FORTRA

SOLUTION BRIEF (Titus)

Email Protective Marking Standards

What's Changed in v2018.2 and What to Consider When Transitioning to the New Version of EPMS

With the rapid growth of email use for interagency communications within the Australian government, a strong case was made for a standardised and machine-readable marking scheme for security purposes. Initially introduced in 2005, the Email Protective Marking Standard (EPMS) was created as part of the Protective Security Policy Framework (PSPF) to meet this need.

At their core, EPMS and PSPF require each entity to identify information asset holdings, assess the sensitivity and security classification of these assets, and implement operational controls for them proportional to their value, importance, and sensitivity. This framework then enables individuals to identify whether any information requires special handling measures.

As all Australian federal government agencies are affected by changes to the framework and standards, so too are organisations contracting with government entities.

Email Protective Marking Standards: How They Have Changed

The Australian EPMS has been updated several times since its origin in 2005, including changes in October 2018 that saw updates to the marking standards. These changes to the classification system came into effect on 1st January 2019, and usage of the previous system will cease on 1st October 2020.

The most recent changes to the EPMS include:

Updates to the Range of Security Classifications:

- UNCLASSIFIED has been renamed OFFICIAL
- CONFIDENTIAL classification has been removed

Change From Consolidated Dissemination Limiting Markers (DIms) to a Single Security Marking

- OFFICIAL: Sensitive

Addition of Information Management

Markers Changes to Caveat Types:

- Added CABINET special handling caveat
- Removed EO caveat
- Included Foreign Government markings in caveat hierarchy

Transition Considerations

While transitioning to EPMS v2018.2, your organisation should keep several considerations in mind:

1. Acceptance of both old and new standards: Does your organisation require users to be able to mark in both new and old versions of the standards at the same time?

2. Updating schema for new fields and adjusted policies: Is your organisation prepared to update schema for new fields and adjusted policies, such as recipient validation, for example?

3. Addition of optional elements: With this transition, do you require the addition of optional elements?

4. Sensitivity level changes: Does your organisation now need to mark material at a higher sensitivity level?

5. Although all of these questions are important, the biggest question to ask internally is "Are our users ready for change?" Without buy-in from users, your organisation's ability to comply with changes to EPMS become increasingly difficult.

How Titus Can Help

Titus has created user-friendly classification tools that clearly and accurately classify emails, documents and other files with user-selected, system-suggested or automatically applied settings, based on your data security policies.

Titus has released tailored solutions for Australian government agencies and contractors, which can assist agencies looking to comply with the new standard and ease the transition from previous versions of the standard. Not only does the Titus solution meet the v2018.2 standard, but it is also interoperable with previous versions of the standard, allowing organisations to transition either gradually or immediately.

How to Get in Touch

Let Titus be your trusted partner in ensuring compliance with EPMS v2018.2 and help make the journey to compliance that much easier. Reach out today to learn more about packages and pricing, and how Titus can be of assistance to your organisation.