Insider Threat Awareness Program

WHO IS THE TRUSTED INSIDER?

1.1 The trusted insider—a current or former Defence employee or contractor— is anyone who has intimate and legitimate inside knowledge of an organisation and how it operates. Using this knowledge, a trusted insider can undertake malicious and disruptive acts, including disclosing classified information and facilitating unauthorised access into Defence facilities.

1.2 Trusted Insiders may intentionally compromise security to cause harm to Defence in a premeditated way, or inadvertently through poor security practices. Sensitive information can accidentally be disclosed when personnel do not carefully follow security policies and procedures.

1.3 External threat groups could target the trusted insider to gain access to Defence information, weapons or other military assets. Sensitive information can be unintentionally disclosed when personnel are targeted by foreign or domestic threats, or even the media. A key trusted insider threat is when personnel make unauthorised disclosures to media outlets. Only authorised personnel may talk to the media.

1.4 There are several main types of Trusted Insider activity:

a. unauthorised or inadvertent disclosure of sensitive information

b. corruption of process

c. facilitation of third-party access to an organisation's assets

d. physical sabotage

e. digital or ICT sabotage. a. appearing intoxicated or affected by a substance at work

2. OUR RESPONSIBILITY

2.1 Defence's and Defence Industry's best weapon against trusted insiders is for all personnel to be aware of the threat and ensure they meet their security obligations as a Defence security clearance holder, by reporting any concerning behaviours of colleagues as a matter of priority.

2.2 Behaviours of concern may include, but are not limited to:

a. appearing intoxicated or affected by a substance at work

b. increased nervousness or anxiety

c. decline in work performance

d. extreme and persistent interpersonal difficulties

e. statements demonstrating bitterness or resentment

f. creditors calling at work

g. sudden and unexplained wealth, and/or

h. unusual interest in sensitive or classified information.

2.3 If you observe any of these indicators, show an interest in that person's welfare and check if everything is okay. Simply having a conversation with them can be the first step. You must also report to supervisors observed changes in a colleague to proactively avoid serious consequences that might threaten the lives of your colleagues, Defence property or national security. This is not the time to think 'She'll be right mate,' or, 'It's un-Australian to dob in a mate.'

2.4 If something doesn't seem right, report it.

3. THIRD PARTY REPORTING OF POSSIBLE TRUSTED INSIDER

3.1 The first thing you should do is approach your supervisor/manager with your concerns.

3.2 Your Security Officer (SO) Nichola Vincent can also provide advice and assistance on contact reporting.

3.3 Complete form XP168 Report of Contact of Security Concern.

4. FURTHER INFORMATION

4.1 For further information contact any of the following:

a. DMV Consulting Security Officer Nichola Vincent using the disp@dmv.com.au.

b. Defence Security Incident Reporting security.incidentcentre@defence.gov.au Phone: 02 6266 3331

Authorised By: David Vincent

Position: Chief Security Officer (CSO)

Date Approved: 18th January 2021

Signature: