

## CHAPTER 9

# THE MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP (MISWG)

### A. INTRODUCTION

1. The origin of the Multinational Industrial Security Working Group, or MISWG (mis-wig), can be traced to mid-1985. At that time, the United States (U.S.) Department of Defense (DoD) under new legislation designed to solicit cooperation with the North Atlantic Treaty Organization (NATO) allies in research and development efforts leading to the production of interoperable weapons systems, had begun to negotiate agreements for cooperative arms programs with those allies. The negotiators of the agreements for these early programs soon began to complain that the information and industrial security requirements of the various governments that were to be participants in the programs were not compatible. This lack of compatibility had become an impediment to international arms cooperation.
2. The U. S. Deputy Under Secretary of Defense (Security Policy) (DUSD(SP)) in 1985 was responsible, for DoD information and industrial security support for international programs. **(Note: The ODUSD(PS) international functions were subsequently transferred to the Office of the Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy (ODUSD/TSP&NDP). The industrial security functions were subsequently transferred to Office of the Deputy Under Secretary of Defense for Counterintelligence and Security.)** The DUSD(SP) instructed his Director for International Security Programs to contact his counterparts in those NATO countries that typically participated in international cooperative arms programs and develop a means to reconcile the security issues. Because bilateral German - U. S. security discussions were already scheduled at the time, the issue was discussed initially with the Director for Industrial Security from the German Federal Ministry of Economics (FMOE). The Germans agreed that incompatible security requirements among governments participating in the cooperative arms programs were becoming a problem, and procedures should be developed to apply standard security procedures to the programs. Both officials agreed that their counterparts in other NATO countries should be contacted to solicit their support of an initiative to solve the security issue. Consequently, they sent a letter signed by the DUSD(SP) and his counterpart in the FMOE, the Deputy Under Secretary of Economics, to their counterparts in the other NATO countries, suggesting that they all meet in Bonn to discuss the issue and seek a solution. They also personally contacted their counterparts to alert them to the initiative. All countries that were contacted expressed an interest in an initiative.
3. Later in 1985 the German Federal Ministry of Economics hosted a meeting in Bonn of industrial security officials from all of the NATO countries, less Iceland. (Iceland declined, because it was not participating in the cooperative arms programs.) The German, United

Kingdom (UK), and U. S. representatives proposed the establishment of a working group which would review each country's security procedures, determine the extent of any differences, and make recommendations for standard procedures. However, the German and Dutch representatives raised two questions: 1) was the NATO Security Committee the appropriate forum in which to discuss the initiative; and, 2) was the group to be an officially constituted group or an ad hoc group? It was agreed that the NATO Security Committee should not be involved because the principal purpose of the initiative would be to address security issues for non-NATO cooperative programs among NATO members, and possibly other countries. It was decided that the representatives would pursue the question of the status of the group with other officials within their respective governments. The Belgian representative agreed to host another meeting to discuss the results.

4. The Belgium meeting was hosted at the facility of the European F-16 Production Group outside of Brussels in early 1986. Each country's representative presented a briefing on industrial security requirements, and differences were noted. When the discussion turned to the status of the group, the French delegation did not favor the establishment of a formal, legally constituted group, and recommended that it operate under an ad hoc arrangement. The other representatives agreed. It was decided that the group would be limited to NATO member nations, a position that was later changed (see below). The name Multinational Industrial Security Cooperation Working Group was also adopted. The name was shortened at a subsequent meeting, hosted in the UK, to Multinational Industrial Security Working Group, abbreviated MISWG. A standard emblem for the MISWG was developed by the Netherlands in 1993.

5. These decisions raised another question – how to ensure that procedures developed by the group were used in cooperative programs. The establishment of the Senior Security Officials answered this question. The National Security Authorities (NSAs) (i.e., those officials recognized in NATO security regulations) or senior officials in each country who were responsible for international industrial security matters (Designated Security Authorities (DSAs)), would represent their countries at Forum meetings. The Senior Officials would meet approximately annually. They would approve any study initiatives that were proposed by the working group and approve any procedures that resulted from the initiatives. This would be accomplished in a set of minutes in which the signatories would “endeavor to ensure” that the procedures recommended by the group would be applied to cooperative programs.

6. It was also decided that because the MISWG is an ad hoc group, it would not be necessary for each member country to subscribe to recommended procedures in order for them to be adopted. Those countries that desired to use the procedures could sign the minutes reflecting their agreement to use them; any country that did not desire to use them would not sign the minutes and not be obligated to use them. In fact, all of the documents were eventually accepted by all of the countries. The Seniors Forum continued to meet until November 1998 when it was decided that, since the Seniors were often participating in the working group meetings, the groups would be combined. Acceptance of the Working Group minutes by the participants was considered intent by the nations to use the procedures in cooperative programs.

