(UPDATED) JUNE 2014

(U) **LEGAL NOTICE:** THIS PUBLICATION HAS BEEN PRODUCED BY THE DEFENCE SIGNALS DIRECTORATE (DSD), ALSO KNOWN AS THE AUSTRALIAN SIGNALS DIRECTORATE (ASD). ALL REFERENCES TO ASD SHOULD BE TAKEN TO BE REFERENCES TO DSD.

Restricting administrative privileges explained

1. Restricting administrative privileges is one of the Top 4 strategies in the Australian Signals Directorate's (ASD) *Strategies to Mitigate Targeted Cyber Intrusions*. This document supports the implementation of the *Strategies to Mitigate Targeted Cyber Intrusions* by providing high-level guidance on how to restrict administrative privileges and examples of approaches that do not meet the intent of this strategy.

Why should administrative privileges be restricted?

2. Users with administrative privileges for operating systems and applications are able to make significant changes to their configuration and operation, modify critical security settings and access sensitive information. Domain administrators have similar abilities over an entire network domain, which usually includes all of the workstations and servers on the network.

3. Adversaries often use malicious code to attempt to exploit vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for an adversary's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.

4. An environment where administrative privileges are restricted is more stable, predictable, and easier to administer and support, as fewer users can make significant changes to their operating environment, either intentionally or unintentionally.

How to restrict administrative privileges

5. Simply minimising the total number of privileged accounts does not meet the intent of the restricting administrative privileges strategy. The correct approach to restricting administrative privileges is to:

   a. Identify tasks which require administrative privileges to be performed.

   b. Validate which staff members are required and authorised to carry out those tasks as part of their duties.

c. Create separate attributable accounts for staff members with administrative privileges, ensuring that their accounts have the least amount of privileges needed to undertake their duties.

d. Revalidate staff members' requirements to have a privileged account on a frequent and regular basis, or when they change duties, leave the organisation, or are involved in a security incident.

6. To reduce the risks of using privileged accounts, organisations should ensure that:

a. Staff members elevate from a standard user account to a privileged account to perform administrative tasks.

b. Privileged accounts do not have the ability to access the Internet or read email.

c. Administrative activities are performed on a separate physical workstation to that used for day to day non-administrative tasks.

d. Multi-factor authentication is implemented for privileged accounts.

e. Administrative activities are performed on hardened workstations that implement at least the Top 4 strategies as outlined in ASD's *Strategies to Mitigate Targeted Cyber Intrusion*.

7. All actions taken with privileged accounts should be logged and archived to provide an auditable history. This can assist in both real-time analysis of unusual behaviour patterns, as well as in any investigations following a cyber security incident.

8. Logging and auditing can also assist in identifying the number of active privileged accounts, the staff members who have access to them, and the tasks for which the privileged accounts are being used. This information will provide a clear understanding of the state of privileged account use in an organisation, and help ensure that a robust secure enterprise administration strategy is implemented.

Approaches which do not restrict administrative privileges

9. There are a number of approaches which, while they may appear to provide many of the benefits of restricting administrative privileges, do not meet the intent of this strategy, and in some cases may actually increase the risk to an organisation's network. These approaches include:

a. implementing shared non-attributable privileged accounts

b. temporarily allocating administrative privileges to regular users

c. placing standard user accounts in user groups with administrative privileges.

Further information

10. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian Government systems. The ISM can be found at: http://www.asd.gov.au/infosec/ism/index.htm.

11. ASD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies and supporting documentation can be found at: http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

Contact details

Australian Government customers with questions regarding this advice should contact the ASD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.