



Changes to DSD's policy on cryptographic hash function SHA-1

Agencies are advised that DSD has removed the cryptographic hash function SHA-1 from the list of DSD Approved Cryptographic Algorithms (DACA) in the 2012 release of the Information Security Manual (ISM).

Since 2004, theoretically impressive attacks have been found against SHA-1. Although these attacks have improved over time, the results are still not practically applicable. SHA-1 is currently weakened but not broken; however DSD now considers the risk of using SHA-1 to be significant enough to remove it from the ISM as a DACA.

DSD currently approves the SHA-2 family of hash functions, and lists this family as DACAs in the ISM.

DSD's decision to remove approval for SHA-1 at this time is part of a staged approach. In 2010 DSD updated its ISM guidance to recommend the use of SHA-2 in preference to SHA-1.

This decision is closely aligned with a recommendation by the USA's National Institute of Standards and Technology (NIST) that the use of SHA-1 by US Federal agencies be discontinued by 2011.

NIST is currently running a competition to develop a new secure hash algorithm, which will be known as SHA-3. Results are expected to be finalised in 2012. When SHA-3 is announced, it will be considered for inclusion in the ISM as a DACA.

As per the ISM, agencies should use the latest version of the ISM when reaccrediting their systems. Agencies are reminded that the period between reaccreditations of systems should not exceed two years; and must not exceed three years.

Further Information

Australian government agencies seeking further information can contact DSD via:

OnSecure (www.onsecure.gov.au) forums, email to: assist@dsd.gov.au or call 1300 CYBER1 (1300 292 371).

T
S
E
C
U
R
I
T
Y