LOSS OF CONTROLLED CRYPTOGRAPHIC ITEM IN AFGHANISTAN

1. On 29 Jul 08, the DSA was advised of the loss of a Controlled Cryptographic Item (CCI) from the Camp Palomino Control Reporting Centre (CRC), Kandahar Airfield Afghanistan. The item is a Sectera wireless terminal (SWLT) which was last accounted for on 24 May, 08. The loss was reported after an inspection of all CCI holdings on 30 May 08.

2. The item, when not in use, is stored with other sensitive CCI equipment in the CRC safe 5. A search of the safe and related areas has failed to locate the item. No explanation has been offered, as to its loss, other than the possibility that it was discarded after being inadvertently dropped into a rubbish bin within the communications security (COMSEC) annex during a security audit of CCI items. Further unsuccessful searches were conducted of rubbish bins and the relevant rubbish disposal points.

3. The investigation revealed a number of circumstances that have contributed to the loss of this item. The DSA is aware of improvements since implemented by the CRC. DSA supports these improvements and further recommendations, as resulting from the routine inquiry and reflected in the enclosed minute.

4. Should you wish to discuss this matter further, my POC is Ms Jacinta Blanks, (02) 6266 4205.

Peter Grace
DSII
07 Nov 08

Enclosure:

A. Minute, Loss of Controlled Cryptographic Item in Afghanistan, dated 10 Oct 08.
LOSS OF CONTROLLED CRYPTOGRAPHIC ITEM IN AFGHANISTAN

Background

1. On 30 May 08, at Camp Palominos Control Reporting Center (CRC), Kandahar Airfield (KAF), Afghanistan, conducted a physical inspection of all key material and Controlled Cryptographic items (CCI) stored in of the CRC, the communications security (COMSEC) annex, demolish area and radar cabinet. Following the inspection, reported that a Sectra Wireless Terminal (SWLT) was missing.

2. The future narrow band digital terminal (FNBTD) device enables a secure exchange of voice, data and faxes over a normal phone line.

3. Every piece of controlled cryptographic items is accounted for on COMSEC Accounting Reporting Distribution System (CARDS). The CARDS is the only way to account for the equipment, capabilities, access or installations which each user then initiates and controls.

Investigation

5. The missing CRC SWLT was issued locally to as an UNCLASSIFIED, model 1BDT1907XDSF, General Dynamics Sectera.

6. The last time the SWLT had been accounted was on 24 May 08, by.

7. After reporting the loss, immediately conducted a search of the safe, COMSEC annex, rubbish bins, skip and burn pits but was unable to locate the SWLT. A subsequent search of the COMSEC annex was also unsuccessful.

8. On 12 Jun 08, FLTLT Gary Mott of ADFIS notified DSA SIC of the security incident.

9. On 24 Jun 08, Captain (CAPT) A. Russell, Routine Inquiry Officer (RIO) conducted an interview with the custodian, who explained:

   a. the SWLT was not keyed;
   b. the SWLT was observed missing during a security equipment check;
   c. a full search of the safe, COMSEC annex and surrounding areas could not locate the SWLT;

DE-CLASSIFIED
d. he was the only one with access to the safe to conduct CCI checks;

e. the last time the CCI were checked was on the 24 May 08, where the items were moved to a workbench for checking, due to poor lighting;

f. following inspection, the CCI's were returned in their packing box to the shelves;

g. that it is possible the SWLT fell into the bin next to the technicians workbench and this is consistent with a previous incident when a phone cable was salvaged from the same rubbish bin;

h. on 24 May 08 and 30 May 08, he removed the rubbish from the COMSEC annex and did not check the bin prior to disposal;

i. there was no difference noticed in the weight of SWLT packaging when it was returned to the shelf; and

j. the plastic casing and power lead were still in the box.

10. then informed the alternate custodian and a further search was conducted proving unsuccessful.

11. Head Quarters Joint Task Force 633 (HQJTF633) and S6 Force Level Logistics Asset (FLLA) were informed of the incident.

12. A Quick Assessment (QA) was compiled and also furnished a follow up incident report.

13. DSA have reviewed correspondence including survey structured interviews arranged by CAPT Russell. The interview results were poor with 'yes' and 'no' answers however all personnel corroborated that the SWLT was not sighted in the COMSEC annex between 24 May 08, and 30 May 08.
16. It is uncertain whether or not the alleged sequence of events leading to the loss of the SWLT is actually plausible. I have significant doubts as a result of the following:

Education, Policy and Training

17. ADFP is qualified and responsible for the correct accounting and security of accountable communications security material (ACM) and received a briefing prior to commencing his custodial duties.

18. The ADFP 6.0.3.1 is the overarching document for COMSEC within the ADF. It outlines the accounting procedures for adherence by ADF personnel in accounting for ACM.

19. The Defence security Manual (DSM) outlines control of commercial grade encryption devices in that they must be handled and safe guarded using Defence asset accounting practices such as:
   a. recorded in the asset register;
   b. counted in a stock take at least once per year; and
   c. protected from theft.

Conclusion

20. 

21. On this occasion the SWLT was not keyed and
22. If the SWLT was opened, the only material that could be potentially be retrieved is the last key exchange which is unique to every connection. If the crypto area of the unit is penetrated then the unit zeroes and nothing can be retrieved.

23. In the long term,

24. The SWLT was removed from the COMSEC Annex between 24 - 30 May 2008;
25. There is a lack of evidence to determine that the SWLT was intentionally removed from the COMSEC annex.

26. It is possible (based on previous anecdotes by but also incredulous, that the SWLT was accidentally or inadvertently dropped in the bin without anyone hearing it or seeing it;

27. There are numerous failings in the management of the CCI in the COMSEC annex that contributed to the loss of the SWLT;

28. demonstrated some awareness of his responsibilities under ADFP 6.0.3.1, by regularly carrying out the respective duties in accordance with the ADFP 6.0.3.1.

29. The RIO reported that there is no apparent or contributing explanation that leads to failure to perform his duties in accordance with the publication.

30. DSA conclude that in terms of the DSM, did not safeguard the CCI item from theft or loss. An example of this is that he did not reassign the position of the bin after aforementioned cable incident, for fear of making waves in his new position.

31. The following are actions since implemented by:

a. lighting has been improved in the COMSEC annex;
b. the rubbish bin has been removed from the COMSEC annex;
c. CCI items have been removed from their packing boxes and placed on the shelves within the safe;
d. daily checks of CCI are carried out within
33. e. weekly checks of all CRC CCI are carried out, conducted by two personnel;
f. safes are now always fully locked and no longer day locked; and
g. an additional checklist has been developed to capture all required tasking.

32. The system of controls now implemented is adequate to prevent accidental loss of CCI.

Recommendations

33. DSA agree and ensure implementations and support the RIO recommendations that:

a. an appropriately constructed separate area for custodial staff should be installed to limit the number of personnel who have access to the area containing CCI;
b. TG 633.12 SOPs be amended to ensure waste bins are inspected prior to the removal from sensitive areas;

SECURITY-IN-CONFIDENCE
-SECRET-AUSTEO-

DE-CLASSIFIED
c. TG 633:12 SOPs be amended to include the wording 'the equipment is to be checked and returned to the store/safe without delay';

d. all personnel deployed into the position of COMSEC are to have COMSEC management refresher training prior to deployment; and

e. [Redacted]

34. Request the following personnel to be informed of the result as direct addressee's:

   a. DSD (R5-G-14)
   b. DCSEA (Russell-GS3-01-37)
   c. HQIOC (Level 5 20A Wylde St Potts Point)
   d. DCCA (R5-SB-053)
   e. ADFIS OIC MEAO (HQTF 633 AFPO 20 ADF NSW 2890)
LOSS OF CLASSIFIED DEFENCE DOCUMENTS ON DOMESTIC QANTAS FLIGHT

1. On 24 Jul 08, DSA was informed of the loss of RESTRICTED classified Defence documents that had been left on a Qantas domestic flight. The incident was reported by [REDACTED] who had possession of the documents and while travelling from Canberra to Melbourne, has removed them from a case during flight and placed them in a seat pocket where they remained after his disembarking.

2. Immediate attempts by [REDACTED] and subsequent enquiries by DSA members failed to locate the documents which have either been destroyed or recovered by unknown persons.

3. The lost documents relate to the Defence White Paper and although classified RESTRICTED, the significance of their loss has been assessed as very low. The Secretary of Defence and CDF have been notified of this incident.

4. The investigation revealed a failure by [REDACTED] to properly control and secure classified Defence information. [REDACTED] should be reminded of his responsibilities in this regard.

5. I agree with the recommendation at paragraph 13(a) of the enclosed minute. My point of contact in this matter is Mr Rohan Schmutz (02 6266 2854).

[Signature]

[Date]

Enclosure:

1. Minute titled, Loss of Classified Documents on Domestic Qantas Flight by Defence Employee, dated 16 Sep 08.
LOSS OF CLASSIFIED DOCUMENTS ON DOMESTIC QANTAS FLIGHT BY DEFENCE EMPLOYEE

Purpose
1. This report is to inform you of the outcome of the investigation of the loss of classified documents that occurred on 23 Jul 08.

Background
2. On 23 Jul 08, the left classified ‘RESTRICTED’ documents on QANTAS flight No. QF 813 from Canberra to Melbourne. The documents were left in the rear pocket of the seat immediately in front of .

3. On discovering the loss of the documents on 24 Jul 08, immediately informed AIRCORE Broderson, Director General Preparedness & POC Companion Review, and the ASSO, Mr Tim Scully.

Investigation
4. SIU started investigation on 28 Jul 08.

5. It was ascertained contacted QANTAS Baggage Handling on 24 and 25 Jul in an attempt to locate the documents without success.

6. was contacted and he advised that the documents were carried onto the plane in a lockable portfolio style briefcase. The documents were removed from the briefcase during the flight and placed in the storage pocket attached to the seat in front of him.

7. SIU investigators contacted QANTAS Baggage Services in Melbourne and Canberra to ascertain if any of the documents had been collected by aircraft cleaners. No documents had been handed in.

8. Investigators were advised that when documents are found loose, or not in any satchel or carrying folder, they are disposed of in general rubbish that is collected from the aircraft when cleaning. Any documents that are contained in folders are taken to baggage claims for collection.

9. In this instance it appears the documents were most likely disposed of by cleaners in general rubbish, or collected by an unknown person.
10. A damage assessment regarding the documents was obtained through AIRCDRE Broderson. The assessment stated that although the documents were classified RESTRICTED, the material is not considered to be of a sensitive nature. However, given the public interest in the Defence White Paper, a brief was prepared for the SEC and CDF.

11. The likelihood of the documents reaching the public was also considered to be very low.

Conclusion

12. As a result of the investigation it was found that safe handling of documents procedures were breached by [redacted] but, due to the threat assessment of the documents and the likelihood of the documents falling into the possession of the media no further action will be taken by DSA.

Recommendation

13. It is recommended that:

   a. [redacted] be reminded of his responsibilities in relation to the security of classified documents

   b. A copy of this report be filed in the PSF of [redacted]

   c. DSA take no further action in this matter and the file is closed.

Robert Schuster
Senior Investigator
DSA - SIU
16 Sep 08
SECRET STATEMENT OF OPERATING INTENT DOCUMENTS MISSING AT

Purpose
1. This informs you of the investigation into missing Statement of Operating Intent (SOI) SECRET documents at [redacted] Afghanistan.

Background
2. On 5 Aug 08, Assistant Unit Security Officer (A/USO) was informed that ten pages of the TG633.12 SOI were found to be missing from the document binder during the evening of 4 Aug 08. The missing pages were numbered from 19 to 28 of the 28 page document. The document was classified [redacted]. This binder had been stored in a larger binder within the TG633.12 OPS safe.

Investigation
3. On 21 Aug 08, three weeks after discovering the breach, reported the security incident to DSA, on behalf of the DIA for the MEA, Flight
4. The SOI document had been stored in the TG633.12 OPS safe. The last recorded must had been undertaken in late July 08 by TG633.12, and formed part of the six monthly, 100 per cent audit. There were no anomalies reported during the must.
5. On 1 Aug 08, the entire document was accounted for by who read the document as part of his induction training.
6. DSA were advised that TG633.12 personnel had ready access to the OPS safe and at the time of the security incident, TG633.12 was in the midst of handing over command from rotation three to rotation four. As part of rotation four training all operations personnel are required to read the SOI.
7. Three days later, on 4 Aug 08, ten pages from the document were reported to the USO as missing. The assessment given of the degree of compromise of [redacted] material has been deemed as medium.
8. On 5 Aug 08, A/USO briefed all operations personnel about the missing pages from the SOI and requested personnel from rotation three and four to come forward with any
information. The A/USO also interviewed all incoming rotation four personnel and asked if they had removed the document from the binder.

9. A search was conducted by the A/USO of all operations areas to no avail. It was therefore concluded that the whereabouts of the missing documents cannot be confirmed. Similarly the A/USO could not establish that the missing pages are still within the confines of

10. DSA were advised A/USO had briefed all operations personnel of the incident, directing personnel that they are not to remove individual pages from the documents or binders, for individual reading.

Conclusion

11. DSA were advised by the A/USO that it was concluded, based on the accessibility of the SOI that someone from rotation three or four has removed the ten pages and accidentally misplaced or destroyed them.

12. The A/USO stated that it was more than likely an incoming member from rotation four was responsible based on the fact that all incoming rotation four members were required to read the documents within the first two weeks of arrival at . However DSA enquires reveal that rotation three personnel continued to have access to all documents within the OPS safe.

13. The USO and A/USO also advised DSA that they both agree the potential for compromise of the classified material cannot be ruled out until the pages are accounted for. The possibility of a deliberate act or compromised also cannot be ruled out. However the USO and A/USO deems it more likely that the loss is due to only one hard copy of the document being available at any one time causing personnel to remove sections of the binder, in an effort to share the reading amongst them, in an effort to expedite the briefing process.

14. The DIA and A/USO advised DSA that they would update any changes of circumstances at .

15. DSA has experienced difficulties obtaining any further information or assistance from the rotation three or rotation four personnel.

16. The DIA have reportedly investigated this security incident and only then reported the breach to DSA some three weeks later. This delay has made it difficult for DSA to undertake a full investigation, due to the change over of personnel within those three weeks.