7. Initially, MISWG member countries were encouraged to consult with their program management officials and defense contractors to develop recommendations for procedures to be analyzed and standardized by the member countries. The current MISWG documents number 1 (Hand Carriage Procedures) and number 7 (International Visits) resulted from that initial effort. Document number 2 contained the original procedures for visits, but these procedures proved to be impractical. Document number 2 was cancelled and new procedures were published as document number 7. Subsequent documents (currently numbering 20) addressed other procedures for industrial security.

8. The MISWG initially met at least twice a year, particularly when the first 20 MISWG documents were being developed. The MISWG now usually meets at least annually. The members are afforded the opportunity to meet face-to-face with their counterparts from other countries and discuss current security issues that would be difficult to discuss by mail, the telephone, or by e-mail. Many participants have noted that by knowing their counterparts on a personal basis, and by meeting with them face-to-face, many problems that might otherwise have been impediments to cooperation have been solved. The MISWG also may designate sub-groups to analyze and prepare recommendations on a particular issue. With the advent of automated information systems, the MISWG participants are able to conduct a lot of business over the Internet.

9. Although the MISWG was established originally to standardize security procedures for non-NATO cooperative arms programs involving NATO member nations, other countries have asked to use the MISWG procedures in their cooperative arms programs. As a result, the procedures were made available to many other countries, and are now posted on the Internet for public use. The procedures also have been used by defense contractors in some countries (e.g., the UK and the United States) to apply standard procedures for commercial contracts. More recently, the NATO Security Committee incorporated many MISWG procedures in the NATO security regulation. Many NATO member nations have adopted MISWG procedures as their national procedures.

10. Membership in the MISWG originally was limited to NATO member countries, however the idea of inviting non-NATO countries to become members was discussed at several meetings. Major concerns expressed by some countries were that non-NATO countries might not have the same objectives and motivation as the NATO countries, and with the addition of new members the group might become too large to remain effective. However, in 1999 at the meeting in Madrid, Spain the original MISWG member countries agreed to invite Sweden into the group. Austria and Switzerland were invited at the meeting in Budapest, Hungary in 2000, and Finland at the meeting in Switzerland in 2005, bringing the total of participant countries to twenty. These non-NATO countries were sponsored by NATO countries whose companies participated in industrial arrangements with companies in the other countries. The Scope of Operations of the MISWG was amended at the meeting in The Hague, the Netherlands in 2001 to describe criteria and procedures under which non-NATO countries might be invited into the MISWG in the future. At that time, the term referring to countries participating in the MISWG was changed from "Member" to "Participant."

11. Finally, in addition to its efforts to standardize security procedures for cooperative programs, the MISWG also conducted briefing sessions related to security and export control for the so-called "Partnership for Peace" countries of Central and Eastern Europe which aspired to join NATO. These sessions, which were held at the Marshall Center in Germany in October 1994 and in Trenčin, Slovakia in September 1996 helped to establish MISWG procedures in those countries' developing industrial security programs.

## **B. PROGRAM DOCUMENTS.**

The MISWG documents are described in the following paragraphs. Some of the documents are procedural in nature; others contain language that is to be placed in international agreements. It is important to note that each government that is a party to an agreement or contract, or that has legal jurisdiction over information involved in the agreement or contract will have to agree to the procedures. Therefore, they must participate in the preparation of the of program or project documents that are based on the procedures. This is particularly important with respect to the Program/Project Security Instruction, or PSI, (Document #5). The documents are guides; they should not be specifically referenced in the documents that support a specific program or contract. Each document is to be used to tailor security procedures that implement the security requirements of agreements and contracts, or as required by a Technology Assessment/Control Plan (TA/CP) or PSI. In some cases, procedural language is suggested. It is the base-line language that has been agreed to by the MISWG countries; therefore, it must be used as the starting point when a particular procedure is to be used. Because an international program will involve several countries, their security authorities will have to approve the procedures to be used; therefore, the final content of a document will have to be negotiated among those authorities. They should, therefore, participate in the preparation of the documents to be used. If the MISWG documents will be used in a PSI supporting an international agreement, the National Security Authorities (NSAs) or Designated Security Authorities (DSAs) of the participating countries will have to approve the PSI (the DSA for DoD is the Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy (DUSD/TSP&NDP)). The Defense Security Service may approve the use of MISWG documents for a commercial initiative.

