DIAC

SPECIAL ACCESS PROGRAM TRAINING BULLETIN

D5-800, DIAC
Number 9

PROGRAM DEVELOPMENT OFFICE

202-373-4073
March 1991

Reporting Security Violations

During the recent DUSD(SP) inspection of DIA SAP management procedures, the comment was made that each program's security plan should contain procedures for reporting, investigating, and resolving security violations.

"Security violation" is a commonly used term that implies a loss or compromise of classified information and subsequent corrective or disciplinary action.

Each program's security plan should contain procedures for reporting, investigating, and resolving security violations.

Procedures used in investigating and resolving possible compromises of classified information are explained in DoD 5200.1-R and DIAR 50-2. The DIA SAP Manual, DIAM 56-3 (draft), contains further guidance for when the possible compromise involves SAP material.

The following is a brief summary of steps to take to report a possible security violation involving SAP material (refer to above references for a complete explanation):

1. *Report.* If you suspect that SAP information may have been compromised, inform the program security officer or program control officer and the OSC VAD[redacted] If the suspected compromise involves computer security, the program control officer will inform DS.

2. *Investigate.* The program control officer ensures that a preliminary inquiry is conducted. The program director and the OSC VADD review the results of the preliminary inquiry to determine whether a compromise took place, to determine if any further investigation is necessary, to correct any systemic problems that may have contributed to the violation, and to direct a damage assessment if appropriate.

3. *Resolve.* A final report of the investigation is made to the DIA SAPOC which may recommend further remedies and relief from accountability of any lost materials.

While few security violations result in a compromise, all violations should be reported and investigated. The violation not reported may do the most damage.

If procedures for reporting security violations are not in your security plan, include them when the manual is updated.

SAP Training Seminar
27 March 1991
0930
Room D5-800

SPECIAL ACCESS PROGRAM TRAINING BULLETIN

D5-800, DIAC
Number 9

PROGRAM DEVELOPMENT OFFICE

202-373-4073
March 1991

Reporting Security Violations

During the recent DUSD(SP) inspection of DIA SAP management procedures, the comment was made that each program's security plan should contain procedures for reporting, investigating, and resolving security violations.

"Security violation" is a commonly used term that implies a loss or compromise of classified information and subsequent corrective or disciplinary action.

Each program's security plan should contain procedures for reporting, investigating, and resolving security violations.

Procedures used in investigating and resolving possible compromises of classified information are explained in DoD 5200.1-R and DIAR 50-2. The DIA SAP Manual, DIAM 56-3 (draft), contains further guidance for when the possible compromise involves SAP material.

The following is a brief summary of steps to take to report a possible security violation involving SAP material (refer to above references for a complete explanation):

1. *Report.* If you suspect that SAP information may have been compromised, inform the program security officer or program control officer and the OSC VADD [redacted] If the suspected compromise involves computer security, the program control officer will inform DS.

2. *Investigate.* The program control officer ensures that a preliminary inquiry is conducted. The program director and the OSC VADD review the results of the preliminary inquiry to determine whether a compromise took place, to determine if any further investigation is necessary, to correct any systemic problems that may have contributed to the violation, and to direct a damage assessment if appropriate.

3. *Resolve.* A final report of the investigation is made to the DIA SAPOC which may recommend further remedies and relief from accountability of any lost materials.

While few security violations result in a compromise, all violations should be reported and investigated. The violation not reported may do the most damage.

If procedures for reporting security violations are not in your security plan, include them when the manual is updated.

SAP Training Seminar
27 March 1991
0930
Room D5-800