17. DSA is therefore been given the understanding by the DIA that the USO and A/USO has conducted a thorough investigation into this matter.

18. As a result of their investigation, DSA are advised that TG633.12 has tightened procedures, by recording the borrower's identification and subsequent movement and return of documents from the OPS safe, despite being in a secure area.

19. This additional security will hopefully prevent multiple personnel accessing material at any one time including the overlap during any future change over.

Recommendation

20. It is recommended that DSA file this investigation.
DE-CLASSIFIED

RESTRIC TED
SECURITY-IN-CONFIDENCE

Jacinta Blanks
ADSIU

Feb 09
FLOPPY DISK FOUND NEAR SKIP BIN – 109 KENT ST, DEAKIN

Purpose
1. This report is to inform you of the outcome of the above investigation.

Background
2. On the 08 Sep 08, it was reported to DSA that a floppy disc with the security classification SECRET AUSTEO was found lying on the ground next to a rubbish removal skip bin at Defence premises at 109 Kent St, Deakin ACT.
3. DSA investigators attended the site and took possession of the disc from the supervisor of the Classified Equipment Destruction Cell Mr Kenneth Podmore.

Investigation
4. DSA commenced an investigation, and on the 15 Sep 08 sought a damage assessment from the listed owner of the files [REDACTED] who is attached to the Support Integration and Test Facility.
5. [REDACTED] informed DSA that the files dated back to 2004-2005. On viewing the files he concluded that the information contained within them was UNCLASSIFIED and at best RESTRICTED.
6. He further stated that the information contained within the files was now readily available on the internet and recalls there was much discussion at the time of the original classification to what level they should have been, and it was decided, to ‘err on the side of caution’ and this is why a SECRET classification was assigned to them.
7. Inquiries were made with units and sections within the Deakin Offices precinct, however, the origin, and means of how the disc was disposed of in the above manner were unable to be determined.

Conclusion
8. It appears the disc has been inadvertently discarded in rubbish during a cleanout of old files from an unknown section within the Deakin Offices. Due to the damage assessment classification of the files this incident is regarded as minor and requires no further investigation.
Recommendations

It is recommended:

a) the reporting officer be informed of the investigation outcome; and
b) the DSA investigation of this matter is closed.

Rohan Schmalz
Assistant Director
DSA SIU
30 Jan 09
LOSS OF RADIO TRANSMITTER/RECEIVER, RAAF WILLIAMSTOWN

Purpose
1. This report is to inform you of the outcome of the investigation of a missing transmitter/receiver during shipment to Boeing USA for repair.

Background
2. On the 23 Sep 08, DSA were advised by the Tactical Fighter Systems Programs Office (TFSP0) of a missing transmitter/receiver for a FA 18 Hornet, that had gone missing during shipment to Boeing USA for repair.

3. The item was an integral part of FA 18 Hornet capability, and was no longer in production, therefore its loss had a significant impact on the FA 18 fleet and service. The value of the item was also estimated to be in excess of $450,000 AU.

4. Initial inquiries revealed that the item was last sighted whilst in the 81 Wing Central Repairable Items Store (CRIS) RAAF Williamstown on or about the 23 Apr 08, whilst awaiting collection by Boeing Australia's courier company. The item was not discovered missing until the 8 Sep 08 when inquiries were made by TFSP0 with Boeing seeking an ETA for the item's repair and return.

5. Subsequent checks with the CRIS, Boeing Australia and US, Boeing's courier company Schenker and Schenker's subcontractor GST Transport, failed to locate the item or any associated consignment notes or shipping documents.

Investigation
6. A complete 100% audit of the goods contained in the CRIS warehouse was undertaken by CRIS staff and completed on the 18 Sep 08. This audit failed to locate the item. Inquiries with Schenker and Boeing both within Australia and the United States, and subsequent checks of their warehouses and respective bond stores, also failed to locate the item.

7. As a result, DSA investigators travelled to RAAF Williamstown where they met with various members of the TFSP0, 82 Wing CRIS warehouse and commenced a review of the procedures involved in the receiving and dispatching of goods from RAAF Williamstown.

8. During this investigation it was found that the procedure that was in place in Apr 08 required no signatories for the dispatching of goods from the CRIS warehouse or the signing of any shipping documents of receipts by the courier company collecting the goods.

9. As a result, no document audit trail was available to track the subject item when it left the warehouse. Contact was made with the courier company GST Transport where they
assured investigators that they had never picked up the item as their manifest indicated that they had only picked up two items on the 23 Apr 08 and not three as they were requested to.

10. Investigators were also advised that Schenker would not accept goods into their bonded warehouses without the correct consignment and shipping notices.

11. Boeing was advised that DSA had commenced an investigation on the whereabouts of the missing equipment and investigators were advised that Boeing and Schenker staff were also conducting an internal audit and review of their procedures.

12. On the 22 Oct 08, DSA where advised by FLTLT Winton, Supply Chain Manager 81 Wing, Williamtown, via email, that the missing item had been located in a warehouse at Los Angeles airport by Schenker staff. It appears the item had been sitting in a transit warehouse and was not accompanied by any consignment notices, so it had remained at the warehouse since May 08. The item was subsequently forwarded to Boeing for repair and returned to Australia.

Conclusion

13. As a result of this incident and investigation the ad hoc inventory and dispatching procedures between the TFSPO, 82 Wing CRIS and Boeing Australia, have ceased and been replaced with more streamlined practices which allow a tracking and auditable trail of dispatched goods.

14. Procedures for the receiving or dispatch of goods with other companies at the CRIS warehouse have also been examined and updated and access to the warehouse has also been reviewed and updated increasing security within the building.

15. Schenker Australia has also conducted an internal review of their procedures where they found their systems had failed in some critical areas. New procedures have now been put in place to prevent the same failures from recurring. Investigators have studied the procedures that have been implemented by the 82 Wing CRIS, Boeing and Schenker and believe they are sufficient to prevent a recurrence of this incident.

Recommendations

16. It is recommended that:

   a. a sanitized version of this report be forwarded to the CO 82 Wing, TFSPO, and MSO NSW for their information.

   b. The investigation file be closed.

Rohan Schmelz
Assistant Director
Security Investigation Unit
14 Jan 09
MISSING N/SEAS NIGHT SINGLE EYE ACQUISITION SCOPE FROM SECURITY CONTROL OFFICE, BUILDING 133, DEFENCE ESTABLISHMENT ORCHARD HILLS (DEOH)

Purpose
1. This minute outlines the circumstances surrounding the disappearance of 1 x N/SEAS Single Eye Acquisition Scope (N/SEAS) located in the Security Control Room (SCR) of building 133 DEOH. The item was provided as Government Furnished Equipment (GFE) to security guarding contractor [REDACTED].

Background
2. The N/SEAS was housed in a black coloured case and stored with other equipment on a shelf within building 133.
3. On 8 Sep 08 shift supervisor [REDACTED] discovered the N/SEAS was no longer in its case.
4. On 22 Sep 08 an entry in the SCR Assignment Log Book referring to the loss of the item. A similar entry was recorded in the Supervisor’s Message Book requesting all supervisors to enquire with their guards if the item had been ‘seen or heard of’.
5. On 1 Oct 08 the incident was reported to the Security Incident Centre and on 9 Oct 08 the matter was forwarded to DSA for investigation.

