IA Insecurities

Technical Security Solution Center (I912)

Diane Strohmer

I9121

Insecurity Overview

- NSTISSI 4003 Revision
- Trends Analysis for CY2008 & CY2009
- Reporting Problems
- Lessons Learned
- Final Analysis

COMSEC Incident Reporting & Evaluation System

- **NSTISSI-4003:** National Security Telecommunications & Information Systems Security Instruction – 4003 (CNSS-4003)
- **Revisions**

NSTISSI-4003 Revisions

- **Responsibilities - Controlling Authorities shall:**
  - Provide assessments/recommendations for keying material they control to the Monitoring Activity and NSA
- **Added Incidents**
  - Incidents involving Electronic Key Processing
  - Incidents involving secure wired/wireless devices
  - Incidents involving CIK/Cards that can be associated with it's equipment.
  - Unauthorized maintenance to COMSEC equipment, (i.e., deviates from established standards or administered by unqualified individuals)

NSTISSI-4003 Major Changes Cont.

- **Greater emphasis on:**
  - Detailed Reporting
  - Investigations
  - Nuclear Command and Control Incidents
  - CCI Reporting
  - Counter Intelligence Support
- **Additional Annexes:**
  - Example Reports
  - NC2 Incidents

Trend Analysis

National COMSEC Incident Reporting System DATABASE

CIRS

COMSEC Incidents CY 2008/2009

	CY08	CY09
Air Force	366	500
Army	612	588
Navy	251	314
Marines	119	79
Coast Guard	58	119
NATO	5	6
Civil Agency	75	68
DOD	57	67

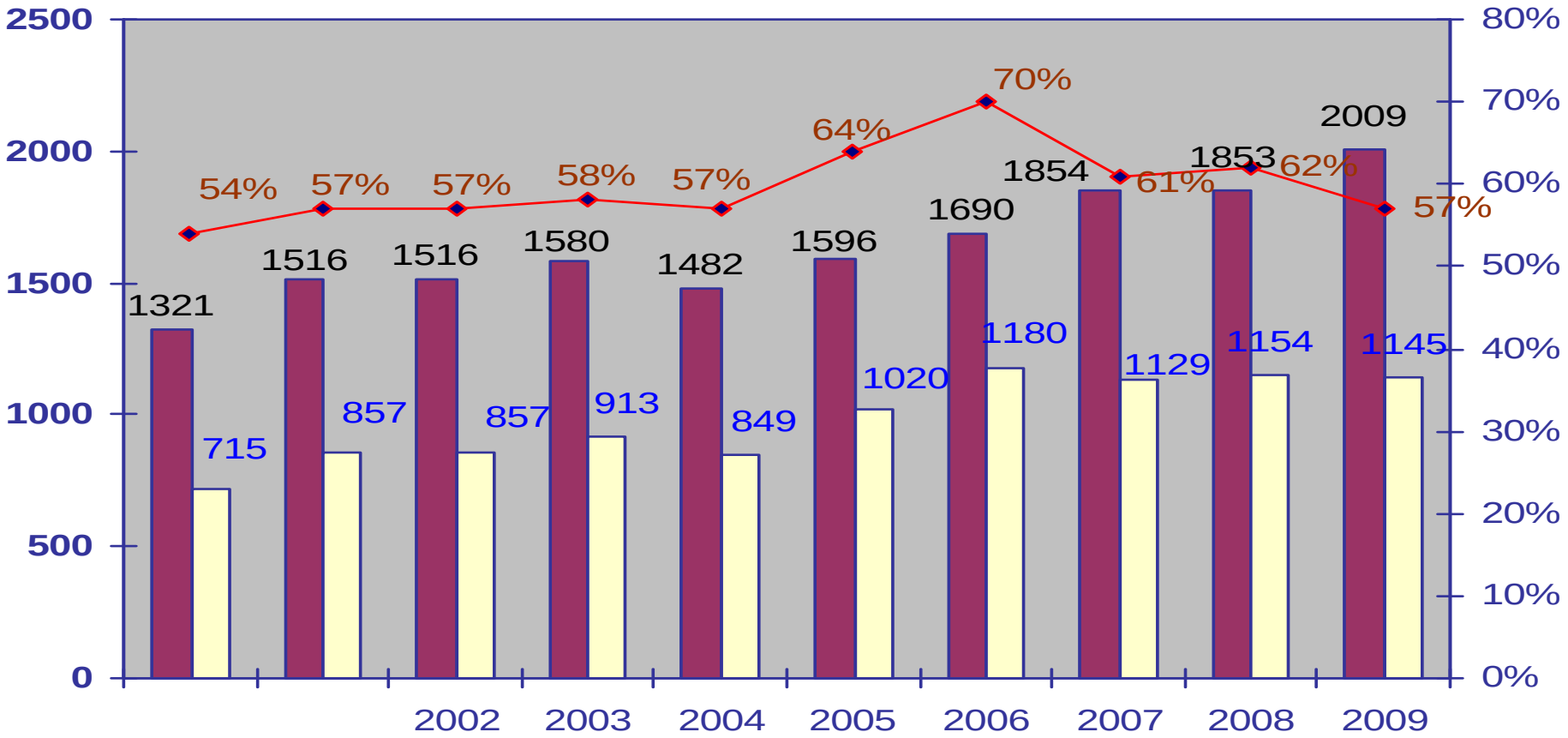
COMSEC Incidents CY 2008/2009 Cont.

