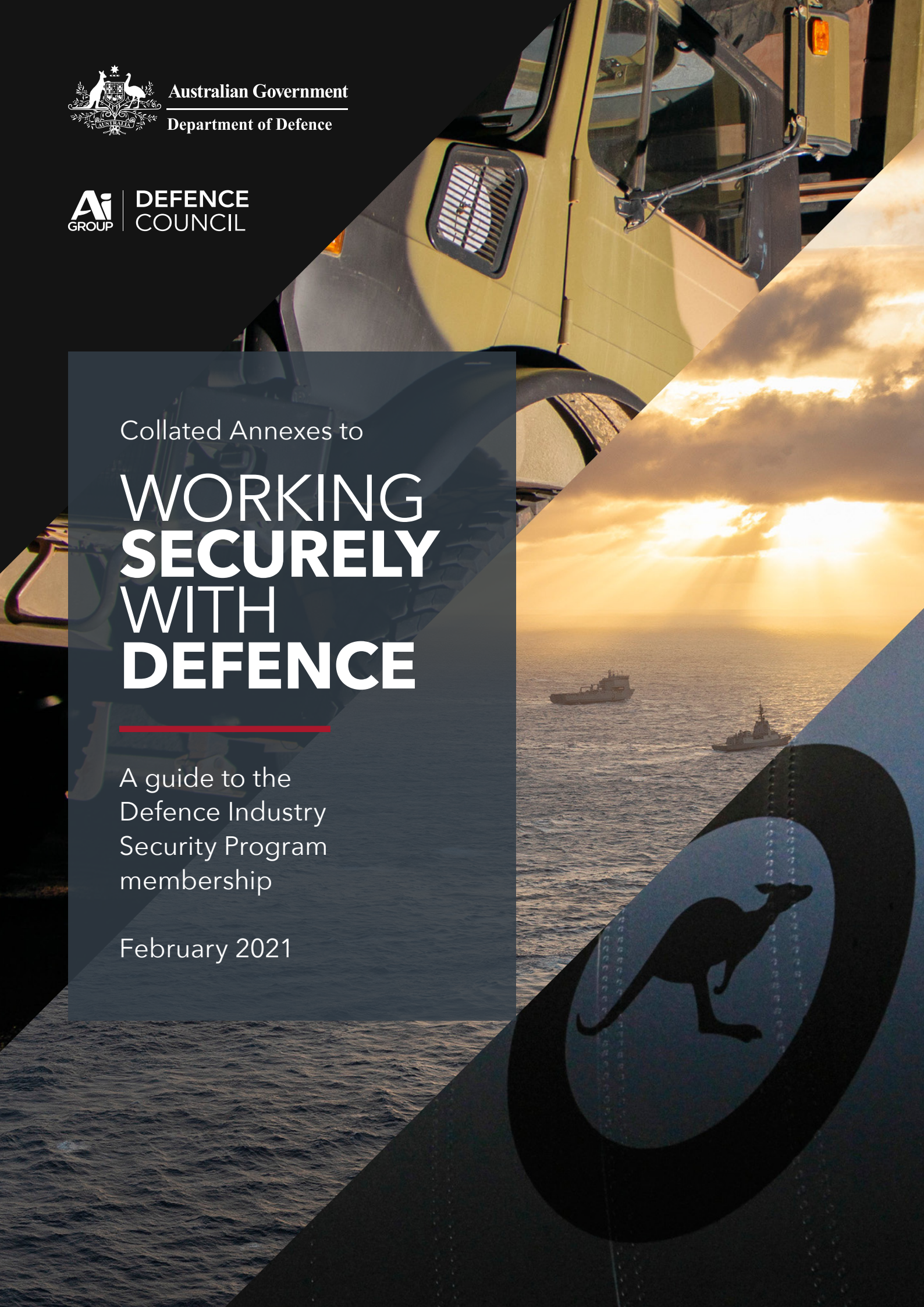
Australian Government
Department of Defence

Ai GROUP | DEFENCE COUNCIL



Collated Annexes to

WORKING SECURELY WITH DEFENCE

A guide to the Defence Industry Security Program membership

February 2021

Contents

Annex A: Important legislation and policies that guide defence industry security

Protective Security Policy Framework (PSPF)	In 2018 the Australian Government released the PSPF which sets out the revised security policy for Government entities, including governance, information, personnel and physical security. The principles and requirements within the PSPF flow down into the requirements for the DISP: https://www.protectivesecurity.gov.au/.
Defence Security Principles Framework (DSPF)	The DSPF was introduced on 2 July 2018. The move to the principles-based framework aligns Defence to the Australian Government PSPF and ISM. The DSPF provides principles, controls and instructions to support Defence personnel, contractors, consultants and outsourced service providers, to manage security risks. The link to an OFFICIAL version of the DSPF is here: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf.
Information Security Manual (ISM)	The Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD) produces the Australian Government ISM. The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats. Again, many of the principles and policies in the DISP flow down from the ISM: https://www.cyber.gov.au/acsc/view-all-content/ism.
Espionage and Foreign Interference Act and the Criminal Code Act	The *Criminal Code Act 1995* (Cth) was amended on 29 June 2018, as a result of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (EFI Act) which was passed by Parliament on 28 June 2018. The EFI Act amendments modernise and strengthen a range of espionage offences and introduce a number of new foreign interference laws, as well as a new aggravated offence for providing false or misleading information during a security clearance process. This provides Australian law enforcement and security agencies the necessary powers to investigate and the option to pursue prosecution. Criminal charges and imprisonment are now possible consequences for actions that would have previously been considered security incidents or breaches of administrative policy. The four main offences which industry need to have plans in place to mitigate are espionage, sabotage, foreign interference and the introduction of vulnerabilities. These offences are broad and applicable under circumstances including: deliberate or reckless acts; no intent to have a person or country in mind when the offence is committed; sabotage; and introduction of vulnerabilities to commonwealth equipment (or during production of equipment for the commonwealth) on industry premises. Therefore, industry should implement reasonable measures to mitigate these offences by having in place planned and risk-based levels of security.

	Many of these security measures also protect industry information against increasing trusted insider, cyber security and commercial threats. A link to the Defence policy is here: https://www.defence.gov.au/dsvs/industry/documents/EFI_Act_2018-Security_Officer_Guidance.pdf.
Privacy Act 1988 (Cth)	This legislation obligates industry to protect the privacy of individuals. It regulates how Australian Government agencies and organisations with an annual turnover of more than $3 million as well as others including smaller businesses with less than $3 million annual turnover, handle "personal information": https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information/. The legislation covers the collection, use, storage and disclosure of personal information. The Privacy Act includes 13 Australian Privacy Principles (APP), which apply to most organisations and Australian Government agencies. These are collectively referred to as "APP entities": https://www.oaic.gov.au/privacy/australian-privacy-principles/.
Notifiable Data Breach (NDB)	This obligation is part of the Privacy Act and applies to all entities with an annual turnover of more than $3 million and existing obligations under the Privacy Act, as well as others including smaller businesses with less than $3 million annual turnover if it meets certain requirements. A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If your organisation is affected, it must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach involving personal information is likely to result in serious harm. As Defence is a high-risk area for targeted cyber threats, a breach of personal data that is likely to result in serious harm may arise. Website: https://www.oaic.gov.au/privacy/notifiable-data-breaches/. More information on what to do in the event of a security incident is in Chapter 10 of the Guide.
Customs Act 1901 (Cth)	This legislation is the basis for controls on the export of tangible Defence and strategic dual-use goods and technologies. As the administering agency for the Customs Act, the Australian Border Force (ABF) has ultimate responsibility for ensuring that exports of regulated items are in accordance with the legislation. Goods may be prohibited for export unless all necessary export permits are obtained from the relevant permit issuing agency. In addition, goods may not be exported, or loaded on a ship or aircraft for export, unless they have been entered for export (some exemptions apply) and the ABF has given approval to export. Further controls may stop vessels or aircraft from departing unless the ABF has issued a Certificate of Clearance – this may be withheld if all export requirements for the cargo have not been met. Defence is responsible for administering Australia's export controls on Defence and strategic dual-use goods, with the exception of nuclear fuels and special

	fissionable material which are administered by the Department of Industry, Science, Energy and Resources.
Defence and Strategic Goods List (DSGL)	Controls are executed through the *Customs (Prohibited Exports) Regulations 1958*, Regulation 13E. This Regulation allows for permission to export regulated goods and technology listed in the DSGL (updated regularly). Defence Export Controls (DEC) is responsible for issuing export permits and licences to individuals and companies seeking to export regulated goods. Website: https://www1.defence.gov.au/business-industry/export/controls.
Australian Human Rights Commission Act 1986 (Cth)	This legislation provides for the Australian Human Rights Commission with the authority to investigate any complaint of unlawful discrimination. The Act permits the Commission to inquire into complaints of unlawful discrimination and any act or practice that may be inconsistent with or contrary to any human right. Employment practices in relation to employee screening may be captured by this legislation.
European Union's General Data Protection Regulation (EU GDPR)	If you are an entity which employs EU citizens (e.g. overseas staff or subcontractors) in your Defence work, you will be automatically obligated to comply with the EU GDPR. The EU GDPR is different to the NDB so it is important to understand your entity's obligations when handling personal data held of EU citizens (if any).

Annex B: How does Defence classify information?

About classification of information and physical assets

Information is assessed and classified (as well as sanitised, reclassified and declassified) by the originator of that information.

As the following is written from the Defence perspective, DISP members are the recipients of the business impact level assessments from the Defence contract managers.

The table below provides a summary of the classification of information.

Protective marking for information only	Business impact level	Compromise of information confidentiality
UNOFFICIAL	No business impact	No damage. This information does not form part of official duty.
OFFICIAL	1 Low business impact	No or insignificant damage. This is the majority of routine information.
OFFICIAL: Sensitive	2 Low to medium business impact	**Limited damage** to an individual, organisation or government generally if compromised.
PROTECTED	3 High business impact	**Damage** to the national interest, organisations or individuals.
SECRET	4 Extreme business impact	**Serious damage** to the national interest, organisations or individuals.
TOP SECRET	5 Catastrophic business impact	**Exceptionally grave damage** to the national interest, organisations or individuals.

Source: Protective Security Policy Framework (PSPF), https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx; https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx.

For a comprehensive list of security classifications, please see section 3.1 of Chapter 2 in the Guide.

The PSPF provides a useful tool for assessing the business impact level associated with classification of information in PDF and Word versions: https://www.protectivesecurity.gov.au/sites/default/files/2019-11/policy-8-table-1-business-impact-tool_0.pdf; https://www.protectivesecurity.gov.au/sites/default/files/2019-11/policy-8-table-1-business-impact-tool_0.DOCX.

Physical assets may have different degrees of value depending on their function or nature. The table below identifies the types of physical assets that may require some form of protection.

Asset category	Factors to consider when assessing and determining business impact levels
Valuable assets	• Financial viability and lead-time to replace/repair. • Capability of entity to operate without asset or in part. • Overall capability to which the asset contributes.
Classified assets	• Classification level of asset. • Asset mobility and accessibility e.g. heavy military equipment. • Assets classified due to confidentiality requirements of information they hold requires proper security classification.
Important assets	• Asset integrity e.g. human resources data or geographical data for aviation. • Asset availability e.g. ground transport fleet or firefighting equipment.
Attractive assets	• Asset desirability e.g. holds information attractive to a foreign adversary. • Asset portability e.g. tablet.
Significant assets	• Cultural or national significance e.g. national identity. • Negative reputational effect.
Dangerous assets	• Storage of assets that can inflict harm e.g. firearms, explosives and ammunition. • Hazardous materials that could cause harm.

Source: PSPF, https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx

Like classification of information, determining the business impact level for physical assets is an important part of an organisation's security risk assessment process. Factors to consider in such an assessment is provided in the table below.

Business impact level	Compromise, loss or damage of physical assets
1 Low business impact	**Insignificant damage** to an individual, organisation or government.
2 Low to medium business impact	**Limited damage** to an individual, organisation or government generally if compromised.
3 High business impact	**Damage** to the national interest, organisations or individuals.
4 Extreme business impact	**Serious damage** to the national interest, organisations or individuals.
5 Catastrophic business impact	**Exceptionally grave damage** to the national interest, organisations or individuals.

Source: PSPF, https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx

Annex C: Subcontractor / supply chain security

Based on the Protective Security Policy Framework (PSPF) and Australian Cyber Security Centre (ACSC) guidance, the following are recommended steps for businesses to consider when they enter into supply chain partnerships (especially cyber security) and/or procuring contracted goods and service providers:[1]

1. Identifying the relevant supply chain or procurement provider.[2]
2. Understanding the supply chain or procurement risk.
3. Setting security expectations with suppliers e.g. through terms and conditions in contracts.
4. Auditing suppliers and others to ensure ongoing security compliance.
5. Monitoring and reviewing security risk e.g. keeping good records of supply chain decisions and tracking assets and appropriately managing security incidents and raising awareness about supply chain security.
6. Improving supply chain security e.g. awareness about latest supply chain security risks including any specific Government directions and building strong relationships with supply chain partners on an ongoing basis.

For further information on understanding and assessing risk in the supply chain (particularly on cyber security) can be found on the ACSC website: https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management.

[1] https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management; https://www.protectivesecurity.gov.au/governance/security-governance-for-contracted-service-providers/Pages/default.aspx.
[2] The definition of supply chain can be interpreted quite broadly to extend to all entities involved in the development of the product or service before it reaches the end customer. For the purposes of supply chain security, refer to ISO 28000: https://www.iso.org/standard/44641.html.

Annex D: Security risk assessment example

Risk Assessment No:			
Initial Date:			
Revision No and Date:			
Person(s) conducting Risk Assessment			
Role	**Name**	**Signature**	**Date**
Risk Assessor or Team Representative			
Relevant Senior Manager			
Quality & Safety Manager			
Capability Acquisition and Sustainment Group (CASG) Acceptance **Position / Australian Public Service (APS) Level _____**			

Description:
Location / Business Group / Area Risk Assessment is being conducted.
Defence, and International Traffic in Arms Regulations (ITAR) Security.

(1.) DEFINE (Clearly define / specify the risk being assessed): Risk management / business continuity and focusing on Defence & ITAR Security.	
(2.) RISK CATEGORY (Please tick)	
Corporate	
Contractual	
Contractual (Project)	
Capital Equipment	
HSE, Hazards, Chemicals	
Contractors (Used on site)	
Suppliers / Subcontractors (AS9100)	
Safety Management Systems (SMS) / Quality Assurance / Regulatory	
Product	
Product Recall	
Security / ITAR	

IDENTIFY		ANALYSE			EVALUATE	
(3.) Identify Potential Risks / Hazards	**(4.) Worst Foreseeable Outcome**	**(5.) Initial Risk Analysis (see Tables 1-3)**			**(6.) Identify Management Controls**	**(7.) Current Control Effectiveness (see Table 4)**
		Likelihood (A-E)	**Consequence (1-5)**	**Risk (Low, Med, High, Ext)**		**Development of Process (A-E)**
Defence Workshop	Non-compliance, Security breach				Compliance, Requirements	
Australian Community Defence US Trade Treaty	Non-compliance				Compliance, Requirements	
Security Clearances	Unable to perform work for Defence contracts				Increase staff with Baseline and NV1	
Export of ITAR Controlled Item	Breach, Fines, Debarment				Insurance, Upskilling, Training, Consultancy, Compliance and licensing	
Technical Assistance Agreement (TAA)	Not in place, Not prepared carefully, Loss of Defence work				Training, Resource allocation	
ITAR Questionnaire & Screening Process	Not completed, Not assessed, Not acceptable status				Induction screening	
ITAR Non-disclosure agreement (NDA)	Not completed, Not assessed, Not acceptable status				Induction screening	
Technology Control Plans (TCP)	Not completed, Fines, Debarment				TCP completed, analysed, communicated	
Defence Industry Security Program (DISP)	Not entered, Loss of Defence work				DISP successful	

Notes:
1. Refer to “Key to Risk Assessment” below to populate the risk assessment.
2. Use a new Sheet for each revision of this risk assessment.
3. Entries in columns (3), (4), (6) and (10) are provided as examples only.

EVALUATE					TREAT		(12.) Risk Opportunity ($)
(7.) Current Control Effectiveness (see Table 4)	(8.) Risk Treatment Options (see Tables 1-3)			(9.) Target Risk Rating (Low, Med, High, Ext) (see Table 3)	(10.) Risk Treatment Option	(11.) Risk Action Plan (Y/N)	
Implementation of Process (A-E)	Likelihood (A-E)	Consequence (1-5)	Risk (Low, Med, High, Ext)				
					Training, Controls		
					Training, Controls		
					Security clearances application, Recruitment		
					ITAR consultant, Training, Time, Effort compliance		
					Resource allocation, Training		
					Induction, Analysis		
					Induction, Analysis		
					TCP completed, analysed, communicated		
					Complete DISP requirements		

KEY TO RISK ASSESSMENT

LIKELIHOOD (Table 1)		
RATING	%	FREQUENCY
A (Unlikely)	5%	Could happen but probably never will
B (Rare)	25%	Could happen but very rarely
C (Moderate)	50%	Could happen sometime
D (Likely)	75%	Could happen anytime
E (Almost Certain)	95%	Will almost certainly occur

CONSEQUENCE (Table 2)				
RATING	PROPERTY	LIABILITY	IMAGE	SAFETY
INSIGNIFICANT (1)	<$1K	<$1K	Minimal publicity	Minor injury
MINOR (2)	$1K - $10K	$1K - $10K	Some media coverage	Serious injury
MODERATE (3)	$10K - $100K	$10K - $100K	Moderate media coverage	Multiple injuries
MAJOR (4)	$100K - $1M	$100K - $1M	Adverse publicity	Disabling injury or death
CATASTROPHIC (5)	>$1M	>$1M	Extremely adverse publicity	Multiple disabling injuries and/or deaths

CONSEQUENCE (Table 2) (continued)				
RATING	QUALITY / SMS	REGULATORY	ENVIRONMENTAL	SECURITY/ITAR
INSIGNIFICANT (1)	Product failure resulting in minor injury	Observation	Negligible and sporadic discharges	Internal personnel providing confidential information to external sources
MINOR (2)	Product failure resulting in serious injury	Minor finding	Some uncontrolled discharges in minor quantities	Access of external personnel to site, and loss of confidential information
MODERATE (3)	Product failure resulting in multiple injuries	Minor finding requiring complex change	Moderate breach of environmental statute	Access to systems, restricted areas or personnel and loss of proprietary/ confidential information
MAJOR (4)	Product failure resulting in disabling injuries and/or deaths	Major finding	Major breach of environmental statute	Access to site and/or systems, restricted areas and loss of proprietary/ confidential information/ documents
CATASTROPHIC (5)	Product failure resulting in multiple disabling injuries and/or deaths	Lose certification	Shut down of operations due to environmental breach	Access to site and/or systems, restricted areas and loss of proprietary/ confidential information/ documents/ equipment

RISK ASSESSMENT MATRIX (Table 3)

		CONSEQUENCE				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
LIKELIHOOD	A (Unlikely)	Low	Low	Medium	Medium	High
	B (Rare)	Low	Low	Medium	Medium	High
	C (Moderate)	Low	Medium	High	High	High
	D (Likely)	Medium	Medium	High	High	Extreme
	E (Almost certain)	Medium	High	High	Extreme	Extreme

EFFECTIVENESS OF CONTROLS (Table 4)

Level of Development/Implementation	Development of Process	Implementation of Process
A	Fully developed	Fully implemented
B	Substantially developed	Substantially implemented
C	Partially developed	Partially implemented
D	Limited development	Limited implementation
E	No development	No implementation

Annex E.1: Personnel security assessment – Recruitment and induction

Notes:

Consider the risk of the individual's position – where required restrict system/administrative access.