Investigation Details
6. On 14 Oct 08 DSA investigators attended building 133 DEOH. The empty item case was sighted in situ upon a shelf in the SCR. It was noted that entry into the building was via a keypad locking system, however, when inside the building all interior doors were open or unlocked. The rear door to the building, secured by keypad lock, was closed, however, investigators were informed that if a security guard wished to have a cigarette they would do so at the rear of the building leaving the door unsecured.
7. On 29-30 Oct 08 all security personnel were spoken to by DSA investigators regarding the loss of the item with a number stating they were unaware of the existence of the item. Those guards aware of the items existence stated they had not used or seen the item for a long period of time. Guard supervisor [REDACTED] stated he saw
the item approximately two months prior to it being reported missing when he was
showing it to another guard in the execution of his duties.

8. Since the item was reported missing one guard has resigned from DEOH.
was employed as a guard for a short period prior to the
disappearance of the item in which time he stated he was a 'private eye' and
'investigator'. was reprimanded by management several times for certain
disciplinary issues during his time at DEOH. Shortly following informing all guards of the DSA investigation failed to attend work and stated
he had to leave the country to visit his has not returned to the workplace. DSA investigators have confirmed has not left the
country and his whereabouts are unknown.

Conclusion

9. There appears no relevant reason the guards have been provided the GFE
item and its use appears to have been extremely minimal with the guards that stated
they were aware of the item only recalling one occasion for its use.

10. Reporting the loss was delayed while guards attempted to locate the item and
initially only verbal requests to locate the item were made. This resulted in a
communication breakdown between shifts and the item was not officially reported for
a number of days.

11. Investigators were made aware the item was not regularly sighted and was not
present on any handover or on check-off lists.

12. At this time the item is still missing with the likelihood of locating it being
low.

Recommendations

13. All GFE be issued on a needs basis to any non ADF personnel such as the
guards.

14. If issued all GFE to be regularly sighted and placed upon shift handover
documentation.

Dean James
Senior Investigator
10 Nov 08
TRESPASS OF DSTO FISHERMANS BEND BY

This report is to notify you of the result of enquiries relating to the alleged trespass by [REDACTED] onto the premises of DSTO at Fishermans Bend, Victoria.

Background

1. Initial advice from the National Security Manager, DSTO Edinburgh alleged that a former employee of DSTO Fisherman's Bend had gained access to his former worksite after hours and removed three cardboard boxes containing unknown items. It was also alleged that there was evidence the IT computer equipment in his area had been tampered with in an apparent attempt to access DSTO IT Systems.

2. [REDACTED] has been employed with DSTO, Air Vehicles Division for approximately the previous ten years. As a result of a number of disputed issues, [REDACTED] has recently lodged a log of claims against DSTO relating to the circumstances leading to his leave and other grievances.

3. [REDACTED] attended at DSTO Fishermans Bend on Sunday 7 December 2008 at approximately 7.00pm and after presenting to the gate a current Defence pass, was allowed entry. On going to the building he had previously been working his swipe access to the building was denied. A security guard at the facility has then provided [REDACTED] access to the building where he went to his former office area. This area is secured with a security coded touch pad for which [REDACTED] did not possess the current code. He has then telephoned a former colleague and was provided the current code. Once inside the area he removed a number of boxes from the area unsupervised.

Investigation

4. DSA has confirmed with the Security Manager DSTO-M, Garry Chilingsworth and from records at DSTO Fishermans Bend that [REDACTED] did access the area as stated. It has also been confirmed with both DRN and DSTO IT areas that [REDACTED] did not access either system. His access to both systems had lapsed and at the time he did not have a current IT account with either system, his last recorded access was in July 2008. In addition to this, management in the area had disabled his desktop computer.
6. IT access records to the building indicated that [REDACTED] had made 2 attempts to gain swipe card access. Both attempts were denied prior to his being given access by the security guard. [REDACTED] confirmed that he had been contacted by telephone at his home address on the evening of the 7 Dec 08 by [REDACTED] and had provided him with the office door access code. [REDACTED] indicated to [REDACTED] that he was, 'there to collect his personal property.'

7. DSA spoke with [REDACTED], former supervisor who provided an outline of the background issues regarding [REDACTED].

8. [REDACTED] stated that [REDACTED] had made a rearrangement of workstations during which [REDACTED] had packed personal belongings of [REDACTED] into three cardboard boxes and moved them to his new allocated workstation. He had also arranged that the workstation at that position be disabled.

9. DSA also spoke with [REDACTED] who confirmed he had accessed DSTO Fishermans Bend Complex as earlier stated and that he did so for the purpose of collecting his personal belongings. He further stated that whilst on site he attempted to access his DRN account for the purpose of completing an online leave application. When he found his terminal was disabled, he attempted to utilise another terminal.

10. He indicated to DSA that in his mind at the time that he entered the DSTO complex he was still employed by Defence. He indicated that he had received nothing from Defence since he submitted [REDACTED]. He stated he had spoken to a person within the Personnel area. During this conversation he indicated that [REDACTED] was to take effect at the expiration of all his leave entitlement. From that conversation he was of the belief that this was at the end of February 2009. He further stated that at no time had he been contacted by anyone from within DSTO in relation to the status of [REDACTED].

11. An examination of the separation procedure within DSTO showed that there was an adequate and appropriate process in place for staff leaving the Organisation in relation to building access, return of passes and other associated matters. [REDACTED] had not been through this process, most likely as a result of his circumstances including his strained relationship with DSTO.

Conclusion

12. From the DSA investigation, there has been no criminal offence capable of prosecution committed by [REDACTED]. At the time that he entered the DSTO facility, he believed he was still a member of Defence. In any event he was granted access by the security staff and provided with the access code by a member of DSTO which is capable of interpretation as tacit consent of entry.

SECURITY IN CONFIDENCE

RESTRICTED

DE-CLASSIFIED
13. The separation process was poorly managed in part due to the apparent unwillingness of [REDACTED] to communicate with DSTO management and the lack of an alternative effective process. There is evidence to suggest that an attempt to contact [REDACTED] was made by letter which he denied receipt of.

14. There was no record within the security office at the Fishermans Bend complex that [REDACTED] had separated from DSTO or that his access to the area had been withdrawn.

15. There is no evidence to support the compromise or disclosure of any DSTO classified information.

Recommendation

16. The following recommendations are made:
   a. The DSA investigation be closed;
   b. DSTO be advised of the findings of this investigation; and
   c. DSTO review their separation process and amend if appropriate regarding separation of members whilst on leave.

Peter Baldwin
Assistant Director
SIU DSA

Dec 08
LOSS OF TOP SECRET DOCUMENTS - CIO GROUP ICT OPERATIONS

Background

1. On 21 May 09, USO CIOG ICT Operations conducted an Audit of documents in the three current TOP SECRET (TS) Classified Document Registers (CDR's). 12 TS CODEWORD documents were unaccounted. An XP188 Incident Reporting form was raised and forwarded to Defence Security Authority (DSA) Security Incident Centre (SIC).

