Submission No. 102

Australian Government
Department of Defence

Defence Signals Directorate
Information Security Group
Locked Bag 5076
KINGSTON ACT 2604

Ph: +61 2 6265-0197
Fax: +61 2 6265-0328

DSD 2002/1734
ASQ 007/04

Mr James Catchpole
Acting Secretary
Joint Statutory Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

ANSWER TO QUESTION ON NOTICE

At our most recent appearance before the Joint Committee of Public Accounts and Audit, DSD was asked to examine returns from Government agencies about IT security incidents experienced over the past few years, and to determine how many of these incidents were reported to DSD under the Information Security Incident Detection, Reporting and Analsyis Scheme (ISIDRAS) for Government agencies.

This task has now been completed and DSD's findings can be summarised as follows. Incidents reported to the Committee were 2453. Of those, 1758 should have been reported to ISIDRAS as per the requirements of the *Commonwealth Protective Security Manual*, but only 51 incidents were actually reported.

The attachment details how we arrived at these figures and includes a summary for each agency.

It is worthwhile noting that, while ISIDRAS as a scheme has existed since 1998, it has only been since 2002 (following the establishment of DSD's Computer Network Vulnerability Team) that DSD has been actively promoting its use. Since 2003, DSD has been promoting the mandatory reporting of successful attempts of breach of security; categories three and four respectively.

Increased agency participation in ISIDRAS has been encouraged with the launch of *OnSecure* on 3 December 2003. *OnSecure* is a joint initiative between DSD and the National Office for the Information Economy for enhanced on-line reporting of IT information security incidents. The objective of the *OnSecure* website is to complement the existing ISIDRAS scheme by giving Government agencies greater opportunity to register reportable IT security incidents.

If you require any additional information or clarification, please let me know. I can be reached on 02 6265-0323.

Yours sincerely

Michael Scotton
Acting Assistant Secretary
Information Security

19 February 2004

SUMMARY OF INCIDENTS

Portfolio	Incidents Reported to the Committee	Incidents Reportable to ISIDRAS	Incidents Reported to ISIDRAS	Notes
Agriculture, Fisheries and Forestry	33	32	0	ISIDRAS as a scheme commenced around 1998, but was not well known until 2002, when a conscious effort was taken to revitalise it. We began quietly promoting the scheme that year, coinciding with the maturing of the Computer Network Vulnerability Team as an incident response resource which could support agencies which required assistance. It was not until 2003 however that DSD actively began promoting the notion that reporting of category three and four incidents to ISIDRAS was mandatory under the *Protective Security Manual.* Hence the low level of reported incidents over the past five years.
Attorney General's	146	115	14	
Communications, IT and the Arts	15	15	2	
Defence	572	568	8	
Education, Science and Training	36	32	0	
Employment and Workplace Relations	49	48	3	
Environment and Heritage	80	78	1	
Family and Community Services	291	231	0	
Health and Ageing	138	122	1	
Industry, Tourism and Resources	207	207	13	
Prime Minister and Cabinet	33	33	2	
Transport and Regional Services	79	79	2	
The Treasury	774	198	5	ATO category 1 and two incidents not included
Totals	**2453**	**1758**	**51**	

Notes

1. It is not possible to determine the ISIDRAS category of many of the reported incidents from the level of detail reported by agencies. W

2. DSD has only been promoting the mandatory reporting of category 3 and 4 incidents since May 2003

AGRICULTURE, FISHERIES AND FORESTRY

Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Equipment loss/theft - 31 laptops and workstations	Y	N	
Wesite defacement June 2003	N	N	Suspected defacement, turned out to be false
Blaster worm infection	Y	N	

ATTORNEY-GENERAL'S

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Attorney-General's Department	Equipment theft - desktop computers (4)	Y	N	
	Equipment loss/theft - laptops (2)	Y	N	
	Equipment loss - PDA	Y	Y	
Administrative Appeals Tribunal	Equipment theft - laptops (3)	Y	N	
	Equipment theft - RAM	N	N	
Australian Crime Commission	Equipment theft - laptops (5)	Y	N	
	2002, Administrator password leak	N	N	
	2003, Virus through email	N	N	
	2003, User id and password given to unauthori	Y	Y	
Australian Customs Service	Equipment theft - laptops (11)	Y	N	

