# APPENDIX DD

# ROLE OF THE FACILITY SECURITY OFFICER

## MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP

**MISWG Document Number 21** **11 September 2003**

### ROLE OF THE FACILITY SECURITY OFFICER

### Introduction

Documents approved by the MISWG for use in bilateral- and/or multilateral classified programs require the appointment of a facility security officer (FSO) to exercise the national protective security requirements for classified information. Whilst the protection of classified information is a responsibility of each employee in the facility, the role of the FSO is the most critical. The FSO has an over all individual responsibility for protecting classified information, a contractual obligation to ensure the effective implementation of security requirements and procedures within a facility involved in classified projects. His actions are vital to provide the overall efficiency of the security system on behalf of facility management and indirectly of the government. The duties and responsibilities of the FSO are organized, met and controlled by national laws and regulations.

This document can not be in any way binding on the nations but involves all important criteria, rules and obligations concerning FSO's, and provides guidance on the requirements for appointment, objectives and requirements for FSO's which may be used by all MISWG countries in their future industrial security activity in this field.

### 1. General

1.1 The FSO should be a part of the facility's management, or directly is to be subordinated to one member of the management. All decisions have to be concerned to security interdependence. For this reason the FSO is the technical advisor to the management on security matters. He is responsible for the proper implementation of security related decisions, for co-ordination of available security resources and measures. His duty is to co-operate efficiently first of all with NSA/DSA and, where appropriate, with the local security services and forces.

1.2 The FSO should draft and maintain an up-to-date version of the security implementation standards and procedures within the facility. He should be the focal point for all security-related aspects of international classified programs, involving review import/export approval requests, foreign contract activity, government-to-government transfers and liaison with various authorities and other involved facilities.

## 2. Criteria

2.1 The FSO can only be a citizen/national of the country where the facility is located. He has to be vetted at the appropriate level as a part of the facility security clearance. The FSO must be an adult. He should be of a sufficient senior rank or should report to a senior member of management in order to exercise security authority. The FSO should be provided with appropriate training.

2.2 The FSO should have at least secondary school education. Knowledge of English is not a requirement for the FSO's position, but in the future, it is advisable. This criteria does not apply to countries whose official language is English.

2.3 The management of the facility nominates the FSO but the appointment has to be approved by the NSA/DSA.

2.4 The FSO's position should be a full time activity, but in the small companies it is acceptable for the FSO position a  to be a part time activity.

2.5 The FSO must be an employee of the given facilities organization.

## 3. COOPERATION BETWEEN THE FSO AND THE NSA/DSA

3.1 The NSA/DSA maintains close co-operation with FSO's through all available means. The FSO's suitability is confirmed by close working relationship, interviews, vetting procedures and training.

3.2 The FSO will report any changes of the ownership, operating name and location of the organization.

3.3 The FSO will report any changes to the information previously submitted for key management personnel, including the names of the individuals they are replacing, in addition a statement will be made indicating, whether the new key management personnel are cleared and if so, to what level. Individuals who have not been vetted will be excluded from access.

3.4 The FSO must report any important changes to physical, document security and to INFOSEC.

3.5 The FSO will report the details of any security risks concerning classified information as soon as possible after they are discovered.

3.6 The FSO must report any possible espionage, sabotage or subversive activities at any of the facility's locations in written form to the NSA/DSA.

3.7 The FSO will direct and co-ordinate the work of his deputy (if applicable), and other security personnel.

3.8 The FSO will report efforts of individual's (regardless of the nationality) to obtain unauthorized access to classified information or to compromise a vetted employee.

3.9 The FSO will seek prior authority from the NSA/DSA for any contractual or any other type of agreement with any foreign interest that involves the release or access to national classified information by foreign organizations or citizens/nationals.

3.10 The FSO is required to report any events that may have an impact on the status of the FSC, PSCs, including any indications of loss, compromise or suspected compromise of classified information.

3.11 The FSO sends the NSA/DSA a registration list about the vetted personnel and annotates it with any corrections. (Organizations in the ISP are not required to do this)

3.12 The FSO will co-operate in routine and unannounced security inspections and investigations involving the protection of classified information and during personnel security investigations of current or former employees and others.

3.13 The FSO will initiate a preliminary inquiry to ascertain all of the circumstances into any security violation, and will submit an initial investigation report of the incident to the NSA/DSA. When the investigation has been completed, a final report will be submitted by the FSO to the NSA/DSA.

3.14 Where necessary this requirement should also apply to foreign governments RESTRICTED information.

3.15 The FSO will report any adverse information coming to her/his attention concerning any of the facility's cleared employees to the management and to the NSA/DSA.