2. A further three TS documents were later found to be deficient in another of the CDR's on hand at ICT Operations.

Investigation

3. On 29 May 09, the matter was accepted as an investigation by DSA.

4. On 3 Jun 09, investigators contacted [REDACTED] at ICTO and a meeting was organised with RADM Jones to canvass issues raised in the XP188.

5. On 3 Jun 09, investigators met with RADM Jones, Head ICT Operations, in his office. He informed investigators that upon his commencement as HICTO in Sep 07, he implemented a reduction of holdings of SECRET and TOP SECRET (TS) documents on hand and removed himself from the distribution list with regards to these particular TS documents. Also, at the time the section did not have a USO in place.

6. In Dec 08, DSA-ACT/NSW office completed a Protective Security Survey (PSS) Report for Chief Information Officer Group (CIOG), Head ICT Operations (HICTO). This report resulted in a number of recommendations, some which related to the recording and destruction of classified documents and updating the Unit Standing Security Orders (USSO's). As a result of the PSS report, RADM Jones undertook a further review of systems to reduce outdated document holdings. He had previously caused the USSO's to be updated. He stated he was keen to reduce risk and move forward in relation to document holdings.

7. Investigators spoke with Miss Michelle Farrugia who on the 21 May 09, was appointed as USO for the section and underwent the required USO course. She stated all three CDR's were commenced in 2006. This number was recently reduced to CDR. The current TS CDR is kept in a TS safe in a locked and alarmed security room. This room was shown to investigators by [REDACTED] who is the person who has access to the safe.
8. Miss Farrugia showed investigators the entries for the missing 12 TS Documents in CDR three. She also showed investigators 3 other missing TS Document entries from CDR book two. She was of the belief that the 12 TS docs and separate three TS docs were destroyed prior to her arrival in Feb 08, as she does not recall having seen them. She had emailed [REDACTED] regarding the documents. [REDACTED] was unable to provide any information, other than they may have been destroyed.

9. She stated HICTO had moved temporarily from R1 to R8 about Apr 08, due to office renovations. Mr Paul Muscat, CIOG Branch Security Office (BSO), had oversight of document security at the time and during the subsequent move back to R1 at the completion of renovations. CIOG had undergone a massive restructure during the previous 12 months and many staff had changed locations. Safes had been moved and sections relocated. It is possible this series of changes may have contributed to the loss of these documents and the difficulties experienced in tracing their movements prior to the loss.

10. Investigators then spoke to [REDACTED] HICTO Staff Officer. She stated that RADM Jones does not usually access the CDRs and prefers to allow his subordinates to handle all documents.

11. [REDACTED] was unaware of the location of the documents. She had never sighted them and believes they were destroyed prior to her arrival at HICTO in Jul 08, and most probably had not been written off correctly in the CDRs. She also thought that a previous staff member, [REDACTED] may have some knowledge of the missing documents.

12. On 4 Jun 09, RADM Jones sent an email to [REDACTED] with some issues for clarification. In a further email on 5 Jun 09, RADM Jones stated that when he received a handover from AIRCDRE David Richards, office administration and documentation holdings were not canvassed as he believed that process was the responsibility of the staff officer and executive assistant. He was not aware of the contents of the missing documents nor was he able to comment on the possible location of the files as he does not get involved in the day to day maintenance of document holdings.

13. On 9 Jun 09, investigators spoke to [REDACTED] at CIOG. She was shown the CDR extract for the missing 12 TS docs and acknowledged that the handwriting for the entries as being hers. She was shown the second CDR extract but could not give any information about the other 3 missing TS documents.

14. [REDACTED] thought the documents had been sent back or destroyed and stated the records must not have been written off correctly. She thought this may have been because there were multiple CDR’s in use at the same time. She believed the files were kept in the old 2IC’s safe and that in Apr 08, there had been a move from R1 to R8 due to office refurbishment. She also believed the safe was an older four drawer type with a spin dial combination lock and that these safes had now been replaced.

15. She did not know if there had been an audit of documents held prior to the move. She did not move to R8 and was herself moved to the ground floor of R1. The documents were assigned escorts for the move and handled in accordance with their classification, including their transfer by safe hand. She repeated there was not a USO appointed to the section at the time. She told investigators that she would make further inquiries.
16. On 12 Jun 09, was again spoken to and stated she had canvassed the missing documents with several staff that may have had dealings with them and that no one was able to give further information on the whereabouts of the documents. She stated that the documents were placed in red secure document boxes and were physically escorted to R8 and back to R1 during the move. She stated that Mr Peter Dower, Principal Adviser to CIOG, had suggested an audit be conducted of safes held within CIOG.

17. A request was sent to Ms Lauren Chamberlain at CIOG requesting a 100% audit of all CIOG safes located at R1 and R8. This audit did not locate the documents.

18. On 16 Oct 09, investigators spoke to Mr Muscat who has worked as the CIOG BSO for 3 years. He was shown the CDR extract for the missing three TS documents and stated they were SIGINT highlights that should have been destroyed immediately. It would appear this was done but the CDR not written off accordingly. He too felt this may have been due to the fact there were several TS CDR’s in use at the time.

19. He further stated that previously, RADM Jones had directed destruction of non current document holdings which did result in a huge reduction of such documents within HICTO.

20. He was shown the CDR extract for the missing 12 TS documents. He knew nothing about these documents as they were mostly dated before he commenced duty at CIOG. He could not understand the distribution but felt they had probably been destroyed. He thought it strange that the 12 missing documents were all in order and thought the CDR had been commenced just for these documents. He felt that, given the nature of TS briefing documents, they should have been destroyed that same day they were received.

21. Mr Muscat added that when the temporary relocation to R8 occurred, all classified document holdings were handled in the appropriate manner, providing no opportunity for the documents to be lost or otherwise compromised during the move. It is the view of Mr Muscat that the documents of concern were most likely destroyed prior to this relocation taken place.

Conclusion

22. Although the documents cannot be located, the risk of compromise is assessed as LOW. It is most likely the documents were destroyed soon after they were received by HICTO and the details of this destruction were not recorded. This was exacerbated by the fact there were three TS CDR’s in use at HICTO at the time. There is now only one CDR.

23. Up till 21 May 09, HICTO did not have a USO in place. This has been rectified by the subsequent training and appointment of Michelle Farrugia as USO. She is aware of the USO responsibilities.

24. HICTO has made a significant effort to reduce document holdings. Security of current document holding at the SECRET and TS level is in compliance with the DSM.

25. USSO’s were updated in Nov 08, and are appropriate.
Recommendation

26. It is recommended that HICTO:

   a. be advised of the outcome of this investigation and accept DSA authorisation to
      formally "write-off" the subject documents and endorse the relevant CDRs in
      accordance with the DSM; and
   
   b. ensure ongoing compliance with the DSM with regard to the management of
      classified document holdings within the CIOG ICT Operations area.

P. Grace
DSII

29 Oct 09
CONTRACTUAL DISPUTE BETWEEN DSTO AND DEFENCE CONTRACT DIRECTOR INVOLVING A COMPACT DISC

Peter Grace
Acting Assistant Secretary Security Operations

18 Jun 09

Enclosure:
1. DSA Report. 'Contractual dispute between DSTO and Defence Contract Director involving a Compact Disc'.

