IO perform?

    - Ask them about the training process
        - What were the holes in the training?
    - Did they get all the tools they felt they needed to succeed?
- Management performance measurement
- Job satisfaction survey
- Survey of IOs that retain long term success and those that left the program due to lack of success (Exit Survey)
- Peer review of product
- Required semi-annual review of training and certification program

Description of process experience using the Best Practice:

- Identification of a potentially qualified IO candidate
    - Can the candidate obtain a Q clearance? If necessary, is the candidate willing to obtain Sigma 15 authority?
    - Can the candidate respond to interview questions intended to measure minimum aptitude in levels such as recall and observation, and situational judgment and reasoning?
    - Does the candidate have previous investigative experience or departmental inquiry official training (preferably both)?
    - Does the candidate have the aptitude to become knowledgeable of appropriate laws, executive orders, departmental directives, and/or regulatory requirements?
- Enterprise-wide and site-specific IO classroom/online training
    - Physical Security Systems courses offered through the DOE National Training Center (NTC)Information Security courses offered through the NTC:
        - ISC-121DE, Introduction to Classified Matter Protection and Control (CMPC)
        - ISC-141DE, Operations Security (OPSEC) Overview
        - ISC-202DE, Legal Aspects of Inquiries
        - ISC-221, Classified Matter Protection and Control I
        - ISC-241, Operations Security (OPSEC)
        - ISC-301, Conduct of Inquiries
        - DOE, 320 Causal Analysis and Corrective Action
        -
    - Derivative Classifier training
    - Safeguards & Security Information Management System (SSIMS) Data Entry and Query Training
    - International Association of Computer Investigative Specialists (IACIS)
    - No Comment Policy training
    - Ethics training
    - Cybersecurity Awareness training
    - Initial COMSEC training
    - Insider Threat Awareness training
    - Records Management training

- On-the-job training (See Attachment 1)

- OJT will vary from site to site depending on nature of work and types of incidents that regularly occur. Attachment 2 includes an example of OJT training relevant to Sandia National Laboratories and can be used as a template for other DOE sites to develop their OJT specifics.

Documentation and annual reviews of the methodologies used to train IOs at each program are essential to the success of an adequate certification process. This will ensure that individuals holding positions as IOs receive the training and development opportunities needed to become proficient and competent in the performance of their assigned IO responsibilities. Appendix B contains a Position Qualification Card used at SNL that can be used a template for development of site-specific documentation if needed.

Attachment 1: Example, OJT Instructors and Participants Procedure

Attachment 2: Example Inquiry Official Certification Documentation

For Copies of Attachment, 1-2, Please Contact

Greg Seligman, Sandia National Laboratory, IOSC Manager

Attachment 3: Sample IOSC Risk Ranking Score Sheet

INCIDENT ELEMENT		SCORE
Highest Classification Level	5: Top Secret 3: Secret 2: Confidential 0: No classified information directly involved	
Highest Classification Category	2: Restricted data 1: Formerly Restricted Data 0: National Security Information, or no classification category directly involved	
Caveats	5: Sensitive Compartmented Information (SCI) 5: Special Access Program (SAP) 3: Nuclear Weapon Data (NWD) 2: Other 0: Not Applicable	
Location	5: Offsite 3: In Property Protection Area 1: In Limited Area 1: In Protected Area 1: In Material Access Area (includes HRP Designated Locations) 0: Physical Location not directly involved	
Disclosure Status (Loss or Compromise of Classified)	5: Did occur 3: Likely occurred 1: Unlikely to have occurred 0: Did not occur, or classified information not directly involved	
Intent	5: Willful 3: Gross Negligence 1: Negligence 0: Inadvertent	
Management Involvement	5: Senior Level Management involved (contributed) or responsible 3: Mid-Level Management involved (contributed) or responsible 2: Front Line Management involved (contributed) or responsible 1: Management aware 0: Management unaware	
Mission Impact	5: Significant program or project interruption (<90 days) 3: Failure to meet DOE or client milestone 1: Failure to meet internal organization milestone 0: No significant mission impact	
External Reaction	5: National Headlines; high level DOE involvement in investigation and/or enforcement action 2: Regional headlines; official inquiries from high level DOE (HQ) 1: Local headlines (all media): no significant inquiries from DOE 0: Little or no public interest; no DOE inquiries	
Resource Loss/Damage	5: Loss or damage to equipment/facilities >$1M 3: Loss or damage to equipment/facilities $100K to $1M 1: Loss or damage to equipment/facilities $10K to $100K 0: Loss or damage to equipment/facilities <$10K	
Additional Contributing Factors (Choose all that apply)	1, 3, or 5: Programmatic Issue (usually involves issues in administrative or management controls □ Weakness in administrative or management controls □ Broad management or process control problem exists □ Need for broad corrective actions	
	1, 3, or 5: Repetitive Event (usually involves multiple instances of different types of issues that include substantially similar conditions, organizations or programs)	

	□ Two or more similar incidents of security concern □ Same or similar causal factors □ Less than adequate implementation of identified corrective actions or corrective actions that were not or less effective in preventing recurrence.	
	1, 3, or 5: Recurrence (usually involve multiple instances of the same type of issue) Self-explanatory	
	2: Electronic transmission outside firewall	
	1: Electronic transmission inside firewall	
	3: Foreign national involved from sensitive country	
	1: Foreign national involved from non- sensitive country	
Total Score/Risk Ranking High: >=16 Medium: 8-15 Low: <8		

A. Programmatic

As cited in EFCOG Guidance Document: Reporting Programmatic and Repetitive Non-compliances in NTS and SSIMS prepared by the EFCOG Safety Working Group Regulatory and Reporting Technical Subgroup (December 2015), "A programmatic problem generally involves some weakness in administrative or management controls, or their implementation, to such a degree that a broader management or process control problem exists and requires broad corrective actions."

Moreover, if it is determined that the incident was a result of problems, events or conditions that is within management's control, then rigorous corrective actions are required to improve management or process controls from a programmatic sense (Subgroup, 2015). Corrective actions are designed to effectively act as lessons learned and heighten awareness of personnel so that the incident does not recur.

Ranking Programmatic Events

□ Weakness in administrative or management controls
□ Broad management or process control problem exists
□ Need for broad corrective actions

One event equals 1
Two events equal 3
Three events equal 5

B. Repetitive

Certain issues, events, or incidents are certain to reoccur if corrective actions do not adequately address the causal factors for the event. A good litmus test as to whether corrective actions adequately address the causal factors for an incident, is whether the incident being investigated is a repeat occurrence.

Issues, events, or incidents that do not occur at the same time yet have similar causal factors or circumstances (involve substantially similar work activities, event location, lost or unaccounted equipment) may be deemed repetitive. Recurrence would not be possible if corrective actions for previous incidents were properly implemented and communicated (Subgroup, 2015).

Ranking Repetitive Events

□ Two or more similar incidents of security concern
□ Same or similar causal factors

 Less than adequate implementation of identified corrective actions or corrective actions that were not or less effective in preventing recurrence.

One event equals 1
Two events equal 3
Three events equal 5

Reference

EFCOG Guidance Document: Reporting Programmatic and Repetitive Non-compliances in NTS and SSIMS prepared by the EFCOG Safety Working Group Regulatory and Reporting Technical Subgroup (December 2015).

Attachment 4: Sample IOSC File Checklist:

For unclassified files:

- ☐ Cover Sheet
- ☐ Copy of SSIMS notification (if Category A)
- ☐ Copy of email notification to management and DOE
- ☐ Risk Ranking form
- ☐ Critique Report (if formal critique held)
- ☐ SSIMS Report (if Category A)
- ☐ Lab/Site IOSC Report (if Category B)
- ☐ Cause Analysis Report (if a separate document, or not included in IOSC Report)
- ☐ Corrective Action Plan (if a separate document, or not included in IOSC Report)
- ☐ Action tracking system report showing actions are complete
- ☐ Signed Infraction Reports (if infractions issued)
- ☐ Copy of email to DOE Site Office indicating closure
- ☐ Relevant supporting documentation (offending emails/documents; logs; statements; photos, etc.)
- ☐ Proper marking (OUO or unclassified) on every page

For classified files:

- ☐ Comment sheet in unclassified file indicating the full report is in safe
- ☐ Classification Cover sheets, front and back
- ☐ Working paper form (if file is not closed)
- ☐ Classified Document Title Page (if file is closed)
- ☐ Classification Determination from Classification Office
- ☐ Copy of SSIMS notification (if Category A)
- ☐ Copy of email notification to management and DOE
- ☐ Risk Ranking Form
- ☐ Critique Report (if formal critique held; include both classified and unclassified versions, as applicable)
- ☐ Signed Nondisclosure forms (if applicable)
- ☐ Computer Sanitization Report (if sanitization was required)

- ☐ SSIMS Report (if Category A)
- ☐ Lab/Site IOSC Report (if Category B)
- ☐ Cause Analysis Report (if a separate document, or not included in IOSC Report)
- ☐ Corrective Action Plan (if a separate document, or not included in IOSC Report)
- ☐ Action tracking system report showing actions are complete
- ☐ Signed Infraction Reports (if infractions issued)
- ☐ Copy of email to DOE Site Office indicating closure
- ☐ Relevant supporting documentation (offending emails/documents; logs; statements; photos, etc.)
- ☐ Proper classification markings on every page in document