3.16 The FSO will report about the administrative actions taken against the individual having access to classified information and other employees, if they are involved in a deliberate disregard of security requirements or gross negligence on the handling of classified material.

3.17 The FSO will develop procedures for safeguarding classified material in emergency situations, and will report any emergency situation to the NSA/DSA which renders the facility incapable of safeguarding the classified material.

3.18 The FSO will periodically attend security seminars offered by the NSA/DSA.

## 4. COOPERATION BETWEEN THE FSO AND THE MANAGEMENT

4.1. The FSO is the technical advisor to management regarding security-related issues. The FSO's duties and responsibilities which relate to national security regulations should be set out in a job description which is to be approved by the head of management.

Additionally a Security Manual must be issued on company level ensuring the effective implementation of national industrial security regulations.

4.2. The FSO should maintain continuous contact with the people in charge of the different administrative and operational areas of the facility.

4.3. The FSO will identify changes of national industrial security regulations and, where appropriate, will inform the management about the changes.

4.4. The FSO will, where required, draft and implement the annual facility inspection plan based on security issues. Having implemented the plan, the FSO will submit the results in the annual report to the management.

4.5. The FSO will record information about employees who violate security requirements. The FSO in consultation with management will establish and apply a graduated scale of actions against the employees' violations, or negligence.

## 5. PERSONNEL SECURITY

5.1. The FSO will develop and implement the procedures necessary to obtain the personnel security clearance of those persons in the organization who require access to classified information.

5.2. The FSO will initiate a new vetting action for new employees who require access to classified information and for existing employees, before the end of the validity of a PSC.

5.3. The FSO provides during the vetting procedure suitable arrangements within the facility for conducting private interviews with employees and provides relevant employment and security records for review, when requested.

5.4. The FSO prepares an access list of vetted persons and updates it on a regular basis or when changes occur.

5.5. The FSO continuously monitors the security profile status of individuals within the organization and will report any changes and circumstances which may adversely affect the individual's loyalty, reliability and trustworthiness.

5.6. The FSO will report any abnormal or suspicious activities that may affect the security of classified information.

5.7. The FSO will ensure that individuals having access to classified information sign a "responsibility declaration".

5.8. The FSO develops and provides security briefings to new employees and to cleared persons before they are given access to classified information.

5.9. The FSO conducts exit interviews with individuals who are terminating employment with the organization and debriefs the individuals on their continuing responsibilities. The FSO will arrange to terminate the security clearances of personnel who no longer require access.

5.10. The FSO will develop and distribute identity cards as well as access cards, whenever required.

5.11. The FSO deals with procedures for international and national travel requests for the organization's personnel involving the handling of classified information.

5.12. The FSO will prepare procedures for handling classified visits to the facility by national or foreign persons.

5.13. The FSO will ensure that only personnel security cleared to the appropriate level and with a "need-to-know" have access to classified information and assets.

## 6. PHYSICAL SECURITY

6.1. Regular maintenance of security systems is necessary to ensure that the equipment operates at optimum performance. It is necessary to re-evaluate the effectiveness of individual security measures and the complete security system periodically.

6.1. FSO's must develop measures for the protection of facilities containing classified information against espionage, terrorism, public disorders, sabotage, bombs, explosive devices and theft. Fire protection procedures must be implemented by the FSO.

6.2. The FSO will develop emergency evacuation plans for personnel and for classified information.

6.2. The FSO should define the boundaries for security areas, as well as the security measures for each of the areas. The FSO shall co-ordinate the security aspects of all construction at the facility.

6.3. The FSO develops procedures for the efficient control of all copies, translations and quotations of classified information, providing for the registration, numbering via the head of the registry. The FSO should also record the receipt, distribution, origination, and transmittal of classified information.

6.4. The FSO develops procedures for the normal and emergency destruction of classified documents and provides suitable means for the purpose.

6.5. The FSO must plan and supervise the work of the security guards, when required..

6.6. The FSO is responsible for protection of combinations to security containers, cabinets, vaults and closed areas.

6.7. Combinations will be changed by the FSO when personnel having knowledge of the combinations terminate employment or transfer to a position where knowledge of the combination is not required or if the combination is suspected or known to have been compromised.

6.8. The personal identification numbers (PIN) and passwords must be changed when it is considered necessary.

6.9. The FSO will check alarm systems periodically and will provide for adequate maintenance of the system.

6.10. The FSO should conduct random checks within the facility during working hours and after working hours in order to verify that no classified material has been left unsecured.