In many cases, security processes (e.g. Security Clearance application) need to be commenced as soon as possible to allow the individual to actually work.

In rare cases, complex security processes (e.g. international clearance recognition) need to be commenced as soon as possible and will take significant time to complete.

NEW PERSONNEL	
Provide name, role, location and telephone number as follows:	Name: Role: Location: Telephone: E-mail:
Clearances?	Baseline ☐ Negative Vetting Level 1 (NV1) ☐ Negative Vetting Level 2 (NV2) ☐ Positive Vetting (PV) ☐

PERSON(S) CONDUCTING PERSONNEL SECURITY ASSESSMENT			
ROLE	NAME	SIGNATURE	DATE
Relevant Manager			
Security Officer (SO)			

Procedure	Responsibility (✓or ×below)		Completed (Signature(s))
	Manager	SO	
Recruitment			
Confirm if the position requires a Security Clearance (if yes, what level): _____			
Confirm if the individual has a checkable background to the required level i.e. 10 years for an NV1 clearance and pre-employment screening			
Confirm if the position requires an International Traffic in Arms Regulations (ITAR) Authorisation			
If the position requires a Security Clearance and/or ITAR Authorisation, confirm that the candidate is suitable			
Confirm that a national police check has been received and any issues discussed with security, prior to any offer being made			
Pre-employment screening in accordance with AS 4811-2006 completed without any concerns identified			
Offer made/Contract signed			
If the position requires a Security Clearance, SO to commence process			
Access card process (in particular Defence Common Access Card (DCAC)) – SO to commence process			
ITAR Authorisation, if relevant, via a Clearance or the ITAR Risk Assessment & Non-Disclosure Agreement (NDA) process (SO to coordinate with the Technology Control Officer (TCO))			

Onboarding			
Site Security induction training			
Security briefing			
Annual Security Awareness and Defence Security and Vetting Service (DS&VS) Document handling completed			
Designated Security Assessment Positions (DSAP) Register completed for security cleared positions			
New personnel has read, accepted and signed the Security Policies and Plans			
ITAR initial familiarity briefing, if relevant (SO to coordinate with TCO)			
Technology Control Plan to be updated, if relevant (SO to coordinate with TCO)			
Confirm and enable access to specific Classified Work Area (CWA)/ITAR/Treaty/“need to know” areas			
Update CWA access lists, if relevant			
Request IT System access, including virtual private network (VPN)			
Request access for Defence Remote Electronic Access and Mobility Services (DREAMS), etc			
Request Defence PROTECTED Network (DPN)/Defence SECRET Network (DSN) Access/Accounts			

Annex E.2: Personnel security assessment – Exit

Note: Where an employee is separated involuntarily from [Insert company name], the local Security Officer (SO) and Security Operations Centre (SOC) must be informed prior to the employee termination occurring.

	Procedure	Responsibility (✓or ✗below)		Completed (Signature(s))
		Manager	SO	
	Actions taken on resignation			
1	Risk assessment undertaken by Manager/HR/SO – outcomes may include: • Inform Company SOC for enhanced monitoring • Office access reduced to working hours • Immediate termination			
	Actions taken on leave date			
2	All access cards/Defence Common Access Cards (DCAC) returned to SO			
3	Credit Card reconciled and destroyed			
4	All Defence and Company keys returned			
5	Safe combinations, alarm codes or pins known to employee changed			
6	Company devices returned (i.e. Personal Protective Equipment (PPE), Phone, Laptop, Thumb Drives etc) and undertaking signed			
7	Create an out-of-office message for email and request SOC cancel/disable account			
8	All IT System access revoked			
9	Removed from all apps			
10	Employee reminded on security and intellectual property obligations in writing			
11	Locker and desk clean out with Manager and SO present (immediate termination)			
12	Company PPE clothing returned			
13	List all locations where the employee stored data including cloud storage platforms and notify the SOC to revoke access			

14	Remove employee from all access control security groups, virtual private network (VPN), etc			
15	If the employee has a clearance, cease Company sponsorship in Defence Online Services Domain (DOSD), complete SVA-007 / Declaration Of Secrecy and complete exit debrief			
16	Cancel Defence PROTECTED Network (DPN) / Defence SECRET Network (DSN) Access/Accounts, and collect Defence Remote Electronic Access and Mobility Services (DREAMS) tokens (if relevant)			
17	Revoke site alarm panel employee code			

Annex F: Physical security assessment example

Purpose

To ensure that [INSERT BUSINESS NAME], third party and Defence's information and assets, including classified information, security protected assets and high-risk unclassified assets are protected in accordance with Defence Security Principles Framework (DSPF) Control 72.1 – Physical Security and contractual obligations.

This Protective Security Survey (PSS) is to be completed to identify what assets and information are discussed, handled, processed or stored in each area, and what personnel have access.

This information is to be used to determine the level of security controls and accreditation for each area to ensure information and assets are being managed appropriately, and to ensure [INSERT BUSINESS NAME]'s compliance to the DSPF and to identify any non-compliances or security incidents relating to incorrect storage, handling etc. This information can also be used in business continuity planning and security risk management.