SECURITY-IN-CONFIDENCE

DE-CLASSIFIED
DE-CLASSIFIED

Australi an Government
Department of Defence
Intelligence & Security

Minute

Defence Security Authority
Campbell Park Offices (J-3-038)
PO Box 7931
CANBERRA ACT 2610
+61 (0) 6210 4205
Email: declassifications@defence.gov.au

DSII (CP3-3-036)
CONTRACTUAL DISPUTE BETWEEN DSTO AND DEFENCE CONTRACT INVOLVING A COMPACT DISC

47F. 47G
SECURITY-IN-CONFIDENCE

DE-CLASSIFIED
MISSING DSD COMSINT LAPTOP

Purpose

1. This report is to notify you of the result of enquiries relating to the reported loss of a TS COMSINT DSD laptop computer following an audit of DSD laptops.

Background

2. DSD notified the DSA that following an audit of DSD laptops in August 2009, a TS COMSINT laptop was found to be missing. Records indicated that this laptop had not been sighted since 2006 and checks indicated that it had not been recorded as having been returned or replaced. No reason was provided as to the reason that the loss, as detected in earlier audits, had not been reported to DSA.

Investigation

3. The DSA conducted a number of enquiries and reviewed documentation relating to the original acquisition and purchase of the laptop. An examination was made of the recording details of the laptop and subsequent audit logs. This revealed a number of discrepancies and anomalies relating to the laptop.

4. An examination of serial numbers and asset numbers indicated that two laptop computers purchased at the same time appeared to have been recorded incorrectly and were allocated three barcode asset numbers. A physical examination of one of the laptops revealed that it bore two barcode stickers including that of the recorded missing laptop.

5. This laptop has two serial numbers, the first is a manufacturer's serial number, the second recorded on the Microsoft software sticker relating to installed software. An examination of the records shows that the two bar code stickers were recorded against each of these serial numbers. This resulted in the one laptop being recorded twice within the records used for audit purposes.

6. Procedures in place relating to the initial recording of devices on asset registers on purchase, if followed, would have eliminated the possibility of this occurrence. The only
explanation for this occurrence being that there was no secondary check of the allocation and recording of the asset number. Due to the date of acquisition, DSA are unable to verify this assumption.

7. The audits conducted on this item had been outsourced and were not conducted by DSD personnel. No reason has been provided for the failure to notify DSA of the previous audit results. Due to circumstances of use, location and prior audit of this laptop, DSA are unable to determine why this error was not reported earlier. Further enquiries will be undertaken to ensure future timely reporting.

Conclusion

8. The supposed loss of the laptop was in fact due to an accounting error which was compounded by continued and unactioned audits involving this item. The initial recording of the laptop, if conducted in accordance with the procedures at that time, would have avoided this error. The relevant DSD personnel were directly involved in the DSA investigation and are fully aware of the circumstances that lead to this incident and the subsequent outcome. As such, there are no recommendations resulting from this investigation.

Peter Baldwin
ADSIU
Aug 11
INVESTIGATION OF LOSS OF SECRET AUSTEO KINGSTON THUMB DRIVE

Purpose

1. This minute is to inform you of the outcome of the DSA investigation into the suspected theft in the MEAO, of an encrypted Kingston Thumb Drive containing SECRET AUSTEO material.

Background

2. On 5 Mar 10, an XP188 from 33 reported a "Major" security incident and "loss of computer thumb drive containing classified material" by 47F.

3. Between 28 Feb and 3 Mar 10, the 47E travelled via commercial aircraft from Dubai to Islamabad via Kuwait, during which time a USB Thumb drive containing SECRET AUSTEO material was stolen from his checked in luggage.

4. In brief, the circumstances surrounding the theft of the USB are that 47F in Nov 09, On assuming the role, he was briefed on the role and duties by his predecessor. On change over of the 47F. remained in this position with his duties unchanged.

5. In brief, the circumstances surrounding the theft of the USB are that 47F in preparation for a visit to Islamabad by the 47F, requested that both his and 47F DSN Lotus Notes files be downloaded from the DSN server at AMAB to a Kingston thumb drive.
6. Prior to travel [REDACTED] requested the Lotus notes be downloaded to a Kingston USB Thumb drive [AW JTF633 Standing Instructions (SI (OPS) 6-03)]. This was completed and a Transfer Certificate issued. The Kingston USB Thumb drive utilised had been issued to [REDACTED] on 21 Jan 10 and at that time was classified as SECRET.

7. [REDACTED] in company with [REDACTED] travelled from Dubai to Islamabad via Kuwait on 28 Feb 10. [REDACTED] placed the SECRET AUSTEO USB Thumb Drive in an unsecured backpack and checked it as luggage. On arrival in Islamabad the parties checked luggage was missing. This luggage was not recovered until 3 Mar 10 in Islamabad.

8. When [REDACTED] recovered his luggage he discovered that the Kingston USB Thumb Drive which he had placed in his back pack was missing as was a pair of Ray Ban sunglasses.

Investigation scope

9. DSA has undertaken an investigation into the circumstances surrounding the loss of the USB thumb drive. The scope of which was to:

   a. Identify the circumstances surrounding the physical loss of this portable data device;
   b. A damage assessment will be prepared by the 'tiger team' and not DSA;
   c. Identify security vulnerabilities whilst travelling within the MEAO;
   d. Identify the extent of use of portable data devices on Defence and other systems within the MEAO;
   e. Assess the extent process and procedures controlling the use of portable data devices;
   f. Identify security vulnerabilities associated with use of ICT in the MEAO; and
   g. Identify and assess the risk associated when travelling within and from the MEAO with portable data devices.

Circumstances surrounding loss

10. [REDACTED] was interviewed by DSA staff in relation to his role, functions and his involvement in the circumstances surrounding the theft of the USB Thumb Drive. He said that when he took over as the [REDACTED] his predecessor provided him with an outline of his roles and responsibilities and that these have not changed whilst he has been in the position or with [REDACTED]

11. As part of his duties [REDACTED] is responsible for managing all travel arrangements for the [REDACTED] The processes were inherited from the previous ADC which included ensuring that [REDACTED] had access to his DSN Lotus note files when travelling within the MEAO.

12. The carriage of this data had previously been undertaken by a SF Sigs member using a laptop computer which was transported via safe hand during travel by [REDACTED]. This procedure was changed by [REDACTED] after suggestions by the former SF Signals Officer that data could be carried by the utilisation of a USB thumb drive.

13. [REDACTED] was notified of the requirement to travel to Islamabad in Jan 10, however, was not provided with the exact dates which prevented arrangements being undertaken prior
to his recreation leave. He returned from leave on 26 Feb 10, and was informed that the travel had been confirmed for 28 Feb 10. He then finalised escort and travel arrangements.

14. As part of these arrangements it was arranged transfer of O'Wn DSN Lotus notes file to a previously issued Kingston USB Thumb Drive. The data transfer was in accordance with SI (OPS) 6-03. On the date of travel this thumb drive had been placed by O'Wn in the top of his back pack. There was no security or locking mechanism on the back pack.

15. The transfer of the data was undertaken as a routine action and not as a specific request by O'Wn as he was unaware of this data transfer. The ICT transfer certificate identifies O'Wn as the requesting officer.

