HIB Number: 000773

Date/Time Transmitted: 23/01/2011 17:02

Subject: RELEASE OF DEFENCE RESTRICTED NETWORK (DRN) USER DETAILS TO THE AUSTRALIAN NEWSPAPER

Comment:

Action Area CIO

LIMITED DISTRIBUTION - NOT TO BE FORWARDED

HOT ISSUE BRIEF

RELEASE OF DEFENCE RESTRICTED NETWORK (DRN) USER DETAILS TO THE AUSTRALIAN NEWSPAPER

SENSITIVITY: The Australian newspaper notified Defence that it could access Defence DRN usernames and passwords. It is expected that this incident will result in a newspaper article by the Australian.

KEY ISSUES:

- On 21 January 2011 the Australian Newspaper contacted Defence Public Affairs to advise that their technical staff could obtain DRN usernames and password from anyone who accessed their website from the DRN.
- The password transferred to the Australian newspaper website was **not** the DRN user password. Rather, it was the password used to access the internet from the DRN. This password does not provide external access to the DRN.
- The Chief Information Officer Group in Defence has identified and remediated the fault.
- As a precaution all DRN users will be required to change their password.

- On 24 January 2011 Defence Public Affairs will thank the Australian newspaper for their assistance and advise them that the DRN passwords were not released to them.

Contact Officer:	**RADM Peter Jones HICTO**	**W: 61444345**	**M:** [redacted]
Authorised by:	**Mr Greg Farr CIO**	**W: 62667302**	**M:** [redacted]

Date issued: 23 January 2011

INADVERTANT RELEASE OF DRN USERNAMES AND PASSWORDS TO THE AUSTRALIAN NEWSPAPER WEBSITE

A number of internet websites, including that of the Australian newspaper, require authentication when connecting to their website. When DRN users access these type websites, the Defence Internet Gateway provided the individuals DRN username and their separate internet access password.

Once alerted to this, the Chief Information Officer Group amended the outgoing information from the Defence Internet Gateway to remove the DRN username and internet access password.

The provision of DRN username and internet access password does **NOT** allow access to the DRN. A risk exists if the individual has aligned their DRN password (which they are required to change every 30 days) with their internet password (which is perpetual). For this risk to eventuate, a threat source would need to have access to both this information and physical access to a Defence DRN terminal. This issue does not present a risk to the current DRN remote access (DREAMS) system, as it has two-factor authentication utilising a one-time use password token.

To mitigate the above risk, Defence will institute a change of all DRN user passwords. Furthermore, all DRN users will be reminded to ensure that their internet access password should be different from their DRN login password.

The requirement for these multiple passwords will no longer exist once the Single Password Project completes its roll out across the DRN early in 2011.

TALKING POINTS

- The Australian newspaper notified Defence that it could obtain some Defence Restricted Network details from those personnel who accessed their website through the Defence Restricted Network. It should be noted that to gain this information a very high level of technical skill was required.
- Defence has identified and remediated the fault.
- While release of Defence Restricted Network details was highly undesirable it did not compromise the security of Defence or individual information.
- Defence appreciates the early advice by the Australian of this matter.

Contact Officer:	RADM Peter Jones HICTO	W: 61444345	M: [redacted]
Authorised by:	Mr Greg Farr CIO	W: 62667302	M: [redacted]
PA Clearance by:	John Anderson	W: 6127 1955	M: [redacted]