U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

INCIDENTS OF SECURITY CONCERN UPDATE

Proposed Changes to DOE 470.4B Attachment 4 and IOSC-related requirements as part of DOE Integrated Project Team (IPT)

OVERVIEW

- Purpose and Priorities
- Sub-Working Group (SWG) Makeup
- Stakeholder Engagement and Feedback
- Significant Proposed Changes
- Challenges
- Anticipated Impacts
- Path Forward

PURPOSE

BLUF: avoid having similar or even identical events being reported differently at different locations/sites)

- Improve consistency and reduce subjectivity of reporting requirements across the Complex while maintaining local oversight (ODFSA) ability to adapt to local needs and risks
- Improve clarity
  - Adjust “should” to “must”
  - Use consistent terminology
  - Improved definitions
- Categorization and initiation IOSC notification report within 5 business (vs. calendar) days
- Consistent objective list of reportable events
- (Added later) Infractions & Violations consistent with Federal Requirements
- (Added later) Capture NISPOM requirements

PRIORITIES

- Background:
  - Developed a wish list of everything SWG members and participants wanted to see changed
  - Clarified these wishes based on group consensus
  - Distributed wish list for feedback to broad audience of stakeholders
- **Result: Overwhelming support and consensus for the SWG path forward (wishes to pursue vs. not pursue)**

Sub-Working Group Makeup

- **BLUF: Diverse SWG and participation ensured broad representation and awareness of diverse needs and context across the Complex**
  - Ensured the new proposed requirements were not focused on a smaller sub-set of Complex members
- IPT solicited participants who were nominated
- 2 experienced IOSC Program Leads as SWG co-leads
- Over 20 SWG members from across the complex (DOE & NNSA) (Labs, sites represented, topical areas)
- Over 20 SWG participants solicited from other IOSC Programs and other topical areas as needed (OE, MC&A, PERSEC (CPSO), CUI, Export Control, Legal)

STAKEHOLDER ENGAGEMENT

- Over 100 stakeholders
- Solicited SMEs from broad topical areas with proposed changes/impacts
- Solicited input from all SWG members and participants
- Asked all SWG members and participants to distribute information to their identified stakeholders
- IPT co-chairs distributed to their designated stakeholders
- Included IOSC Advisory Panel

SIGNIFICANT CHANGES (NOT INCLUDED)

- All IOSCs in SSIMS
- Develop unclassified database for all IOSCs across Complex (e.g., U-SSIMS)
- Extend Cat A IOSC Closure beyond 90 days
- Limit IOSCs to events impacting SNM or classified material
- Report only infractions/violations to CPSO

SIGNIFICANT CHANGES (ADDITIONS)

- Clarified loss/theft of badges
- Clarified when IOSCs “closed”
- Clarified consistency/subjectivity
- Clarified definitions of Cat A and B IOSC Categories, Types, and related processes
- Identified specific reportable events and provided examples of As and Bs
- Defined culpability (intent) and provided examples
- Reduced “site” specific language to be more inclusive of all IOSC Programs (contractor and federal)
- Should/may → must/will
- Consolidated IOSC Program Plan requirements

ADDITIONS (CONT.)

- Clarified compromise types (suspected/potential, occurred, remote)
- Infractions and Violations
- Clarified Graded Approach
- Investigated (and incorporated and eliminated some) redundant reporting streams (ORPS, Cybersecurity)
- Limited IOSC reporting to events with direct security impact/nexus
- 5 business days and “clock” starting point (and allowances for extensions with ODFSA approval)
- New terms: PIOSC, disposition, violation, security asset (vs. interest), suspected → potential compromise
- Clarified responsibilities to include processes and damage assessments for Significant Nuclear Defense Intelligence Losses
- Clarified roles for IOs in training

ADDITIONS (CONT.)

- CPSO reporting for infractions and violations
- Special Reporting Situations (SRS) types incorporated for DOE and NNSA
- Specify sanitization processes, designate Cyber as primary stakeholder in carrying out and establishing requirements
- Clarified FIE and SAP responsibilities
- Clarified contingency notification options when SSIMS unavailable
- Clarified requirements for loss/theft/diversion SNM
- Clarified IOSC reporting requirements for CUI in accordance with new CUI requirements
- Reportable based on merits at time of event (vs. discovery or subsequent mitigations)
- Incorporated guidance/info from DBT

CHALLENGES

- Sync NNSA and DOE requirements
- Redundant Reporting Streams (ORPS, Cyber)
- Local Oversight Flexibility
- 5 “business” days
- National Security Presidential Memo 32
- Dealing with timeline exceptions
- Changes to SSIMS (i.e., violations)
- Stakeholder Identification and Engagement
- Future of IOSC Standard

IMPACTS

- Local Flexibility → Complex Consistency
- SSIMS changes (AU/EHSS)
- DOE Infractions (and Violations)
  - Significantly more infractions
  - More CPSO engagement/reporting
  - DOE Infraction Form (DOE 5639.3) update
- More comprehensive IOSC Program Plans
- Removal of the current Standard (DOE-STD-1210-2012)

PATH FORWARD

- Continued stakeholder engagement and review (before RevCom)
- Into RevCom Aug. 30, 2023
- Published Feb. 16, 2024
- Questions/further discussion
  - alan.johnson@pnnl.gov (Alan Johnson)
  - grselig@sandia.gov (Greg Seligman)