[INSERT BUSINESS NAME] is required to apply the minimum security controls detailed in the DSPF as determined by the classification and Business Impact Levels (BILs) of the information or assets being protected with consideration of the security risks. Where [INSERT BUSINESS NAME] is unable to meet requirements, or to enable security to be managed within the context of our business, a security risk assessment is to be undertaken and the residual risk accepted at the appropriate level as outlined in the DSPF or direction from the Capability Acquisition and Sustainment Group (CASG).

Facility Accreditation is to be undertaken in accordance with DSPF Control 73.1 – Physical Security Certification and Accreditation is required to assess the application of minimum security controls and permitting operation of a facility.

The PSS must be completed by the Chief Security Officer or Security Officer. If there is not enough room to provide detail in each section, make additional notes in the comments section referring to the section.

Details

Site:	
Project/s:	
Building/Room name or number:	
PSS completed by:	
Date completed:	

Section A: Room/Building

Does the room/building currently have an accreditation?	☐ YES ☐ NO
What is the current Security Zone for the room/building?	☐ Zone 1 ☐ Zone 2 ☐ Zone 3 ☐ Zone 4 ☐ NA ☐ Zone 5 ☐ Unknown
Answer this question last What Security Zone is required for the room/building?	☐ Zone 1 ☐ Zone 2 ☐ Zone 3 ☐ Zone 4 ☐ NA ☐ Zone 5 ☐ Unknown

Section B: People

Do uncleared personnel work in the room/building?	☐ YES ☐ NO	Comments:
Do/will security cleared personnel work in the room/building?	☐ YES ☐ NO	Comments:
Are/will all personnel working in, and with access to, the room/building appropriately cleared in accordance with the DSPF?	☐ YES ☐ NO	Comments:
Are foreign nationals working in the room/building?	☐ YES ☐ NO	Comments:
Will contractors/outsourced service providers require unescorted access to the area?	☐ YES ☐ NO	Comments:

Section C: Information/Material

What levels of commercial-in-confidence, OFFICIAL and classified information/material are or will be stored in room/building?	☐ Commercial-in-Confidence ☐ OFFICIAL ☐ OFFICIAL: Sensitive ☐ PROTECTED ☐ SECRET ☐ NA
What storage types are located within the room/building?	☐ Non lockable commercial storage ☐ Lockable commercial storage ☐ SCEC CLASS C ☐ SCEC CLASS B ☐ NA ☐ SCEC CLASS A ☐ Server rack(s) Detail: _____ _____
What levels of commercial-in-confidence, OFFICIAL and classified information or material is or will be handled or processed in room/building?	☐ Commercial-in-Confidence ☐ OFFICIAL ☐ OFFICIAL: Sensitive ☐ PROTECTED ☐ SECRET ☐ NA
What classification levels of information are discussed in the room/building?	☐ Commercial-in-Confidence ☐ OFFICIAL ☐ OFFICIAL: Sensitive ☐ PROTECTED ☐ SECRET ☐ NA
What is the level of commercial-in-confidence/Defence accredited ICT equipment installed/to be used within the room/building?	☐ OFFICIAL ☐ OFFICIAL: Sensitive approved ☐ Defence PROTECTED Network (DPN) ☐ Defence SECRET Network (DSN) ☐ NA ☐ **Other** Detail: _____ _____

Is there aggregation of information that should be considered?	☐ Yes ☐ No
Is foreign sourced material or information stored in the area? If yes, what is its classification level?	☐ OFFICIAL ☐ OFFICIAL: Sensitive ☐ RESTRICTED ☐ PROTECTED ☐ CONFIDENTIAL ☐ SECRET ☐ NA ☐ **Other** Detail: _____ _____

Section D: Assets

Does the room/building hold or will hold any security-protected assets? If yes, what are their classification level(s)?	☐ OFFICIAL ☐ OFFICIAL: Sensitive ☐ PROTECTED ☐ SECRET ☐ NA ☐ Unknown
Does the room/building/area hold or will hold high-risk OFFICIAL assets? [These were previously known as categorised assets – major, important, sensitive & attractive, support, routine.]	☐ YES ☐ NO☐ NA ☐ Unknown Details: _____ _____
What is the high-risk OFFICIAL asset/security protected asset allocated BIL? Also, provide details.	☐ 1 (Low-Medium) ☐ 2 (High) ☐ 3 (Very High) ☐ 4 (Extreme) ☐ NA ☐ 5 (Catastrophic) ☐ Unknown Details: _____ _____

Section E: Additional comments

Record additional details or comments

SECTION	ADDITIONAL COMMENTS

Section F: Non-compliances

Record any identified non-compliances for immediate follow up

SECTION	NON-COMPLIANCE DETAIL

Section G: Recommendations

Record any recommendations from the PSS

SECTION	RECOMMENDATION

Annex G: Further information about physical security zones

The following table provides additional information on how physical security zones relate to the DISP levels.[3]

Zone name	Description	Security classification / business impact level (bil)	Personnel security level clearance
Zone One	• Public access. • Examples: building perimeters, public foyers, public front desk, out of office areas including vehicles.	• Storage and use of sensitive and security classified information and assets with BIL of Low to Medium. [DISP Entry Level] • Use of sensitive and security classified information and assets with BIL of High. Storage not recommended but permitted if unavoidable. [DISP Level 1 and above] • Use of sensitive and security classified information and assets with BIL above High – only under exceptional circumstances with approval of originator. Storage not permitted. [DISP Level 1 and above]	• Employment screening.
Zone Two	• Restricted public access. • Unrestricted access for authorised personnel. • May use single factor authentication for access control. • Examples: office, out-of-office areas (including vehicles) with access control, front desk with authorised access.	• Storage and use of sensitive and security classified information and assets with BIL of High. [DISP Level 1 and above] • Use of sensitive and security classified information and assets with BIL of Extreme. Storage not permitted unless originator approves. [DISP Level 2 and above] • Use of sensitive and security classified information and assets with BIL of Catastrophic – only under exceptional circumstances with	• Min requirements: Ongoing access based on security risk assessment. • For stored security classified information and assets: Personnel security level clearance required corresponds with highest classified resources being accessed. • Ongoing access can be given to individuals without a security clearance or holding different levels of security clearances.

[3] The DISP levels identified in square brackets in the table are suggestions only based on the business impact levels and their associated security classifications (see Annex B). These business impact levels and classifications are set by the originator of that information (in this case, Defence), so it is important that DISP members (as recipients) understand how the classified information or asset is treated and associated security classifications to identify the relevant Physical Security Zone and DISP membership level.

Zone name	Description	Security classification / business impact level (bil)	Personnel security level clearance
		originator's approval. [DISP Level 3]	
Zone Three	• No public access. • Visitor access only for visitors with a need to know and with close escort. • Restricted access for authorised personnel. • Single factor authentication for access control. • Examples: security areas with access controls, work area with security classified work up to PROTECTED level.	• Storage and use of sensitive and security classified information and assets with BIL of Extreme. [DISP Level 2 and above] • Use of sensitive and security classified information and assets with BIL of Catastrophic – requires originator's approval. Temporary storage may be permitted up to 5 consecutive days. [DISP Level 3]	• Min requirements: Ongoing access based on security risk assessment. • For stored security classified information and assets: Personnel security level clearance required corresponds with highest classified resources being accessed. • Ongoing access can be given to individuals without a security clearance or holding different levels of security clearances.
Zone Four	• No public access. • Visitor access only for visitors with a need to know and with close escort. • Restricted access for authorised personnel with appropriate security clearance. • Single factor authentication for access control. • Examples: security areas with access controls, work area with personnel clearance at Negative Vetting Level 1.	Storage and use of sensitive and security classified information and assets with BIL of Extreme. [DISP Level 2 and above] Use of sensitive and security classified information and assets with BIL of Catastrophic. [DISP Level 3]	• For stored security classified information and assets: Personnel security level clearance required corresponds with highest classified resources stored. • Ongoing access given to individuals with same security clearance level for stored information and assets.
Zone Five	• No public access. • Visitor access only for visitors with a need to know and with close escort. • Restricted access for authorised personnel with	• Storage and use of sensitive and security classified information at TOP SECRET or information with BIL of Catastrophic. [DISP Level 3]	• Personnel security level clearance required corresponds with highest classified resources stored. • Ongoing access given to individuals with same security clearance level

Zone name	Description	Security classification / business impact level (bil)	Personnel security level clearance
	appropriate security clearance. • Dual factor authentication for access control. • Examples: Highest security areas, Australian Intelligence facilities.		for stored information and assets.

Source: PSPF, https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx; https://www.protectivesecurity.gov.au/sites/default/files/Table-2-security-zone-descriptions.pdf.

Another aspect for consideration relates to the use of security containers for classified information in physical security zones. See Annex H for further information.

Annex H: Additional physical security measure considerations

Security containers and cabinets

Appropriate storage of information or physical assets will depend on the classification and/or business impact level and the physical security zone in which they are stored.

The table below sets out the types of containers (or cabinets) that can be used in accordance with classifications, business impact levels and physical security zones. These include SCEC-approved security containers, which are designed for storing sensitive or classified information and assets.

Classification / Business Impact Level	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
OFFICIAL information – the compromise of information confidentiality of which would have a BIL of 1 (Low).	Lockable container	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access
OFFICIAL: Sensitive information – the compromise of information confidentiality of which would have a BIL of 2 (Low to Medium).	Lockable container	Lockable container	Lockable container	Lockable container	Lockable container
PROTECTED information – the compromise of information confidentiality of which would have a BIL of 3 (High).	Ongoing storage not recommended, if unavoidable Security Construction and Equipment Committee (SCEC) Class C	SCEC Class C	SCEC Class C	Lockable container	Lockable container
SECRET information – the compromise of information confidentiality of which would have a BIL of 4 (Extreme).	Not permitted	SCEC Class A	SCEC Class B	SCEC Class C	SCEC Class C

Classification / Business Impact Level	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
TOP SECRET information – the compromise of information of confidentiality of which would have a BIL of 5 (Catastrophic).	Not permitted	Not permitted	Not normally permitted. (In exceptional circumstances SCEC Class A)	Not normally permitted. (In exceptional circumstances SCEC Class B)	SCEC Class B

Source: PSPF, INFOSEC-8, https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.