## **C. MISWG DOCUMENTS**

**1. Arrangements for the International Handcarriage of Classified Documents, Equipment and/or Components.** These arrangements provide an exception to transmitting classified material through official government channels. In order to meet an urgent need to transfer documents and small items of hardware between contractors in connection with a government project, program or contract, these special arrangements may be used on a case-by-case basis with approval of each Designated Security Authority. An urgent situation is one when official government channels are not available or their use would result in a delay that would adversely affect performance on the project, program or contract to an unacceptable degree, and it is verified that the information is not available at the intended destination. The arrangements apply to the handcarriage by an appointed courier of classified documents and hardware that are of such size, weight, and configuration the courier can maintain personal control over them at all times. The highest classification must not exceed SECRET and the documents and hardware

must have been authorized by the responsible Government agency for release in conjunction with the project, program, or contract. The procedures applicable to this document are discussed in detail in this Chapter and Appendix K.

2. (This paragraph was left blank to allow the paragraphs that describe the MISWG Documents to correlate with the numbers of the Documents. There is no #2 Document.

**3. Use of Cryptographic Systems.** These procedures (Appendix L) provide for the electrical transmission, using approved crypto systems, of classified information across international borders by participating governments and contractor organizations in support of a government project program or contract. The use of such equipment will be authorized on a case-by-case basis by National Security Authorities or Designated Security Authorities when there is a compelling requirement, after coordination with national communications security authorities.

**4. Security Clauses.** These clauses (Appendix M) are tailored for the typical international agreement. The International Agreements Generator (IAG) clause data base maintained by the Navy International Programs Office (IPO) should be consulted for the appropriate clauses (see Chapter 5, subsection C.7.).

**5. Program/Project Security Instruction.** Appendix N provides a sample standard format for a Program/Project Security Instruction (PSI). Most cooperative program agreements require a PSI.

a. The PSI is supplementary to the national security rules of the participants under which classified information and material are normally protected. It should be used to reconcile differences in national policies so that standard procedures will be used for the program/project and to consolidate in a single security document the other security arrangements for a project, program or contract (e.g., handcarriage, transportation plan, etc.). When a program or project involves the use of both national and NATO procedures, special attention must be given to differences in the procedures, particularly with regard to access control.

b. The minimum elements of information to be provided for each section are described, and in some cases, suggested language is provided. These descriptions and suggested language are for guidance only. However, it is advised that the guidance be followed because the suggested format and procedures have been agreed upon by many nations. Additional requirements may apply depending on the size and complexity of the program/project, sensitivity of the information involved, and any extraordinary security requirements that may be determined by the foregoing factors.

c. The decision on the specific procedures to use is one that requires an understanding of the overall organization and requirements for the program or project. Program managers and participating contractors must ensure security and technology transfer personnel are provided this information. The agreement and TA/CP also must be consulted. The final decision on which procedures to use is thus a joint decision. Consideration should be given to the establishment of a security team to develop the PSI. The team should be comprised of

representatives from all participating governments and contractors. When several sets of procedures are determined to be necessary, they should be consolidated in a program security instruction.

d. The PSI will include the other MISWG documents, but only those that are required for the program. Each document that is to be used must be developed as a final procedure for the particular function that is described. The exact content must be negotiated to ensure compliance with each government's laws and regulations. The MISWG documents at Appendices K, O, P, S, T, U, Z and BB and procedures for secure communications will appear in most PSIs. Also to be included are procedures for handling program information.

**6. Procedures for the Protection of Restricted Information.** This document (Appendix O) provides agreed upon procedures for handling RESTRICTED information. Participating countries that have a classification level of RESTRICTED will so mark their documents appropriately. The participating countries that do not have a classification level of RESTRICTED will apply an identification marking (it may be a national classification marking) which appears in the "Security Classification Guide" and the "Comparison of National Security Classification Markings" appended to the PSI. Whatever the markings may be, they must provide the information a degree of protection no less stringent than that provided by the control procedures described in MISWG Document Number Six. The United States normally applies the marking, "Handle as CONFIDENTIAL--Modified Handling Authorized" to this category of material.

**7. International Visit Procedures.** This document (Appendix P) covers international visit procedures for both government and contractor personnel. It provides standard procedures for one-time and recurring visits, emergency visits and a standard request format for visit requests. It contains a table which gives the number of working days prior to the date of the onetime visit or the date of the first recurring visit that the request must be in the possession of the receiving NATO member nation National Security Authority or Designated Security Authority. See also Chapter 7 of this handbook.

