



Incidents of Security Concern Revision

DOE M 470.4-1, Section N

Zero-Based Policy Review

Evaluation and Feedback Working Group

May 6, 2008



Evaluation and Feedback Working Group



- SMEs from HS-71, HS-81, Oak Ridge, Pantex, and PNNL
- Consolidated Working Group and HS-81 initiatives
 - Solicited feedback for revision of IMI tables
 - HS-81 SSIMS/ITAC staff
 - HS-43 Office of Security Enforcement
 - DOE and NNSA Incident SMEs from the field
 - DOE M 470.4-series topical area SMEs



Current Program Issues



- All assets/events within a topical area are not appropriately captured, defined, and/or categorized
- Lack of structure within the tables
- Inconsistent initial notification and inquiry report content



Current Program Issues (cont.)



- Confusion regarding closure date determination
- Inability to account for incidents/events of management interest
- Difficulty in changing IMI rating
- IMI-4 incidents lack tracking and trending



Why Revise the IMI Tables?



- Descriptors too broad or unclear
- Assets and/or events (i.e., incidents) not covered
- Inconsistent application of IMIs
- Redundancies in reporting (i.e. CIAC, ORPS, CI)



Why Revise the IMI Tables? (cont.)



- IMIs have not kept pace with current trends and issues
 - New technology
 - ACREM
 - PII
 - Security failures
- Need to account separately for events of Management Interest
- “Catch all” IMIs



Proposed Methodology



- Evaluate all topical areas by assets and events (incidents)
 - Provide a mechanism for adding, modifying, or deleting existing IMI categories sorted by the topical areas
 - Create new method for identifying events of Management Interest
- Align IMIs with the topical areas of the DOE M 470.4-series (with SSIMS structure) for improved reporting, tracking, and trending
- Improve process for reporting, updating, and closing incidents



Proposed Methodology (cont.)



- Improve process for notification to upper management
- Eliminate “catch all” IMIs
- Revise the reporting time requirements
 - IMI 1 and 2 will remain same
 - IMI 3 and 4 will become 24 hours



Proposed Methodology (cont.)



- Numbering system

– X1.Y1.Z1.X2.Z2

X1 = initial severity (IMI 1, 2, 3, or 4)

Y = topical area (2 – Physec 3 – PF, 4 – IS, 6 – MC&A, 1 – Mgmt Interest)

Z1 = event (theft = 1, loss = 2, etc.)

X2 = final severity (IMI 1, 2, 3, or 4; may stay the same or could up/downgrade)

Z2 = final event (theft = 1, loss = 2, etc.; may stay the same or change based on inquiry)



Path Forward



- Finalize draft DOE M 470.4-1, Section N
 - Finalize IMIs
 - Update the process flow diagram
 - Address time for discovery vs. determination
 - Revise report content
 - Clarify closure requirements
 - Clarify root cause and corrective actions requirements



Path Forward (cont.)



- Meet with the OCIO to resolve overlapping cyber security reporting requirements
 - PII: Electronic vs. Hard copy
 - Dual reporting of cyber security incidents such as intrusions and compromises
 - Unauthorized computer use (personal misuse)
- Develop an incident reporting guide
- Update SSIMS incident module



??????

QUESTIONS

??????



Numbering Example



1.3 Confirmed or suspected loss, theft, or diversion of Category I or II quantities of special nuclear material (SNM).

Loss of Cat II

- X = 2 (IMI)
- Y = 6 (MC&A)
- Z = 3 (loss)
- X2 = 2
- 2.6.3.2 = IMI1, MC&A, loss, IMI2

Theft of Cat II

- X = 1 (IMI)
- Y = 6 (MC&A)
- Z = 1 (theft)
- X2 = 2
- Z2 = 3 (loss)
- 1.6.1.2.3 = IMI1, MC&A, theft, downgraded to IMI2, event has been downgraded to loss

Diversion of Cat II

- X = 1 (IMI)
- Y = 6 (MC&A)
- Z = 2 (diversion)
- X2 = 1
- 1.6.2.1 = IMI1, MC&A, diversion, stays IMI1



Numbering Example



1.5 Confirmed or suspected loss, theft, diversion, unauthorized disclosure of Top Secret information, Special Access Program (SAP) information, or Sensitive Compartmented Information (SCI), regardless of the medium, method, or action resulting in the incident.

