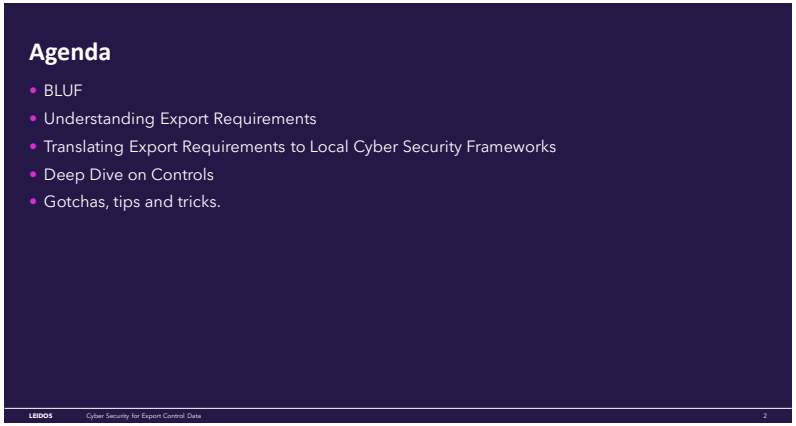
1



2

Note:

- This presentation focuses on United States export requirements
- There are likely to be similarities between countries, but apply the same process to their requirements.
- I'm also not an expert on legislation. There may be additional requirements not covered here.
- This is based on our current view of the legislation and requirements. In this uncertain world, this is likely to change.

3

BLUF

- If you meet an Australian security framework already, you most likely meet the requirements for storage of Export Control Data.
- Controls from legislation map to AU security frameworks as per below.

	CFR Reference	AU Reference	Mandatory/Best Practice
Encryption at Rest	22 CFR 120.54(a)(5) 22 CFR 120.54(b)	ISM-1080	Mandatory
Encryption in Transit	22 CFR 120.54(a)(5) 22 CFR 120.54(b)	ISM-0469	Mandatory
Access Control	22 CFR 120.55	ISM-1852	Mandatory
Data Tagging	Implied	PSPF-0063	Best Practice

4

Understanding Export Requirements

5

Key US Policy (1)

22 CFR 120.54(a)(5)

(5) Sending, taking, or storing technical data that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES-128); and

(iv) Not intentionally sent to a person in or stored in a country proscribed in § 126.1 of this subchapter or the Russian Federation; and

Note 1 to paragraph (a)(5)(iv): Data in-transit via the internet is not deemed to be stored.

(v) Not sent from a country proscribed in § 126.1 of this subchapter or the Russian Federation;

6

Key US Policy (2)

22 CFR 120.54(b)

(b)

(1) For purposes of this section, end-to-end encryption is defined as:

(i) The provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and

(ii) The means of decryption are not provided to any third party.

(2) The originator and the intended recipient may be the same person. The intended recipient must be the originator, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, such as by a license or other approval pursuant to this subchapter.

7

Key US Policy (3)

22 CFR 120.55 & 22 CFR 120.56

§ 120.55 Access information.

Access information is information that allows access to encrypted technical data subject to this subchapter in an unencrypted form. Examples include decryption keys, network access codes, and passwords.

§ 120.56 Release.

(a) ***Release.*** Technical data is released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person;

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad;

(3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or

(4) The use of access information to cause technical data outside of the United States to be in unencrypted form.

(b) ***Provision of access information.*** Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data.

8

What does that all mean?

- 22 CFR 120.54(a)(5):
  - Encrypted
  - FIPS 140-2 standard OR equivalent to AES-128
- 22 CFR 120.54(b):
  - Encryption-in-transit AND
  - Encryption-at-rest;
- 22 CFR 120.55 & 22 CFR 120.56
  - Access control for data and encryption material
  - Specified approved users

9

Translating Export Requirements to Local Cyber Security Frameworks

10

Australian Context

- We have a number of Australian security frameworks
  - Defence Industry Security Program
  - Information Security Manual
    - Independent Registered Assessors Program
    - Essential 8
  - ISO27001 Information Security Management Systems
  - Australian Energy Sector Cyber Security Framework

11

Key Australian Documents

Whole of Government Security Framework

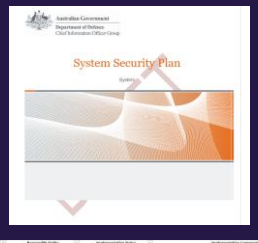
Defence Specific Security Framework

Whole of Government Cyber Security Framework

12

System Security Plan & Annex

- The System Security Plan:
  - Describes the architecture of the system
  - People, Processes and Technology
  - High level explanation of what security controls are implemented.
- The System Security Plan Annex:
  - Describes each control in detail and its implementation details.



13

Deep Dive on Controls

14

Encryption at Rest

Encrypting data at rest

When encryption is applied to data at rest it provides an additional layer of defence against unauthorised access by malicious actors. In doing so, it is important that full disk encryption is used as it provides a greater level of protection than file-based encryption. This is due to the fact that while file-based encryption may encrypt individual files, there is the possibility that unencrypted copies of files may be left in temporary locations used by an operating system. When selecting cryptographic equipment or software for this purpose, the level of assurance required will depend on the sensitivity or classification of the data.

Control: ISM-1080; Revision: 5; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media.

Control: ISM-0457; Revision: 9; Updated: Mar-22; Applicability: OS, P; Essential Eight: N/A
Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data.

Control: ISM-0460; Revision: 13; Updated: Sep-23; Applicability: S, TS; Essential Eight: N/A
HACE is used when encrypting media that contains SECRET or TOP SECRET data.

Control: ISM-0459; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition, is implemented when encrypting data at rest.

15

Encryption in Transit

Encrypting data in transit

When data is communicated over network infrastructure, encryption should be used to protect the data from unauthorised access or manipulation. When selecting cryptographic equipment or software for this purpose, the level of assurance required will depend on the sensitivity or classification of the data and the environment in which it is being applied.

Control: ISM-0469; Revision: 6; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
An ASD-Approved Cryptographic Protocol (AACP) or high assurance cryptographic protocol is used to protect data when communicated over network infrastructure.

Control: ISM-0465; Revision: 9; Updated: Mar-22; Applicability: OS, P; Essential Eight: N/A
Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used to protect OFFICIAL: Sensitive or PROTECTED data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.

Control: ISM-0467; Revision: 12; Updated: Sep-23; Applicability: S, TS; Essential Eight: N/A
HACE is used to protect SECRET and TOP SECRET data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.

16

ASD Approved Cryptographic Algorithms

ASD-Approved Cryptographic Algorithms

There is no guarantee of a cryptographic algorithm's resistance to currently unknown attacks. However, the cryptographic algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting. Approval for the use of the cryptographic algorithms listed in this section is limited to cases where they are implemented in accordance with these guidelines.

The approved asymmetric cryptographic algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Elliptic Curve Diffie-Hellman (ECDH) for agreeing on encryption session keys
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures
- Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for digital signatures
- Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) for encapsulating encryption session keys (and similar keys)
- Rivest-Shamir-Adleman (RSA) for digital signatures and transporting encryption session keys (and similar keys)

The only approved hashing algorithm for general purpose use is Secure Hashing Algorithm 2 (SHA-2). However, Secure Hashing Algorithm 3 (SHA-3), including its extendable-output functions (XOFs), is approved exclusively for use within ML-DSA and ML-KEM.

The only approved symmetric cryptographic algorithm is Advanced Encryption Standard (AES).

Where there is a range of key sizes for a cryptographic algorithm, some key sizes are not approved as they are insecure against current attacks or do not provide an adequate safety margin against possible future attacks. For example, advances in integer factorisation methods have rendered some RSA moduli sizes vulnerable and could render other RSA moduli vulnerable in the future.

17

AES

Using symmetric cryptographic algorithms

When using AES, a key size of 128 bits provides 128 bits of effective security strength, with larger key sizes providing more bits of effective security strength. However, for interoperability and maintainability reasons, AES-128 and AES-192 will not be approved beyond 2030.

The use of Electronic Codebook Mode with block ciphers allows repeated patterns in plaintext to appear as repeated patterns in ciphertext. Most plaintext, including written language and formatted files, contains significant repeated patterns. As such, malicious actors can use this to deduce possible meanings of ciphertext. The use of other modes, such as Cipher Block Chaining, Cipher Feedback, Galois/Counter Mode or Output Feedback, can prevent such attacks, although each has different properties which can make them inappropriate for certain use cases. AES is the only approved symmetric cryptographic algorithm.

Control: ISM-1769; Revision: 1; Updated: Dec-24; Applicability: NC, OS, P, S; Essential Eight: N/A
When using AES for encryption, AES-128, AES-192 or AES-256 is used, preferably AES-256.

Control: ISM-1770; Revision: 0; Updated: Mar-22; Applicability: TS; Essential Eight: N/A
When using AES for encryption, AES-192 or AES-256 is used, preferably AES-256.

Control: ISM-0479; Revision: 5; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.

18

ASD Approved Cryptographic Protocols

ASD-Approved Cryptographic Protocols

There is no guarantee of a protocol's resistance to currently unknown attacks. However, the protocols listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting. Approval for the use of the protocols listed in this section is limited to cases where they are implemented in accordance with these guidelines.

The AACPs are:

- Transport Layer Security (TLS)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format
- Internet Protocol Security (IPsec)
- Wi-Fi Protected Access 2
- Wi-Fi Protected Access 3.

19

Access Control (1)

Unprivileged access to systems

Personnel seeking access to systems, applications and data repositories should have a genuine business requirement validated by their manager or another appropriate authority.

In addition, centrally logging and analysing unprivileged access events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-0405; Revision: 7; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Requests for unprivileged access to systems, applications and data repositories are validated when first requested.

Control: ISM-1852; Revision: 0; Updated: Jun-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Unprivileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.

Control: ISM-1566; Revision: 3; Updated: Dec-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Use of unprivileged access is centrally logged.

20

Access Control (2)

Recording authorisation for personnel to access systems

Retaining records of system account requests will assist in maintaining personnel accountability. This is needed to ensure there is a record of all personnel authorised to access a system, their user identification, their agreement to abide by usage policies for the system and its resources, who provided the authorisation for their access, when their authorisation was granted, and when their access was last reviewed.

Control: ISM-0407; Revision: 5; Updated: Sep-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A

A secure record is maintained for the life of each system covering the following for each user:

- *their user identification*
- *their signed agreement to abide by usage policies for the system and its resources*
- *who provided authorisation for their access*
- *when their access was granted*
- *the level of access that they were granted*
- *when their access, and their level of access, was last reviewed*
- *when their level of access was changed, and to what extent (if applicable)*
- *when their access was withdrawn (if applicable).*

21

Optional Controls: Data Tagging

9.5 Security Caveats and Accountable Material

9.5.1 Security Caveats

Security Caveats are a warning that the information has special protections in addition to those indicated by the security classification. Security Caveats are not classifications and must appear with a security classification of PROTECTED or higher.

There are four categories of security caveats:

- Codewords (sensitive compartment information that requires a compartmental briefing)
- Foreign Government Markings
- Special Handling Instructions, and
- Releasability Caveats.

Each security caveat is governed by a 'controlling authority', responsible for managing and administering the security caveat. See the Australian Government Security Caveat Guidelines for details.

Requirement 0063 | INFO | All entities | 31 October 2024

The Australian Government Security Caveat Standard and special handling requirements imposed by the controlling authority are applied to protect security caveated information.

Requirement 0064 | INFO | All entities | 31 October 2024

Security caveats are clearly marked as text and only appear in conjunction with a security classification of PROTECTED or higher.

22

Tips and Tricks

23

Tips and Tricks

- **1: Cloud Services Inheritance**
  - Building off existing cloud services saves time, sustainment cost, and enables faster development
  - Services that deliver to Australian Federal Government must also have a System Security Plan.
  - They have also undergone an Independent Registered Assessors Program (IRAP) Audit.
  - Ensure that the cloud providers do not have the encryption material, and they are not hosted in a proscribed country.
    - AWS, Azure, Google, all allow external encryption management.
- **2. Know where you can store your data**
  - Organisations generally manage a register of their ICT systems
  - You can use this to put together a list of "approved export control" storage facilities
- **3: Get to know your cyber security lead**
  - DISP, Information Security Manual, ISO27001 all define a dedicated person for management of security.
  - Get to know them, understand what they manage, and get involved in their processes.

24

BLUF

- If you meet an Australian security framework already, you most likely meet the requirements for storage of Export Control Data.
- Controls from legislation map to AU security frameworks as per below.

	CFR Reference	AU Reference	Mandatory/Best Practice
Encryption at Rest	22 CFR 120.54(a)(5) 22 CFR 120.54(b)	ISM-1080	Mandatory
Encryption in Transit	22 CFR 120.54(a)(5) 22 CFR 120.54(b)	ISM-0469	Mandatory
Access Control	22 CFR 120.55	ISM-1852	Mandatory
Data Tagging	Implied	PSPF-0063	Best Practice

25

26