Almost all security classified and other official information is at some time held on a computer system. From time to time these systems and networks become targets for people who want unauthorized access to the information to read, alter or destroy.

The Commonwealth Government expects its agencies and all contracted service providers to recognise that official information is held on behalf of the Australian people and that it requires appropriate protection.

The Defence Signals Directorate (DSD), through the Information Security Group (ISG), is responsible for reporting to the Government on information technology and telecommunications security. All government agencies are required to report all significant IT security incidents to the DSD. (Protective Security Manual 2000: Part G)

ISG have developed a reporting and analysis scheme to help departments meet the security requirements set down in the Protective Security Manual. This scheme is called ISIDRAS (Information Security Incident Detection Reporting and Analysis Scheme).

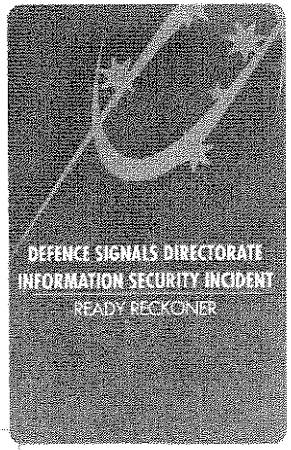
This scheme enables us to analyse trends in information security incidents and therefore help organizations secure themselves against future incidents.

ISIDRAS has been in existence since 1998 and the people within DSD who manage this scheme have learned that one of the most important IT security practices is to have a clear understanding of the procedures that should be followed if an IT security incident is suspected.

This pocket guide has been written for those Commonwealth Government agency employees with a responsibility for IT security.

It has a logical map of procedures to follow, relevant contact information, links to reporting forms and details of the services available to complement the good work already done by Commonwealth Government agencies.

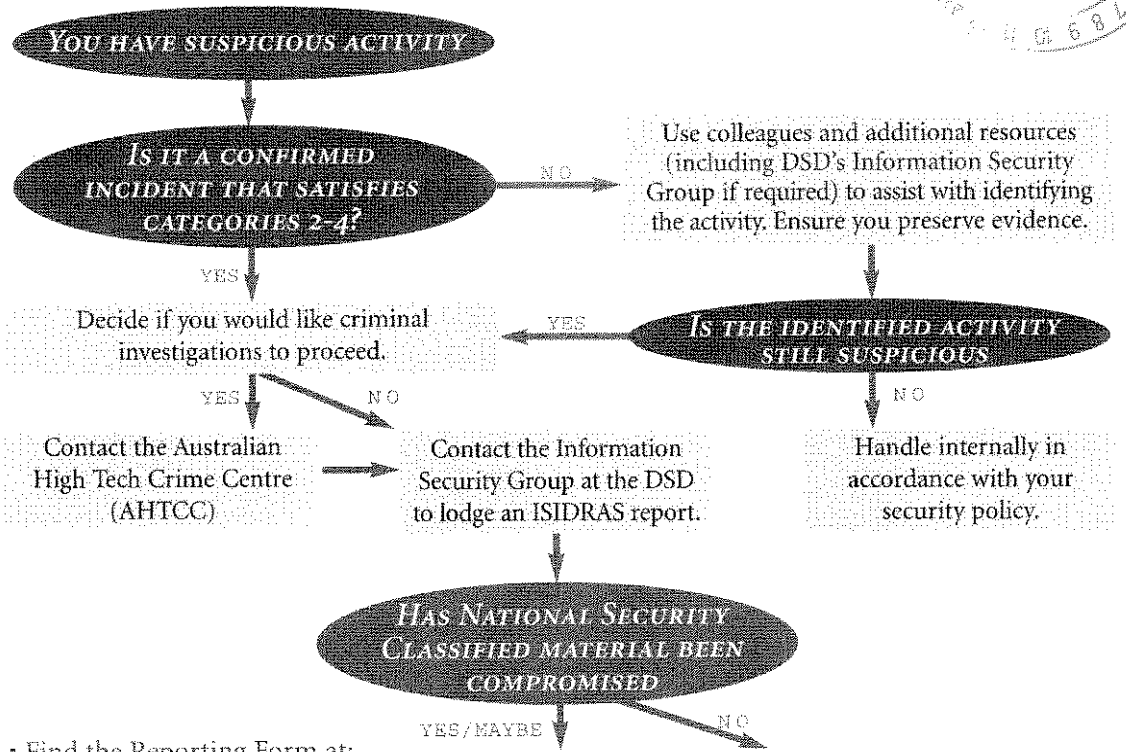
Please keep this guide handy and feel confident to make reports about significant IT security incidents your agency experiences.



LYNWEN CONNICK
Assistant Secretary
Information Security
Defence Signals Directorate

PROCEDURES FOR AN INCIDENT

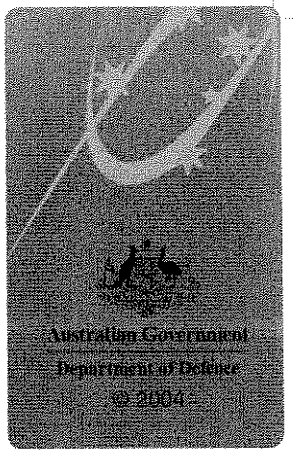
IMPORTANT: Where possible, keep detailed notes of your actions to assist investigators (whether or not you pursue criminal proceedings). Be aware that anything you do at this point may contaminate evidence.



• Find the Reporting Form at: www.dsd.gov.au/infosec/assistance_services/incident_reporting.html or the Onsecure website.