	CY08	CY09
NSA	65	36
Contractors	203	219
Bilateral	28	11
DCS	0	0
USPS	4	0
Commercial Carrier	9	1
Total cases	**1853**	**2009**

Incident Breakdown by Command & Service

Service	TOTALS	Area Unassigned	CENTCOM	EUCOM	NORTHCOM	PACOM	SOCOM
Air Force	500	22	31	50	**316**	81	0
Army	588	1	137	68	**270**	93	19
Bi-Lateral	11	0	4	**1**	1	2	0
Civil Agency	68	6	1	1	**60**	0	0
Coast Guard	119	21	17	0	**66**	14	1
Courier Services	1	0	0	0	**1**	0	0
Contractors	219	1	1	1	**214**	1	0
DOD	67	2	1	0	**55**	5	4
Marines	79	52	**7**	0	17	3	0
NATO/Allied	7	0	0	**7**	0	0	0
Navy	314	3	13	3	**263**	32	0
NSA	36	3	2	2	**29**	0	0
Totals	2009	112	214	133	**1296**	230	24

Yearly Comparison



CY 2009 Evaluations

- 57% Total Insecurities (Comp+CCRO)
  - 5% Compromise
  - 52% CCRO
    - ✓ 2008 Insecurities 62% (10% decrease)
- 36% No Compromise
- 1% PDS
- 6% Pending Evaluation

CY09 Incident Physical Locations

- Aircraft 56
- Area Not Specified 69
- Communications Center 02
- Field 54
- Multiple Locations 78
- Office / Plant / Lab / Production Areas 1,502
- Residence 12
- Ship 192
- Vault / Closed or Non-User Area (SCIF) 6
- Vehicle 35

CY09 Incident Violator Positions

- Commercial Carrier ……8
- Courier ……10
- Custodian ……642
- Depot Personnel …… 17
- Not Provided in Report …… 45
- Plant / Lab / Production Personnel …… 28
- User …… 1261

CY09 Incident Material Types

- Ancillary Devices (CFD/DTD, etc.)……78
- Classified Device……195
- Documents / Publication……15
- Key (Including Proms / CIKS)……879
- Nuclear Command & Control……02
- Other Material (safe combos, non-CCI)…… .13
- Paper Systems……94
- Parts (die, chips, wafers, boards, tri-graph)……12
- Unclassified/Unknown at time of case entry…… 0
- CCI Equipment……749

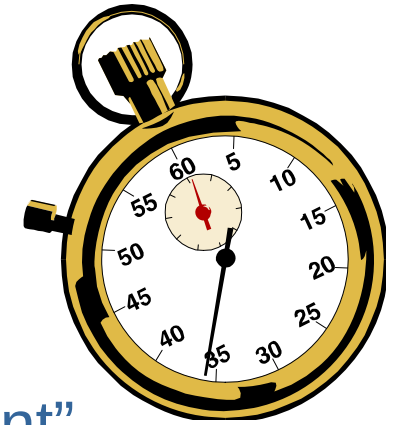
CY09 Insecurities Major Trends

- Permanent physical loss - 39%
  - 32% no explanation
- Destruction irregularities - 2%
- Unattended/Abandoned - 12%
- Cryptographic violations - 4%
- Unsecured safe/vault - 5%
- Unauthorized access - 10%
- Other - 28%

(Production, shipping, distribution, damaged packaging, and accounting errors)

Problems in Reporting

- ✓ Initial Reports Not Timely
- ✓ Not Addressed to Major Players
  - ALL ContAuths, Monitoring Activity, NSA, Chain of Command (Ensure evaluation authority is ACTION Addressee)
  - Evaluation authorities need assessments
- ✓ Include Office Symbols (I9123)
  - Old office symbols better than none
  - (I01P3, I413, V514, X81, X71A)
- ✓ Subject line need the words “COMSEC Incident”
  - Indicate if amplifying and/or final



Problems in Reporting (cont.)

- ✓ Lack of Detailed Information
- ✓ Lost Material
  - When last sighted?
  - Was equipment keyed? What key?
- ✓ Location/Operation
  - Not Just Longitude/Latitude
  - Iraqi Freedom & Enduring Freedom
- ✓ Unclass systems (Internet) <u>are not</u> OK for reporting

Problems in Reporting (cont.)

- ✓ Include recommendations to prevent recurrence
  - Re-train
  - Re-brief
  - Update security/operational procedures
  - Don’t need to include
    - reprimands/punishments

Final Analysis?

Possible Solutions

- Leadership Awareness / **Intervention** - COMSEC Incidents
- Increased COMSEC Account Manpower - **Primary Focus**
- Good COMSEC Account **Incentive Programs/Awards**
- Mandatory Annual COMSEC **Web-Based Training**
- Monitoring Activities Support Increased **Trends Analysis and Awareness**
  Provide feedback to Department/Agencies COMSEC Community.
- Incident Investigations – Forward **Summarize Findings** in Final Reports
  To Support Trends Analysis and Counter Intelligence.

********** YOUR THOUGHTS **********

- Recommendations / Suggestions - Send to: **iainsecurities**@nsa.smil.mil

Questions/Comments

IA Insecurities (I9121) Contact Us

STE/STU III - (410) 854-6811

Secure Fax (410) 854-6793

DSN - 244-6811

SIPRNet: iainsecurities@nsa.smil.mil

Diane Strohmer, USAF/Gov Contractors - ddstroh@nsa.smil.mil

Jack Urbanski, USA/DoD/Civil Agencies/NSA/NATO - jeurban@nsa.smil.mil

Connie Thomas, USN/USMC/USCG – cmthom5@nsa.smil.mil