ATTORNEY-GENERAL'S

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
	Equipment theft - desktop computers (3)	Y	N	
	Equipment theft - Lite Pro	N	N	
	Equipment theft - internet modem	N	N	
	Equipment loss/theft - encryption equipment	Y	N	
	Equipment theft - server computers (2)	Y	Y	
	1998, unauthorised access to AFP database	Y	N	
	2000, unauthorised access to network	Y	Y	
	Goner.scr virus attack	Y	Y	
Australian Federal Police	Equipment theft - laptops (11)	Y	*	One laptop theft reported in March 2003
	Equipment theft - hard drive and memory	N	N	
	Equipment theft - modems (3)	N	N	
	External unauthorised access attempts (4)	*	N	These incidents may be category 2, hence reporting to ISIDRAS is optional
	Internal unauthorised access attempts (8)	*	N	These incidents may be category 2, hence reporting to ISIDRAS is optional

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
	Inappropriate use (2)	*	N	These incidents may be category 2, hence reporting to ISIDRAS is optional
	Virus attacks (17)	Y	*	Three of the 17 have been reported
Australian Institue of Criminology	Equipment theft - desktop computers (3)	Y	N	
	Equipment theft - other hardware and software	N	N	
	Web server intrusion	Y	Y	
ASIO	Equipment theft - laptop	Y	N	
CrimTrac	Equipment theft - laptop	Y	N	
Director of Public Prosecutions	Equipment theft - desktop computers (11)	Y	N	
	Equipment theft - laptops (3)	Y	N	

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Family Court	Equipment theft - laptops (4)	Y	N	
	Virus infections	Y	Y	The Family Court has twice reported significant virus infections to ISIDRAS (Bugbear and Nachi infections)
Federal Court	Equipment theft - laptops (2)	Y	N	
	Equipment theft - desktop computers (2)	Y	N	
	Equipment theft - file server	Y	N	
Federal Magistrates Service	Equipment theft - laptop	Y	N	
High Court of Australia	Equipment theft - laptop	Y	N	
Human Rights and Equal Opportunity Commission	Equipment theft - desktop computers (6)	Y	N	
	Equipment theft - laptops (3)	Y	N	
	Equipment theft - PDA	Y	N	

ATTORNEY-GENERAL'S

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Insolvency and Trustee Service, Australia	Equipment theft - unused computers (4)	*	N	As the computers were new and unused, DSD would class these as category 2 incidents, reporting to ISIDRAS is optional
National Native Title Tribunal	Equipment theft - laptops (5)	Y	N	
	Test website defacement	*	N	Agency considered this to be a category 2 incident and chose not to report
	Website defacement	Y	Y	
Office of Film and Literature Classification	Equipment theft - laptops (2)	Y	N	
Office of Parliamentary Counsel	Equipment theft - computer memory (2)	N	N	

COMMUNICATIONS, IT AND THE ARTS

Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Equipment theft - desktop computers (5)	Y	N	
Equipment loss/theft - laptops (7)	Y	N	
Equipment loss - PDA	Y	N	
Website defacement	Y	Y	
Loss of backup tapes	Y	Y	Reported by PM&C on behalf of Group V

DEFENCE

Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Equipment loss/theft - 1998-99 (117 computers)	Y	N	
Equipment loss/theft - 1999-00 (172 computers)	Y	N	
Equipment loss/theft - 2000-01 (145 computers)	Y	N	
Equipment loss/theft - 2001-02 (64 computers)	Y	*	Three of 64 reported, all by DSD
Equipment loss/theft - 2002-03 (23 computers)	Y	*	One reported, by DSD
Unauthorised access to computer systems (13 incidents)	Y	*	One reported to ISIDRAS
Inappropriate use of computer systems (18 incidents)	Y	*	Three of 18 reported to ISIDRAS

