

**APPENDIX O****PROCEDURES FOR THE PROTECTION OF RESTRICTED INFORMATION****MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP****MISWG Document Number 6***(Amended 16 June 1999)***15 June 1989****PROCEDURES FOR THE PROTECTION OF RESTRICTED INFORMATION**

Some governmental information that is shared or exchanged in support of cooperative defence programmes and is not qualified under national rules for classification at the CONFIDENTIAL or higher level may not be disclosed publicly for reasons of national interest. It is, therefore, subject to specified protective procedures and is identified.

Documents and material containing such information shall be marked "RESTRICTED" by the Programme/Project Participating Countries that have such a security classification level. The Programme/Project Participating Countries that do not have this classification level shall apply an identification marking<sup>1</sup> (it may be a national classification level).

The chosen marking by all the Programme/Project Participants will appear in the "Security Classification Guide" and in the "Comparison of National Security Classification Markings" appended to the Programme/Project Security Instruction.

Whatever the markings may be they must provide for the information a degree of protection no less stringent than that provided by the control procedures described below.

These procedures will be appended to the Programme/Project Security Instruction when a Programme/Project includes a Participating Country that does not have a national security classification level of RESTRICTED or the equivalent. In those cases when there is no requirement for a programme security instruction, these procedures will be appended directly into a contract.

**A. RELEASE**

RESTRICTED information will be released only to the establishments or facilities in the NATO countries whose access is necessary for participation in a government programme, project, or contract, or for participation in a multinational cooperative defence programme. Release to any other government or institutions of another country, requires prior written approval by the originating country.

---

<sup>1</sup> For the United States the identification marking for Foreign Government Restricted Information will be "[enter country of origin – Restricted Information]" and additionally marked "Confidential- Modified Handling Authorized."

## B. ACCESS

1. Access to RESTRICTED information will only be given to those persons whose access is considered to be necessary in connection with a government programme/project or contract or for participation in a multinational cooperative defence Programme/Project.

2. All intended recipients of RESTRICTED information will be informed of their responsibilities for the safeguarding of such information and they may acknowledge these with a "binding declaration," where applicable.

## C. MARKING

Documents and material containing RESTRICTED information, and derivatives and reproductions containing the information, shall be marked to identify the RESTRICTED information and country of origin. The Programme/Project participating countries that have the security classification level "RESTRICTED" will mark such documents and material in accordance with their national rules for marking the documents. The Programme/Project participating countries that do not have this security classification level will mark such documents with the chosen marking that appears in the "Security Classification Guide" and in the "Comparison of National Security Classification Markings" appended to the Programme/Project Instruction.

## D. PROTECTION

RESTRICTED information will not be left unattended or otherwise handled in a manner that would result in unauthorized access. Documents or other material containing RESTRICTED information must be stored in a locked room, or in a locked cabinet, desk, safe or other such container that can be reasonably expected to preclude unauthorized access.

## E. TRANSMISSION

RESTRICTED information may be transmitted, including when necessary across national borders, by secured means through officially approved channels, in accordance with the national rules of the originating country. These channels may include use of government approved commercial encryption operated in accordance with approved security operating procedures, and overnight delivery services between specific points as authorized by contract.

## F. DESTRUCTION

Unnecessary documents or material containing RESTRICTED information shall be destroyed by any means that ensure that reconstruction of the residue is not possible.

## G. VIOLATION OF PROCEDURES

Violations of the safeguarding procedures that result in unauthorized access to

RESTRICTED information shall be investigated by the appropriate authority. Action will be taken, as appropriate, to limit the damage and to preclude a recurrence. When compromise is certain the owner of the information will be informed of the outcome of the investigation and corrective action.