**8. Controlled Unclassified Information Clauses.** The clauses (Appendix Q) cover the handling of controlled unclassified information exchanged between governments or generated under an international program. Using the clauses, the section of the MOU dealing with controlled unclassified information must properly cross-reference the security, third-party sales and transfers, and disclosures and use of program information sections of the MOU (See Chapter 5, of this handbook).

**9. Security Education and Awareness.** This document (Appendix R) provides guidance for security education and awareness programs. When used in connection with an international program, the guidance may be tailored to the program and incorporated into the PSI. Individual security education plans should be tailored to fit the specific requirements of each program or project. Some programs/projects may not require elaborate security education and awareness plans because of their limited size or duration.

**10. Transportation Plan for the Movement of Classified Material as Freight.** When international programs involve the use of commercial carriers and freight forwarders to move classified material between participants, comprehensive transportation plans are required. Work on the transportation plan should be initiated early in the security planning process. Transportation plans must be approved by the National Security Authorities/Designated Security Authorities of the involved countries prior to implementation. A discussion of the transportation plan is in Chapter 6, above and Appendix S. If several shipments are necessary under the same program, details of each shipment will be provided in a Notice of Classified Consignment.

**11. Control of Security Cleared Facilities.** When a program or project involves the exchange of classified information, a record should be maintained of all facilities among which classified information is exchanged. It facilitates the implementation of security arrangements, such as visits, handcarriage and transportation. Appendix T provides instructions to the responsible Program/Project Office (RPO) on how to compile, distribute and amend the list of contractors and sub-contractors to whom classified information/material will be distributed.

**12. Facility Security Clearance Information Sheet.** Appendix U provides a sample format to be used for the quick exchange of information between National Security Authorities/Designated Security Authorities with regard to the facility security clearance of a facility involved or to be involved in classified tenders, conferences, contracts or subcontracts.

**13. Protection of Information Handled in IT and Communication Systems.** Appendix V provides a suggested format for preparing standard operating procedures when Information Technology (IT) and Communication Systems are to be used within a program. It describes the responsibilities and procedures for the protection of classified information that is processed on automated data processing systems and/or networks, and describes the elements of information that should be included in each section.

**14. Contract Security Clauses.** These clauses (Appendix W) were developed in order to standardize security clauses used in multinational and bilateral international contracts. They are provided primarily for guidance.

**15. International Transportation by Commercial Carriers of Classified Documents and Equipment or Components as Freight.** Appendix X establishes minimum security requirements for the international transportation by commercial carriers of classified consignments as freight. The procedures and requirements described may be supplemented when more stringent security requirements are established by National or Designated Security Authorities of the governments of the commercial carriers.

**16. Guidelines for Assessing Protection and Control of Classified Information in a Multinational Non-NATO Cooperative Defense Program.** These guidelines (Appendix Y) are intended to assist government industrial security specialists (national inspectors) in the assessment of security measures that must be in place at contractor facilities to safeguard classified information.

**17. International Handcarriage of Classified Documents, Equipment, and/or Components by Visitors.** These arrangements (Appendix Z) expand the scope of MISWG Document 1 (Appendix K) to permit visitors dispatched for other purposes, that is, on a visit outside of the international program, on loan, or attending a conference, to handcarry classified material in support of an international program pursuant to the terms of the program agreement and PSI.

**18. International Industrial Security Requirements Guidance Annex.** Appendix AA provides guidance for participating governments to provide their contractors with the security requirements and classification guidance required for the performance of classified contracts related to international programs with respect to pre-contractual negotiations, tenders, contracts, and subcontracts. DoD will use the DD Form 254, "Contract Security Classification Specification," for this purpose.

**19. Personal Security Clearance Information Sheet.** Appendix BB provides the standard format for confirmation of a personnel security clearance. It does not constitute a personnel security clearance certificate and is for information purposes only.

**20. International Transfer of Material Classified RESTRICTED by Express Commercial Couriers.** Appendix CC describes eligibility and security requirements for the urgent international transfer of RESTRICTED material by express commercial carriers. This document was found to be unworkable, and is scheduled for cancellation.

**21. Role of the Facility Security Officer.** Appendix DD is the result of a survey of the industrial security practices of more than 30 nations and reflects the best practices of those nations as to the functions, and qualifications of a Facility Security Officer (FSO). Unlike the earlier MISWG documents it is advisory only and intended as guidance to those nations which are just beginning to have international programs.