DEFENCE HOUSING AUTHORITY

Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Equipment loss/theft - desktop computers (3)	Y	Y	
Equipment loss/theft - laptops (13)	Y	N	
Equipment loss/theft - computer monitors (2)	N	N	
Equipment loss/theft - digital cameras (2)	N	N	

EDUCATION, SCIENCE AND TRAINING

Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Equipment loss/theft - desktop computers (4)	Y	N	
Equipment loss/theft - laptops (24)	Y	N	
Equipment loss/theft - mobile phones (4)	N	N	
Equipment loss/theft - hard drive from office PC	Y	N	
ILOVEYOU virus infection	Y	N	
Denial of service attack on web server	Y	N	
Welchia virus infection	Y	N	DEWR reported Welchia infection, no separate report from DEST

EMPLOYMENT AND WORKPLACE RELATIONS

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Department of Employment and Workplace Relations	Equipment theft - 24 computers	Y	N	
	Bogus email	N	N	
	ILOVEYOU virus infection	Y	Y	
	Welchia worm infection	Y	Y	
COMCARE	Equipment theft - laptops (4)	Y	*	The most recent of the four was reported to ISIDRAS
Office of the Employment Advocate	Equipment theft - laptops (3)	Y	N	
	1999 Unauthorised access to web server	Y	N	
	2001 Unauthorised access to web server	Y	N	
Defence Force Renumeration Tribunal	Equipment theft - laptop	Y	N	

EMPLOYMENT AND WORKPLACE RELATIONS

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Equal Opportunity for Women in the Workplace Agency	Equipment theft - laptops (3)	Y	N	
National Occupational Health and Safety Commission	Equipment theft - laptops (8)	Y	N	
	Equipment theft - desktop computer	Y	N	

FAMILY AND COMMUNITY SERVICES

Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Equipment loss/theft - desktop computers (94)	Y	N	
Equipment loss/theft - laptops (117)	Y	N	
Equipment loss/theft - PDAs (2)	Y	N	
Equipment loss/theft - printer, CD writer, zip drive	N	N	
Unauthorised access by FaCS staff (17 cases)	Y	N	
Unlawful information disclosure (59 cases)	N	N	
FTP server used to store images and music	Y	N	

HEALTH AND AGEING

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Department of Health and Ageing	Equipment loss/theft - desktop computers (4)	Y	N	
	Equipment loss/theft - laptops (40)	Y	N	
	Equipment loss/theft - PDAs (4)	Y	N	
	Equipment loss/theft - printer, CD ROM	N	N	
	Equipment loss/theft - hard drive	*	N	If new, would not be reportable
	Unauthorised access by former Minister	Y	N	
	SOBIG virus infection	Y	N	
Australian Institute of Health and Welfare	Equipment loss/theft - desktop computers (14)	Y	N	
	Equipment loss/theft - laptops (4)	Y	N	
	Equipment loss/theft - projector	N	N	
	ILOVEYOU virus infection	Y	N	
	Homepage worm infection	Y	N	

HEALTH AND AGEING

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
CRS Australia	Equipment loss/theft - desktop computers (14)	Y	N	
	Equipment loss/theft - laptops (14)	Y	N	
	Equipment loss/theft - printers (7)	N	N	
	Equipment loss/theft - MUXes, modems (2)	N	N	
	Equipment loss/theft - projector, scanner, UPS	N	N	
	Virus infections	*	N	Category two infections are optionally reportable
Food Standards Australia New Zealand	Equipment loss/theft - laptop	Y	N	
	ILOVEYOU virus infection	Y	N	
	Code Red worm infection	Y	N	
Australian Radiation Protection and Nuclear Safety Agency	Equipment loss/theft - printer	N	N	
	FTP server compromise	Y	Y	

HEALTH AND AGEING

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Accreditation Australia	Equipment loss/theft - laptops (8)	Y	N	
Private Health Insurance Administration Council	Equipment loss/theft - laptops (2)	Y	N	
Professional Services Review	Equipment loss/theft - desktop computer	Y	N	
	Equipment loss/theft - laptop	Y	N	
Health Insurance Commission	Equipment loss/theft - desktop computers (3)	Y	N	
	Equipment loss/theft - laptops (5)	Y	N	
	Equipment loss/theft - printer, CD burner	N	N	