NOTES:

1. Follow your organisation's security incident procedures.
2. Keep the AHTCC, the Information Security Group and your supervisors informed of what is happening.
3. Call the Information Security Group at any point if you need advice or you are unsure of how to proceed. We can help you with incident containment, eradication, recovery and follow up. Contact details are over the page.



CHECKLIST

Consider the following before calling the Information Security Group or the AHTCC.

- Is the incident over or continuing?
- What type of system was affected – corporate network, web server etc.?
- What is the classification of the affected system?
- Has a source of the incident been identified?
- What actions were taken on the system – data modification, deletion, copying, etc.?
- What records are available – full header details, system logs, etc.?
- What classification level will you give to the details of your incident report? (Consult the Protective Security Manual for guidance).

ISIDRAS CATEGORY CHART

The Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) improves knowledge of both threats and vulnerabilities to Australian Government information systems. Incident reports are the basis for identifying trends in incident occurrences and for developing procedural, doctrinal, and training measures to prevent recurrence of similar incidents.

Each agency is requested to report incidents from categories 2 to 4 to Information Security Group at the Defence Signals Directorate, and can request assistance from us in the resolution of an incident if needed.

Category 1 Incidents	Recommended Action
These include events which cannot definitively be identified as incidents or attacks, and have no effect on system operations such as: - Isolated and non-repeated scans or pings from an external uncontrolled network. - Virus, trojan or worm detected and removed prior to being placed on an operational system or network. - Inappropriate content on a machine. - Abuse of privileges or password confidentiality by agency employee (not extending to superuser or root or administration privileges).	These incidents should be routinely handled by internal procedures and need not be reported to ISIDRAS.

Category 2 Incidents	Recommended Action
These also have no effect on system operations, and comprise identified but unsuccessful attempts to actively breach an information system security policy. Such events include: - Repeated active probes or port mapping from an external network. - Virus/trojan/worm found on a single system which has been successfully contained or removed. - Unsuccessful DOS/DDOS attempts (blocked at external firewall or router). - Attempt to gain unauthorised access to agency resources, either from within or outside of an Agency network. - Multiple repetitions of category 1 incidents.	These incidents should be routinely handled by internal procedures and reported to ISIDRAS.

Category 3 Incidents	Recommended Action
These include any successful attempt to actively breach an information system security policy on a single system, and may result in a minor or moderate effect on system operations. These could include: - Unauthorised access acquired by one or more unauthorised people to any account, at any access level. - Abuse of privileges or password confidentiality by agency employee, extending to super user, root or administration privileges. - Virus/trojan/worm found on more than one system, or an inability to contain and remove the code from a single system. - Defacement, alteration or deletion of web server files. - A successful attack against system services, for example, NIS, DNS, NFS, email, WWW, etc. including denial of service attacks. - A prank or hoax perpetrated from an external uncontrolled network. - Unauthorised access to or through a firewall. - Unauthorised modification to system files and system access controls. - Unauthorised modification to system hardware or software without the owner's or administrator's knowledge or permission. - National security compromises and disclosures arising from accidental or deliberate breaches of security policy whether intentional or unintentional. - Theft of equipment, loss resulting in possible compromise of classified or sensitive data. - Accidental equipment loss, resulting in possible compromise of classified or sensitive data.	Incidents of this nature must be reported to ISIDRAS. DSD can also provide incident response to such incidents if requested.

Category 4 Incidents	Recommended Action
These include any situation in excess of the examples given above, particularly where high level intervention or crisis management is required. Such incidents will usually have a major effect on system operation.	Incidents of this nature must be reported to ISIDRAS. DSD's Information Security Group and PSCA can provide assistance in handling such incidents if requested.

ISIDRAS IS NOT A SUBSTITUTE FOR A REFERRAL TO THE AHTCC IN THE CASE OF SUSPECTED CRIMINAL ACTIVITY

Contact Information

Defence Signals Directorate,
Information Security Group (ISG)
Telephone: ..... (02) 6265 0197
Fax: ..... (02) 6265 0328
E-mail: ..... infosechelp@dsd.gov.au
incidents@dsd.gov.au
admin@onsecure.gov.au
Web site: ..... www.dsd.gov.au/infosec
www.onsecure.gov.au

Other Contacts

Australian Federal Police (AFP)
Telephone: ..... (02) 6275 7575
Fax: ..... (02) 6275 7330
Web site: ..... www.afp.gov.au

Australian High Tech Crime Centre
Telephone: ..... (02) 6246 2101
Fax: ..... (02) 6246 2121
E-mail: ..... enquiries@ahtcc.gov.au
Web site: ..... www.ahtcc.gov.au

Reporting Information

The ISIDRAS reporting form can be found at:
www.dsd.gov.au/infosec/assistance_services/incident_reporting.html or the Onsecure website.
The classification of your report should be considered and it should be relayed to the Information Security Group at the Defence Signals Directorate in accordance with handling procedures described in the Protective Security Manual (PSM).

Unclassified details can also be posted, emailed, lodged via Onsecure or reported verbally by phone. Security-in-Confidence details can be posted or lodged via Onsecure. Please consult the contact information above.

Service Information

DSD's Information Security Group plays a key role in the protection of Australia's official communications and information systems.

As well as IT security incident reporting and assistance, the following services are available:
- Security audits
- IT advice and assistance
- Policy and doctrine guidance
- Information security product evaluation and;
- Management of an Evaluated Product List (EPL) to assist appropriate information security product selection.

Contact us if you would like to know more.

Notes: