Security Classification Guidance:

Counter-UAS (CUAS) Innovation Challenge

1. Purpose

This guidance provides proponents with security classification expectations for proposals submitted under the Counter-UAS (CUAS) Innovation Challenge. It is intended to support consistent classification of proposal information, project outputs, test data, technical documentation and capability development activities.

This guidance has been developed using Australian Government security classification principles and is aligned with the approach adopted in Defence Security Classification Guides, including the principle that contractors are responsible for assigning classifications to information they generate and that, where doubt exists, the higher classification should be applied pending Defence review.

2. Australian Security Classifications

For this Challenge, proponents should use only the following Australian protective markings:

- **OFFICIAL**
- **OFFICIAL: Sensitive**
- **PROTECTED**
- **SECRET** (only where specifically directed by Defence)

The majority of activities under the CUAS Innovation Challenge are expected to be conducted at **OFFICIAL** or **OFFICIAL: Sensitive**. Proponents are responsible for assigning appropriate classifications to information they generate and should apply the higher classification where uncertainty exists pending Defence advice. Information provided by Defence retains its assigned classification, and aggregated information may require a higher classification than individual elements if it reveals operationally sensitive capabilities, vulnerabilities or system-level understanding. Public release of any Challenge-related information is not permitted without Defence approval.

3. Classification Definitions

OFFICIAL

Apply to information where unauthorised disclosure would have limited impact on Defence interests.

Typical examples include:

- Administrative proposal information.
- Company capability statements.
- Collaboration arrangements.

- Technology development roadmaps.
- TRL assessments.
- Open-source research.
- High-level, non-sensitive technical concepts.

OFFICIAL: Sensitive

Apply to information where unauthorised disclosure could reasonably prejudice Defence capability development, reveal operationally useful technical information, or assist adversaries in understanding capability design or employment.

Typical examples include:

- Technical architectures and designs.
- Sensor integration approaches.
- AI algorithms and threat-classification methodologies.
- Swarm tracking and sensor fusion techniques.
- Defence integration concepts.
- Demonstration and test plans.
- Project schedules and milestones.
- Risk assessments.
- Test data and analysis.
- Functional descriptions.
- Design details.
- Manufacture and supply information.
- Photographs of prototypes, demonstrations or capability components.
- End-item descriptions and specifications.
- Capability information relating to Enable, Detect, Classify, Track, Neutralise and Exploit functions, consistent with the Annex C capability element classification guide.

PROTECTED

Apply where information reveals sensitive operational capabilities, performance limits, vulnerabilities or Defence-specific operational information that could materially degrade capability effectiveness if disclosed.

Typical examples include:

- Detailed system performance parameters.
- Detection, classification and tracking performance data.
- Detailed force-protection requirements.
- Defence operational threat data.
- Security architecture details.
- Identified system weaknesses or vulnerabilities.
- Vulnerability analysis reports.
- Electronic warfare susceptibilities.
- Communications vulnerabilities.

- Detailed integration information relating to operational Defence networks.
- Data revealing Defence tactics, techniques, procedures or operational limitations.

4. Default Classification Matrix

Information / Deliverable	Classification
Administrative proposal information	OFFICIAL
Company capability statements	OFFICIAL
Technical concepts	OFFICIAL: Sensitive
Project schedules and milestones	OFFICIAL: Sensitive
Methodologies and technical approaches	OFFICIAL: Sensitive
System architecture descriptions	OFFICIAL: Sensitive
Functional descriptions	OFFICIAL: Sensitive
Design details	OFFICIAL: Sensitive
Algorithms and software architectures	OFFICIAL: Sensitive
Interface specifications	OFFICIAL: Sensitive
Demonstration and test plans	OFFICIAL: Sensitive
Test results and reports	OFFICIAL: Sensitive
Operational analysis reports	OFFICIAL: Sensitive
Photos and imagery	OFFICIAL: Sensitive
Enable capability information	OFFICIAL: Sensitive
Detect capability information	OFFICIAL: Sensitive
Classify capability information	OFFICIAL: Sensitive
Track capability information	OFFICIAL: Sensitive
Neutralise capability information	OFFICIAL: Sensitive
Exploit capability information	OFFICIAL: Sensitive
End-item descriptions and specifications	OFFICIAL: Sensitive
Detailed performance data	PROTECTED
Security architecture details	PROTECTED
Vulnerability assessments	PROTECTED
Identified exploitable weaknesses	PROTECTED or higher
Defence-furnished information	As assigned by Defence

5. Test and Demonstration Data

Unless otherwise directed by Defence:

- Laboratory results, controlled trial results, demonstration outcomes and performance assessments should be treated as **OFFICIAL: Sensitive**.
- Detection, tracking, classification, sensor fusion and EW-resilience performance data should be treated as **OFFICIAL: Sensitive**.

- Any results revealing vulnerabilities, defeat mechanisms, capability limitations, exploitable weaknesses or Defence operational sensitivities should be classified **PROTECTED** as a minimum and referred to Defence for further assessment.

6. Security Declaration

Proponents should identify within their submission:

- The anticipated classification of the proposed technology and associated data.
- Any expected requirement to handle OFFICIAL: Sensitive or PROTECTED information.
- Available facilities, ICT systems and personnel clearances.
- Security controls for managing sensitive information.
- Any export control, foreign ownership, foreign influence or foreign partnership considerations.

7. Public Release

No proposal information, technical data, imagery, conference papers, publications, media releases or demonstration material associated with this Challenge is approved for public release unless expressly authorised by Defence.

8. Aggregation Principle

Information that is individually classified as OFFICIAL or OFFICIAL: Sensitive may require a higher classification when combined if the aggregation reveals:

- End-to-end CUAS architectures.
- Detailed operational performance.
- System vulnerabilities.
- Sensitive Defence integration pathways.
- Capability limitations or operational weaknesses.

Proponents must assess both the individual content and the cumulative effect of aggregated information when assigning classifications.