6.11. The FSO must implement procedures for cleaning and maintenance operations in the secure areas of the facility, and must provide, as a minimum, an annual inventory of classified information and assets.

## 7. INFORMATION SECURITY (INFOSEC)

INFOSEC is the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. INFOSEC involves security risk management, security approval, security-related documentation, security inspection, computer and local area network security, interconnection of network security, cryptographic security, transmission security and emission security.

7.1. Automated Access Control Systems and electronic, mechanical, or electromechanical devices may be used provided they have been approved/accredited by NSA/DSA and controlled by the FSO.

7.2. The FSO will ensure the confidentiality, integrity and the availability of classified information, which is processed or handled, via information technology systems, networks, and other devices.

7.3. The FSO develops procedures for the registration of all incoming classified information via all information technology systems.

7.4. Computer and networking systems used to capture, create, process and to distribute classified information must be operated to ensure that all information is protected in accordance with its level of sensitivity.

7.5. The ADP security plan should be prepared using the special skills of the computer

specialist, under the supervision of the FSO.

7.6. The management of the facility, the FSO, the system security representative (ADP Security Officer) and the NSA/DSA (in case of CONFIDENTIAL and above) are all responsible for the safe operation of all classified systems. Security management mechanisms and procedures must be in place to deter, prevent, detect, and recover from the impact of incidents affecting the confidentiality, integrity and availability of classified information.

7.7. The FSO will develop procedures for the security of ADP systems and for communications security.

7.8. The FSO must control the issue of passwords and other access control devices and should ensure they are changed regularly in accordance with the Threat and Risk Assessment.

7.9. The FSO will brief system users on system security responsibilities.

## 8. PROJECT SECURITY

8.1. FSO's of the prime contractor and the subcontractors should be in direct contact throughout the life of the classified project as stipulated in written agreements. All organizations involved in the classified project must possess an appropriate Facility Security Clearance. The FSO will obtain approval from the NSA/DSA prior to subcontracting contracts having security requirements.

8.2. The FSO ensures that the government contract security clauses are properly included in any subcontracts.

8.3 The Project Security Instruction and Security Classification Guide must be prepared at the appropriate level and approved by the NSA/DSA. The FSO must ensure that all security requirements are adhered to.

8.4. The appropriate requirements of the PSI and Security Classification Guide will apply to subcontractors involved in classified international projects and must be reflected in contractual documentation.

8.5. In the implementation of international classified projects, the security requirements related to security clearances, visit procedures and the transmission of classified material must be in accordance with international agreements, Arrangements or Treaties.

8.6. The FSO will collaborate in the drafting of transportation plans and in the implementation of the plans.

8.7. The FSO will prepare procedures for international and national travel requests for the organization's personnel.

8.8. Classified material will be hand carried and delivered according to the MISWG document N° 1.

8.9. The FSO must ensure that Visit Clearance Requests are prepared and forwarded in accordance with MISWG Document No. 7.

8.10. The FSO develops procedures and promotes the proper implementation of security measures for the security of the facilities where meetings, conferences, briefings and other activities are held for the purpose of protecting classified information.

8.11. The FSO maintains records of all visitors, including their names, the organization's they represent, the dates of the visits and the names of the person's who were visited.

8.12. The FSO ensures that visitors have approval for access to classified information based on "need-to-know" principle and that their movement is controlled as needed.

8.13. Where permitted by national security rules, and regulations, RESTRICTED level visits may be arranged directly between the FSO of the visitor and the FSO of the facility to be visited.

8.14. The FSO must inspect all secure facilities or areas that the facility will no longer use to ensure that no classified material is left there after the area has been vacated.

8.15. The FSO when required, review news, articles, advertisements and public notifications that may refer to classified programmes in order to ensure that classified information is not disclosed.

8.16. The FSO will inform the NSA/DSA prior to any physical move or new construction which could affect the protection of classified information and assets.

8.17. The FSO will plan and co-ordinate the security of assets during relocations.

## 9. SECURITY AWARENESS

9.1. The FSO is responsible for taking part in security training deemed appropriate by the NSA/DSA.

9.2. The FSO may obtain protective security, threat awareness, other education and training information from their NSA/DSA.

9.3. The FSO provides security training for the facility's personnel at least once a year and more frequently if required.

9.4. The FSO will provide initial security briefings to employees about threat awareness, protective security, classification systems, reporting obligations, security procedures and

other security requirements prior to granting employees' access to classified information.

9.5. The FSO will debrief vetted employees when their PSC's are terminated, suspended or revoked and upon termination of the FSC.