INDUSTRY, TOURISM AND RESOURCES

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Portfolio	Equipment loss/theft (46 occurences)	Y	N	
	2002 unauthorised access from Internet	Y	Y	
	2003 denial of service	Y	Y	
	2003 loss of backup tapes	Y	Y	
	Virus infections	Y	*	7 reports (including 3 for FY 03-04)
Australian Government Analytical Laboratories	Equipment loss/theft - (11 occurences)	Y	N	
Australian Geological Survey Organisation	Equipment loss/theft - (9 occurences)	Y	N	
Australian Institute of Marine Science	Equipment loss/theft - (1 occurence)	Y	N	
Australian Nuclear Science and Technology Organisation	Equipment loss/theft - (4 occurences)	Y	N	

INDUSTRY, TOURISM AND RESOURCES

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Australian Sports Drug Agency	Equipment loss/theft - (1 occurence)	Y	N	
Australian Sports Commission	Equipment loss/theft - (22 occurences)	Y	N	
Australian Tourist Commission	Equipment loss/theft - (12 occurences)	Y	N	
	2002 website defacement	Y	N	
Australian Survey and Land Information Group	Equipment loss/theft - (8 occurences)	Y	N	
Commonwealth Scientific and Industrial Research Organisation	Equipment loss/theft - (64 occurences)	Y	N	
Geoscience Australia	Equipment loss/theft - (11 occurences)	Y	*	3 reports have been made
IP Australia	Equipment loss/theft - (11occurences)	Y	N	

PRIME MINISTER AND CABINET

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Department of the Prime Minister and Cabinet	Equipment loss/theft (7 occurences)	Y	N	
	2003 loss of backup tapes	Y	Y	Reported by PM&C on behalf of all affected Group agencies
Commonwealth Ombudsmen	Equipment loss/theft - (1occurence)	Y	N	
Australian National Audit Office	Equipment loss/theft - (19 occurences)	Y	N	
Australian Public Service Commission	Equipment loss/theft - (4 occurences)	Y	N	
	Gazette web site defacement	Y	Y	

TRANSPORT AND REGIONAL SERVICES

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Department of Transport and Regional Services	Equipment loss/theft - laptops (4)	Y	*	One incident in 2003 was reported, but only after it made the press and DSD investigated
	Loss of backup tapes	Y	Y	Reported by PM&C on behalf of Group
Civil Aviation Authority	Equipment loss/theft - laptops (17)	Y	N	
	2000 website defacement	Y	N	Advice given, but no formal ISIDRAS report made
Airservices Australia	Equipment loss/theft - laptops (46)	Y	N	
	Equipment loss/theft - desktop computers (10)	Y	N	

TREASURY

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
Australian Bureau of Statistics	Equipment loss/theft - laptops (22)	Y	N	
	Equipment loss/theft - desktop computer	Y	N	
	Equipment loss/theft - PDA	Y	N	
	2003 Blaster worm infection	Y	Y	
Australian Consumer Competition Commission	Equipment loss/theft - laptops (4)	Y	*	Two of four reported
Australian Securities and Investment Commission	Equipment loss/theft - laptops (6)	Y	N	
	Equipment loss/theft - desktop computer	Y	N	
	2003 unauthorised access	N	N	
Australian Taxation Office	Equipment loss/theft - server	Y	N	
	Equipment loss/theft - desktop computers (16)	Y	N	

TREASURY

Agency	Incident	Reportable to ISIDRAS	Reported to ISIDRAS	Notes
	Equipment loss/theft - laptops (137)	Y	N	
	FP&C incidents (574)	N	N	
	SecureNet team category 1 and 2 incidents	N	N	
	SecureNet team category 3 incidents (4)	Y	N	
Productivity Commission	Equipment loss - printer	N	N	
The Treasury	Equipment loss/theft - laptops (2)	Y	N	
	Website defacements (2)	Y	Y	