16. Travel from AMAB to Dubai airport took the travelling party in excess of two hours due to traffic congestion, rather than the expected 30 minute drive. On arrival at the Emirates Airlines check in counter, it was found that due to the traffic congestion, the flights departure had been delayed. O'Wn made the decision during his check in to check his back pack as luggage rather than retain it as carry on baggage.

17. O'Wn checked their baggage whilst retained his back pack as carry on luggage. The party then travelled by commercial aircraft. The route was Emirates Airlines from Dubai to Kuwait and then Kuwait Airways for the trip from Kuwait to Islamabad. On arrival at Islamabad all checked baggage of the travelling party was identified missing and was subsequently not recovered until the party's departure from Islamabad on 3 Mar 10, some days later.

18. On discovering that the checked baggage of the travelling party was missing the party spoke to Kuwait Airways officials and completed lost baggage forms. Information obtained during DSA interviews indicates that a large number of other passengers on this flight were also completing missing baggage claims. From descriptions obtained of these passengers it appears that both westerners and locals were impacted in addition to the.

19. The made enquiries with both airlines concerned and was informed that the missing baggage was in Kuwait and had not been transferred onto the Kuwait Airways aircraft. A representative of Kuwait Airways blamed Emirates for not transferring the baggage. During the next three days the DA made numerous enquiries in an attempt to locate the missing baggage. The DA and were informed the baggage had been located in Kuwait and they then made a request to have the baggage returned to Dubai and held there. At this time the had forgotten that the USB was in his back pack.

20. The baggage was eventually located on 3 Mar 10, at the Islamabad airport after having been unloaded from the same aircraft in which the party were due to return to Dubai. The DA recovered his backpack and immediately took it to the departure gate and handed it to The DA returned to the luggage carousel and recovered the remaining bags. Due to the pending departure of the party the DA notified via SMS that the baggage had been recovered and he would have it transported back to Dubai.

21. An examination of the airline baggage labels indicates that the baggage had travelled to Kuwait from Dubai before being returned to Dubai and then travelled direct to Islamabad. This supports the belief that the bags had not been transferred during the change of aircraft in Kuwait during the initial flight.
22. A DSA review of the missing baggage (Photographs attached at Annexure A) revealed that the bags carried by both [REDACTED] and [REDACTED] are of military appearance and both are clearly marked with the members names and in the case of [REDACTED] also included his rank. The bag carried by [REDACTED] was a civilian type case with no identifying markings or labels.

23. Due to the fact that the party's bags were unable to be checked on the flight from Islamabad to Dubai, the DA itemised each bag and then returned them to Dubai by DHL. As a result it is impossible to determine if all bags had been tampered with prior to their recovery in Islamabad. [REDACTED] on recovery of his backpack discovered the USB thumb drive and a pair of Ray Ban sunglasses missing, both of which had been placed in the top zippered compartment of the backpack.

24. None of the baggage had been secured by any type of locking mechanism.

Travel Security Vulnerability

25. During the investigation DSA identified a number of security vulnerabilities [REDACTED].

a. 

b. 

c. [REDACTED]

d. 

e. 
26. DSA spoke to the Business Management Cell (BMC) in relation to contract arrangements in place involving BMC. BMC commenced operations in Nov 09 and indicated they have concerns in regard to the tender and contract process in place. BMC are conducting their own review however, this is not security focused.

Portable Data Devices

27.

28.

29.

30.

31.

32.

33.

34.
38. The loss of the USB was a deliberate theft and not accidental. This is based on the knowledge that when the backpack was checked in and later, when recovered, it was found to be in a secure state, suggesting the USB and more so, the sunglasses, could not have simply fallen from the pack.

39. It has been established after examination of baggage labels that after being checked in, the bags left Dubai and arrived in Kuwait before being returned to Dubai. The bags were immediately recovered from the flight on arrival in Islamabad. It is therefore assessed that the theft took place whilst the bags were in either Kuwait or Dubai airport, the most likely being
Kuwait due to the timeframes associated with luggage storage at each airport and the known higher security standards within the Dubai airport.

40. DSA was informed and assessed that the data transfer procedures in place in the MEAO are integral to data exchange in the environment and operational needs of the JTF. The Standing Instructions governing this practice were at the time in place and sufficiently robust to have prevented this occurrence, had they been adhered to.

41. The review undertaken following this incident has identified additional measures relating to user requirements to establish the operational imperative need to transfer data before approval is granted, which provides additional security protection.

42. Observations made in the MEAO during the investigation highlighted the requirement for the appointment of a dedicated information manager to coordinate and manage IT information within theatre. The principles contained in the Australian Government Information Security Manual as they pertain to an agency security officer could be applied to an Information Manager role within the MEAO.

43. This role should also include oversight of EDMS and DRMS. DSA, in the course of investigations conducted,

44. Due to their geographical location and difference in time-zones, a current deployed group normally cannot obtain an appropriate degree of support or advice from specialist agencies whilst deployed. This, accompanied by the operational focus of the group, can lead to the relegation of some processes. For these reasons, the appointment of a dedicated person in the role of Information Manager within the Task Force would assist in maintaining the integrity of all forms of stored electronic data.

45. A deficiency in CI awareness and the lack of regular CITA briefings are a contributing factor to the theft of the USB. There appeared to be minimal understanding of the current FIS threat. Had a greater emphasis been placed on CI awareness from training and regular relevant CITA been provided to managers and staff, an appropriate attitude would likely have been adopted.

46. The Unit Security Officers appointed to the various units and areas within the MEAO, perform this function in addition to their primary role.

consolidation and comprehensive register of electronic items capable of data storage being another example. In order to safeguard Defence information and assets, there is a compelling case for the appointment of a full time Security Manager within the MEAO. In addition to the areas identified, there is a need for a single point of contact for security training, advice, liaison and coordination, in addition to addressing security issues identified.
Recommendations

47. The following recommendations are made;
   a. CJOPS assess any potential action to be initiated against [b l a c k o u t]
   b. CJOPS consider the appointment of an Information Manager for JTF633;
   c. CJOPS and the CSO consider the appointment of a Security Manager for JTF’s;
   d. [b l a c k o u t]
   c. CJOPS review the manner in which Command elements move between locations within the MEAO via civilian transport to minimise the success of any FIS collection efforts;
   f. DSA, HQJOC and CIoG conduct a joint review of current data transfer instructions and processes; and
   g. CJOPS and CIoG review the current ICT management structure and programs to ensure the most effective and consistent provision of ICT services.

Peter Baldwin
ADSiu
12 Apr 10

Annexes:
A. Photographs of subject baggage
CLASSIFIED COLLINS CLASS SUBMARINE SCALE MODEL PROPELLER
UNACCOUNTED FOR AT DSTO EDINBURGH

Purpose
1. To inform you of the DSA investigation into a security incident involving a Classified Collins Class Submarine scale model propeller, which could not be accounted for at building 79, Maritime Operations Division (MOD) at Defence Science and Technology Organisation (DSTO), Edinburgh, SA.