For storage of mobile devices that process, store or communicate information, there may be different storage requirements depending on the physical security zone and level of security classification for that information. For further details, refer to PSPF INFOSEC-8.

For physical assets that are OFFICIAL or do not hold any classified information, commercial safes and vaults are an option. A useful summary of the minimum requirements for commercial safe and vaults at each Physical Security Zone is available from the PSPF in PDF and Word versions:
https://www.protectivesecurity.gov.au/sites/default/files/2019-09/policy_15_table_3_commercial_safes_and_vaults.pdf;
https://www.protectivesecurity.gov.au/sites/default/files/2019-09/policy_15_table_3_commercial_safes_and_vaults.docx.

In terms of maintenance of security containers and cabinets, the following practices should be considered:

- Access (including security keys) should be limited to the approved custodians who are authorised and appropriately security cleared personnel, and responsible for the contents and controlling access to the security container.
- The Security Officer (SO) should record details of the security containers, their locations and their custodians in the Security Register.
- The SO should maintain a register of all facility keys, security containers, combinations and keys. Combinations should be recorded in a manner that is only accessible to authorised personnel.
- Keys to containers holding classified material should be treated with the same level of security classification as the material stored in the containers.
- A key register must be maintained by the SO. Duplicate keys are not to be made except on the authorisation of the SO and recorded in the key register. An audit of your facility's keys must be performed at least every six months. The loss or compromise of a security key must be reported in accordance with DSPF Principle 77 Security Incidents and Investigations using the online form XP188 Security Incident Report: https://www1.defence.gov.au/security/industry/make-security-report.
- In the event of a compromise or suspected compromise of a security container, the SO must be informed immediately.
- Combinations should be changed regularly (at least every six months), after repairs, after change of personnel, and if there is a suspected compromise.

Security alarm system

Security alarm systems (SAS) are designed to detect unauthorised access and used with other measures to delay and respond e.g. security lighting. There are two types of SAS: one that detects unauthorised access along the perimeter of the facility; the other detects unauthorised access within the perimeter. Choice of alarms vary according to whether they are SCEC-approved or commercial, and their associated class level or type which will determine their suitability and function. For the purposes of this Guide, the PSPF summarises the appropriate SAS in the given physical security zones:
https://www.protectivesecurity.gov.au/sites/default/files/Table-3-physical-protections-for-security-zones.pdf.

In terms of maintenance of SAS, the following practices should be considered:

- If applicable, the SO should ensure that the SAS is installed, operated, maintained and monitored in accordance with the manufacturer's specifications and, where applicable, Australian Government specifications.
- The SO must ensure that detailed instructions are provided to the monitoring station and the contracted response team.
- Staff responsible for operating the system and responding to call outs need to be briefed by the SO on their role and the reporting actions required of them in the event of an alarm, or of any incident which threatens to reduce the effectiveness of the SAS.
- All alarm incidents and response actions are to be reported to the SO. The SO must investigate all reported incidents, provide advice and take necessary action to correct any security deficiencies immediately. Details of alarm incidents and response actions will be recorded in the Security Register.

Security guards

Security guards can play an important role in deterring unauthorised access as well as responding rapidly if there is a breach. Consideration needs to be given to the following when deciding on using security guards:

- If applicable, you may provide details of the guard entity contracted to your business to provide security services at each of your business's facilities. Guarding entities that provide services to Defence or DISP member sites must also be DISP members.
- The SO should ensure that detailed guarding instructions are provided to the guard entity's guards, that they are maintained, and that a backup procedure is in place. The SO should also ensure that the guards and other members of the response team are briefed on their role, and the response and reporting actions required of them in the event of an emergency or other reportable incident.
- A copy of the guarding instructions, response and reporting procedures within the Security Standing Orders, including the names and contact numbers of response team members, is recommended to be located where it can be readily accessible (e.g. this could be on your organisation's intranet site) and should be available to the relevant DS&VS officers.
- Eligibility to undertake security guard duty will need to meet personnel security requirements, and they will need to meet jurisdiction licensing requirements.
- Security guard response times, availability of guards, whether they are contracted or employed in-house, and whether they are stationary or patrolling all need to be factored into the security risk assessment.

ICT facilities

It is important that physical security is given special attention for ICT facilities. These facilities include: server and gateway rooms; data centres; backup repositories; and storage areas for ICT equipment that hold OFFICIAL information, communication and patch rooms. The appropriate physical security zoning including certification and accreditation, and/or implementation of physical measures will need to apply in accordance with the level of ICT sensitive and classified information located in that zone.

Further information regarding ICT and cyber security requirements are covered in Chapter 7 of the Guide.

Australian Government

Department of Defence

Ai GROUP | DEFENCE COUNCIL