Verbal Disclosure of Top Secret - Confirmed/Compromise

- X = 1 (IMI)
- Y = 4 (IS)
- Z = 4 (disclosure)
- X2 = 1
- 1.4.4.1 = IMI1, Infosec, verbal disclosure, stays IMI1

Verbal Disclosure of Top Secret - No Compromise

- X = 2 (IMI)
- Y = 4 (IS)
- Z = 4 (disclosure)
- X2 = 2
- 2.4.2.2 = IMI2, Infosec, verbal disclosure, stays IMI2



Proposed Events



Events	Z1	Definitions
1	Theft	The removal of Government property and/or materials from a DOE or contractor operated facility without permission or authorization and contrary to law.
2	Diversion	1. the unauthorized removal of special nuclear material from its approved use or authorized location. 2. an act that attempts to reposition the protective force to a location other than where the actual adversarial action is taking place.
3	Loss	The inability to locate Departmental interest.
4	Shipper Receiver Gain	DRAFT
5	Shipper Receiver Loss	
6	Marking	
7	Transmission Hard Copy	
8	Transmission Electronic	
9	Unauthorized Discharge	
10	Intentional Discharge/Use of Force	
11	Protective Force Fatality or Injury	
12	Procedural	
13	Access Control	
14	Unauthorized Removal	
15	Inventory Difference	



DRAFT

Proposed Information Protection Table



EVENTS	Event Condition	ASSETS			
		IMI-1 (1hr)	IMI-2 (8hr)	IMI-3 (24hr)	IMI-4 (24 hr)
Information Protection					
Theft		All Classified, OGA, NATO, FGI, PII (?)		OUO, UCNI, NNPI, ECI,	
Loss	Confirmed/suspected Compromise - based on evidence	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20, ACREM, PII	SRD, S/FRD, S/NSI, C/RD, OGA	C/FRD, C/NSI, NATO, FGI	OUO, UCNI, NNPI, ECI,
Transmission Electronic-(fax, e-mail, phone call, etc.) (discuss Firewall/compromise/No Compromise)	No Compromise	PII	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20	S/RD	All others
Transmission Electronic (fax, e-mail, phone call, etc.)	Confirmed/suspected Compromise - based on evidence	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20, ACREM, PII	S/FRD, S/NSI, C/RD, OGA	C/FRD, C/NSI, NATO, FGI	OUO, UCNI, NNPI, ECI,
Transmission Hardcopy (paper, slides, ESM, etc.) to include hand carry	No Compromise (same as electronic except S/RD)	PII	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20		All others
Transmission Hardcopy (paper, slides, ESM, etc.) to include hand carry	Confirmed/suspected Compromise - based on evidence	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20, S/RD, PII	S/FRD, S/NSI, C/RD, OGA	C/FRD, C/NSI, NATO, FGI	OUO, UCNI, NNPI, ECI,
Verbal Disclosure	Confirmed/suspected Compromise - based on evidence	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20, S/RD, PII	S/FRD, S/NSI, C/RD, OGA, any disclosure to a foreign national	C/FRD, C/NSI, NATO, FGI	OUO, UCNI, NNPI, ECI,
Verbal Disclosure	No Compromise		TS/SCI/SAP/Sigma 1, 2, 14,15, and 20		All others
Improper Handling - other than verbal; includes destruction	No Compromise		TS/SCI/SAP/Sigma 1, 2, 14,15, and 20		All others
Improper Handling (example: visual disclosure, i.e., improper escorting) (examples: Classified information placed/processed on an unapproved system) includes destruction, ACREM not put into accountability, classified on unclassified system	Confirmed/suspected Compromise - based on evidence	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20, S/RD, PII	S/FRD, S/NSI, C/RD, OGA	C/FRD, C/NSI, NATO, FGI	OUO, UCNI, NNPI, ECI,
Improper Storage (Also includes not properly securing [lock and/or alarm] containers, vaults, vault-type rooms)	No Compromise		TS/SCI/SAP/Sigma 1, 2, 14,15, and 20		All others
Improper Storage (Also includes not properly securing [lock and/or alarm] containers, vaults, vault-type rooms)	Confirmed/suspected Compromise - based on evidence	TS/SCI/SAP/Sigma 1, 2, 14,15, and 20, S/RD, PII	S/FRD, S/NSI, C/RD, OGA	C/FRD, C/NSI, NATO, FGI	OUO, UCNI, NNPI, ECI,
Disclosure through Controlled Article					



DRAFT

Proposed MC&A Table



EVENTS	Event Condition	ASSETS			
		IMI-1 (1hr)	IMI-2 (8hr)	IMI-3 (24hr)	IMI-4 (24 hr)
NMC&A					
Theft		Cat I , II, III, IV SNM		Nuclear Material	
Unauthorized Removal from a MBA where the removal crosses a security areas [e.g. PPA, LA, PA, MAA] boundary		Cat I and II SNM		Cat III and IV SNM	Nuclear Materials
Improper Storage (Also includes not properly securing [lock and/or alarm] containers, vaults, vault-type rooms)	no compromise				Cat I - IV, Nuclear materials
Diversion (confirmation of an intentional act)		Cat I , II, III, IV SNM		Nuclear Materials	
Loss (missing item qty or process difference; time period is more immediate)			Cat I and II SNM	Cat III and IV SNM	Nuclear Materials
Inventory Difference (w/in an MBA; distinction of time (over a period of time)			Cat I and II SNM	Cat III and IV SNM	Nuclear Materials
Shipper Receiver Gain (came from external)			Cat I and II SNM		Cat III, IV and Nuclear Materials
Shipper Receiver Loss (came from external)		Cat I and II SNM		Cat III and IV	Nuclear Materials
Handling (unauthorized movement from an MBA where removal does not cross the security area boundary)			Cat I and II SNM		Cat III & IV and Nuclear Materials



DRAFT

Proposed Management Interest Table



EVENTS	Event Condition	ASSETS			
		IMI-1 (1hr)	IMI-2 (8hr)	IMI-3 (24hr)	IMI-4 (24 hr)
Management Interest					
Any Arrest on DOE property excluding public access areas			any person (employee or non-employee)		
Arrest of DOE cleared personnel in HRP			any DOE or contractor employee		
Any Detaining on DOE property excluding public access areas with physical restraint (e.g. hand cuffs)				any person (employee or non-employee)	
Attacks An act directed against Departmental assets or personnel that whether successful or unsuccessful, that could result in damage or loss of Departmental property/assets, the environment, injury to Departmental or contractor employees, or the public		All other assets		Gov't Property >\$10K	
Demonstration/Protest (this assumes Peaceful if not then it should fall under attacks)					Any person
Non-willful breach or entry (inadvertant; unintended) by the public - does not include authorized visitors - that penetrates a security boundary	(need to differentiate btwn crashing thru a door and crashing thru a pidas and fleeing in the guide)			Cat I & II; BSL 5 & 4 facilities; Security Area (SCI, SAP, TS, Sigmas 1, 2, 14, 15, & 20)	Cat III & IV, BSL 1-3, , security area non-SNM; Radioactive Mat'l Facility
Investigation (LLEA/federal LEA) - this pertains to criminal investigation				any DOE or contractor employee	
Labor Strike or threat of strike that impacts the security posture			actual DOE or contractor employee strike	threat of any DOE or contractor employee strike	
Suspicious Activity (suspected - Surveillance/watching/casing); Incidents of apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees or protective force, unusual calls for information, etc.).				Any person/activity	
Threats ; Detection of activities involving individuals who have been confirmed as physically watching/casing/surveillance or planning a terrorist-type attack		Any person/activity			



DRAFT

Catch All



IMI-3.4, Confirmed or alleged non-compliance with laws or DOE directives/standards that jeopardizes protection of the facility or site security interests

IMI-3.4 8/1/05 - 7/31/07

	Non incident/Rescinded	2
controlled articles	Cell Phone w/Conversation in secure area	2
	Cell Phone w/Conversation during Class Discussion	1
	Cell/Camera 1 hr +	2
	Cell in SCIF	2
Improper Handling/Storage/Transmission/ Destruction of Classified	Marking	2
	Handling	15
	Storage	40
	Transmission	15
	Destruction	1
Policy/Procedure Violations	Policy/Procedure violations - Property/Removal	2
	Non Compliance	7
	Badging procedures	4
	No security Plan	1
	Improper storage of weapon	1
	Improper Escort	9
	Disposition of Hard Drive not positively ID	1
	Improper storage of Classified Degraussed Hard Drive	1
	Classified Info Discussed/Voicemail unsecure phone	3
	Non HRP SPO's allowed access to DAF	1
	Unsecured VTR/MAA/LA/Security Area	12
	Failure to Report DUI	1
	Class on unapproved system	6
	CREM Not in accountability	3
	Facility Termination	1
	Access Problems	1
Unauthorized use of unclass computer	1	
Misc	Lost Keys	2
	Admin Error	2
	Subcontractor Drug Possession	1
	Malfunction of system	1
		143



DRAFT

Catch All



IMI-4.17 8/1/05 - 7/31/07

IMI-4.17, Other

Continues to be used but is not a valid incident number.

Protection of Classified	Failure to secure class no likely disclosure	1
	Protection of Classified	19
	Improper Transmission of Classified	1
	Improper Storage of ACREM	9
	ACREM not in accountability	2
	Unauthorized Acces to CDIN	1
	Protection of Information	14
Protection of OOU	Improper Handling	3
	Improper Marking	6
	Protection of OOU	20
	Improper Transmission of OOU	5
Policy Violations	Improper Escort	9
	Unauthorized Computer Use (personal/Porn)	18
	Unauthorized Access to SRSNet	2
	Unattended Crypto Ignition Key	2
	Unsecured Door/Seal (MBA/Cat IV)	10
	Non compliance with procedures	11
	Accidental Destruction of OOU	1
	Lost OOU Documents	1
	Unauthorized Access to Site Entrance	3
	Prohibited Articles (Cell, Thumb Drive)	7
	Employee (Waste/Fraud/Abuse Govt Resources)	2
	Employee (Threating/Disgruntle)	2
	Argus Unsecure	1
	Class on Unclass system	1
	Improper Protection Cat IV	1
Misc.	Expired badge	1
	Stolen/Lost/Missing (Laptop, Badge, Cell)	3
	Accountable Inventory Discrep	1
	Suspicious Behavior (taking pictures)	1
	System Failure	1
	Denial of Service	1
	Inaccurate Shipping Documents	1
		161