Background
2. On 30 Mar 10, Mr Shane Wood, manager of the Acoustic Test Water Tank Facility at MOD Edinburgh was escorting official visitors through building 79 and showed them a Collins Class model submarine which he manages as part of his duties. At this time, he noticed the model's scale propeller and propeller end screw were missing. The propeller is a 1/76th scale model. It is made of brass and is approximately 50mm in diameter.

3. Enquiries were conducted locally with other staff to determine if the whereabouts of the propeller were known. On 1 Apr 10, the items were officially reported as missing at MOD. Over the following week, further searches by staff failed to locate the propeller. On 7 Apr 10, a search of the acoustic testing water tank also failed to locate the items.

4. On 8 April 10, an email was sent to all staff by Mr Chris Gillard, Head of Group for testing, seeking the whereabouts of the propeller and requesting it be returned. A second email was sent out by Chris Gillard on 9 Apr 10, emphasising the importance of locating the propeller. A third email was sent on behalf of the Chief of MOD (CMOD), cancelling all testing in the water tank until further notice.

5. On 14 Apr 10, the internal mailbag was emptied by Miss Julie Vaughan in building 79, MOD. Miss Vaughan located a non Defence envelope addressed to Mr Gillard, which she immediately took to him. The envelope was found to contain the scale model propeller and end screw.

6. MOD were still unable to determine how or when the items went missing or if they had been compromised. An XP188 Security Incident was raised and forwarded to the Defence Security Authority (DSA) Security Incident Centre. It was raised that there were capability issues due to the working propeller possibly being used on two current Collins Class Submarines.
Investigation

7. The matter was accepted for investigation by DSA on 16 Apr 10.

8. On 21 Apr 10, investigators attended DSA, South Australia (SA) and were given an overview of the incident by Mr Darryl Barreau, Principal Security Advisor. He informed investigators that due to the circumstances of the item’s loss and its return, it appeared the propeller may have been compromised. Foreign Intelligence Service (FIS) involvement could not be ruled out.

9. Investigators then attended MOD at DSTO Edinburgh where they spoke to Deputy Director MOD, Dr David Liebing and Mrs Vicki Maskell, the Unit Security Officer. Dr Liebing outlined MOD expectations regarding security, staffing and the potential for mistrust.

10. Mrs Maskell informed investigators that building 77 is the administration area where the mailbags are located. Building 79 is the laboratory building and building 211 is the acoustic testing water tank facility. Mrs Maskell showed investigators a spreadsheet she had prepared which indicated staff who had accessed Buildings 77 and 79 during the period 9 Feb 10 to 14 Apr 10, when the propeller could not be accounted for. There was no CCTV footage of the buildings concerned.

11. Mrs Maskell then retrieved the model propeller, end screw, the tissues the items were wrapped in and the envelope they were found in. She informed investigators the envelope was not Defence issue and checked the stationery stores for MOD, confirming it was not a type of envelope they had in stock. Mrs Maskell stated the items had been handled by numerous staff since they were found in the mailbag and as a result, it was determined there would be little benefit in preserving the items for fingerprint analysis. Mrs Maskell offered a view that it was possible the propeller may have been sitting on a work bench or desk and may have been inadvertently misplaced or alternatively, that someone within the unit may have intentionally removed the items, so as to highlight lax security measures that exist within the MOD.

12. A photocopy of the envelope was made, showing size, colour and the handwriting on it. Photographs were taken of the propeller and end screw, the Collins class model submarine, the compactus, the secret computer terminal room (building 79, room 16) which contains the compactus and building 211.

13. On 22 Apr 10, investigators returned to MOD and commenced interviewing a number of staff who have access to building 79 which houses the secret terminal room and compactus and building 77 where the internal mail was kept. Information obtained during these interviews includes:

   i. No person admitted to having knowledge of or being involved with the missing propeller whilst it was unaccounted for or its return;

   ii. All persons interviewed denied having written on the yellow envelope and could not otherwise identify the handwriting;

   iii. It was not able to be determined when the propeller went missing or where it went missing from. It was last used on 9 Feb 10;

   iv. The movement of the propeller was not recorded and the compactus that it was meant to be secured in was not always locked;

SECURITY IN CONFIDENCE

DE-CLASSIFIED
The propeller is not always used in conjunction with the model submarine;

The most likely scenario for the missing propeller is that it was put aside and forgotten about until the issue became serious and that the person returning it did not want to draw any undue attention;

Staff were aware of the missing propeller due to emails sent by Mr Gillard; and

Passive searches of the work areas failed to find the missing propeller.

On 23 Apr 10, investigators had a meeting with Dr Leibing, Mrs Maskell, Mr Gillard and Dr John Riley, Chief MOD who participated by telephone link. Investigators informed them it could not be concluded that the model submarine propeller did not leave MOD. The whereabouts of the propeller between 9 Feb and 14 Apr 10 cannot be determined. It is not known what the last known location of the propeller was. Investigators could not rule out sinister activity or the involvement of FIS.

At the suggestion of investigators, an email was circulated to all staff at MOD, informing them that DSA was investigating the incident and offering individuals the opportunity to speak or meet with investigators discreetly and informally. Despite these efforts, no person has come forward offering information about the unaccounted for propeller.

On 27 Apr 10, an email was sent to Dr Riley, requesting a Damage Assessment (DA) be conducted. A DA was conducted by Mr Gillard in consultation with a subject matter expert, Dr Chris Norwood from Maritime Platforms Division at DSTO Fishermans Bend. This type of propeller (generation 1) is no longer used on Collins Class Submarines. It is unlikely that if the propeller was compromised, it could be used to compile any useful information that might threaten the operations of the MOD or impact on national security.

The damage assessment was forwarded to DSA on 25 May 10.

Conclusion

This incident has identified a number of security issues at MOD, however, management appear keen to rectify this issue and seek DSA involvement in the conduct of a Physical Security Survey. The compactus where these items are ordinarily secured is in a secret terminal room with limited access but was not always locked. New security procedures have been introduced since the incident, including a new lock and code for the compactus. MOD have stated the compactus is now kept locked at all times when not in use. It is anticipated that Unit Standing Security Orders will be updated to include this requirement.

The movement of the propeller was not previously recorded, allowing for possible compromise. Access to the model propeller has now been reduced to two staff. A Classified Document Register has been introduced to record all movement of the propeller.

During the investigation, different theories were provided by MOD staff to account for the missing propeller. These included a person using it to highlight MOD security failings. It is also quite possible that an individual has made a genuine mistake in simply failing to secure the items correctly and has returned them anonymously so as to avoid any adverse criticism. Foreign Intelligence involvement is considered unlikely, due to the circumstances of the propeller's return.
20. The security investigation was unable to ascertain how or why the propeller went missing, or the persons responsible for its return. Investigators were unable to establish if the propeller was removed accidentally or deliberately. The Damage Assessment revealed the level of risk, if compromised, would be MINIMAL. There is a requirement for further improvements in security at MOD, due to the unit's ongoing involvement in sensitive projects.

Recommendation

21. As a result of this investigation it is recommended Chief MOD:
   a. consult with DSA – SA with a view to conducting a Physical Security Survey within the facility, specifically buildings 79 and 211; and,
   b. consider a review of the level of security training provided to MOD staff.

Paul Maynard
Assistant Director
Security Investigations Unit
Defence Security Authority