MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP

MISWG Document Number 24 **09 September 2010**

SYNOPSIS
of an
INDUSTRIAL SECURITY MANUAL

PART I: Foreword

PART II: Table of Contents

PART III: References (to nation-specific legal background)

PART IV: Acronyms

PART V: List of possible annexes

PART I: FOREWORD

PART II: TABLE OF CONTENTS

PART II.

CHAPTER 1: GENERAL PROVISIONS AND REQUIREMENTS

1.1. INTRODUCTION

- This manual is issued in accordance with the national laws and regulations;
- It prescribes the requirements, restrictions, and other safeguards to protect classified information and to prevent unauthorized disclosure of classified information with regards to participation of companies in classified projects;

1.2. THE PARTICIPATING AUTHORITIES AND THEIR INDUSSEC RELATED OBLIGATIONS

- NSA;
- DSA;
- any other competent authorities/services;

1.3. GENERAL REQUIREMENTS

- Basic security principles (e.g. „need-to-know", requirement of FSC, PSCs, FSO, handling of classified information according to classification level);
- Definition of classified information;
- Security reviews;
- Security training and briefing (Establishment of such internal position, that cleared employees are aware of their responsibilities)

1.4. REPORTING REQUIREMENTS

- Contractors are required to report events that might have an impact on the status of the FSC, PSCs, and proper safeguarding of classified information, such as: suspicious contacts, probable or possible espionage, sabotage, terrorism, or subversive activities;
- If applicable: international classified contracts;

- Any change in ownership, operating name, address, financial background, storage capability, inability to safeguard classified material, security equipment vulnerabilities);
- Reports of loss, compromise, or suspected compromise of classified information (preliminary inquiry, initial report, final report, individual culpability reports)
- Change in vetted employees' status;
- Unauthorized handling of classified information by any employee;
- Changes in security arrangements.

CHAPTER 2: INDUSTRIAL SECURITY PROCEDURES

2.1. GENERAL RULES OF INDUSEC PROCEDURES

- The contractor will not be granted access to classified information until the FSC has been granted;
- An FSC is valid for access to classified information at the same or lower classification level, as the FSC granted;
- FSC will be registered by the NSA/DSA;
- FSCs are required for sub-contractors, if applicable;
- PSCs are required in connection with the FSC.

2.2. PRECONDITIONS FOR GRANTING FSC (OPTIONAL)

- *Valid certificates of national and/or international standards (i.e.:ISO, AQAP);*
- *Positive evaluation of the financial balance;*
- *Minimum 3-year-long business activity;*
- *The company must not be under FOCI;*
- *Official invitation to a bid to a classified contract.*

2.3. REQUIREMENTS FOR ISSUING FSC

- Vetting of company as a legal entity – no security risk;
- Vetting of company employees required to have access to classified information – no security risk;
- Appointment of FSO;
- Capability to protect classified information

Optional:

- *Establishment of administrative and security areas, sub-registry on company site; various security measures for personnel, physical, document administration and IT security;*
- *Issuance of a Company Security Instruction.*

2.4. CONTENT OF INDUSEC VETTING PROCEDURE

Required documentation from the facilities:

- Written request for vetting of the applicant (written Sponsorship Letter);
- Personnel Security Questionnaires;
- A proof of the ownership structure of the company;
- Legal background: facility is registered with the competent court;

Optional:

- *FSQ of legal entity* ;
- *Certificate, that the facility has no criminal records;*
- *Certificate issued by the Tax Office;*
- *Declaration about facility's balanced financial position*;
- *Copies of licenses and certificates giving the right for performing activities on the classified contract;*
- *A copy of the tender which involves classified information;*
- *Relevant security documentation of company;*

2.5 Possible grounds for DENIAL, SUSPENSION OR REVOCATION OF FSC

- Verified security risk (e.g. adverse security checks, FOCI, loss or compromise of classified information, breach of security);
- No FSO;
- Verified economical instability of the company;
- Upon the request of the company.

Optional:

- *The contractor did not apply for any new classified contract during … consecutive years.*

- *If the withdrawal has taken place, the facility shall not be granted a new FSC until such time specified by national rules;*

2.6 APPEAL PROCEDURE AT DENIAL OF FSC (OPTIONAL):

Any appeal procedures are specified by national laws and regulations.

2.7 POST-FSC REQUIREMENTS

- Regular facility visits by NSA/DSA;
- Return of classified information furnished and/or generated after completion of classified project;
- Acknowledgement of secrecy even after the PSC has been terminated.
- Supervising the implementation of contract with sub-contractors involving access to classified information by all competent authorities, FSOs;
- Supervising the signing of a new contract involving access to classified information;
- Request of additional security vetting, when necessary.

Optional:

- *Periodical check of the validity of ISO and/or AQAP;*
- *Annual written report to the NSA/DSA about the changes of most important data of facilities (e.g. annual financial report);*

CHAPTER 3: FACILITY SECURITY OFFICER (FSO)

3.1. CRITERIA OF THE FSO

- FSO has to be vetted at least at the level of the FSC;
- FSO is recommended and appointed by the management, based on the agreement with the NSA/DSA;
- National citizen;
- Professional training provided by NSA/DSA;
- FSOs are required to be placed in a sufficiently high position to be able to influence the management regarding the protection of classified information;
- Professional knowledge of the security rules;
- Close co-operation with the NSA/DSA;

  Optional:

  - *Full time employment with the company granted FSC;*
  - *A signed agreement between the NSA/DSA and the facility.*

3.2. FSO'S GENERAL DUTIES IN THE SECURITY SYSTEM OF THE COMPANY

As spelled out in MISWG Document No. 21.

CHAPTER 4: PERSONNEL SECURITY

4.1 GENERAL PROVISIONS

- Providing conditions for requesting PSCs;
- Maintaining PSQ forms;
- Initiating personnel security vetting procedures (limited to the minimum to meet contractual requirements);
- Issuing/withdrawing PSCs by NSA/DSA;
- Establishing and maintaining Security Awareness Program

  - Security trainings;
  - Travel briefings/debriefings;
- Reviewing PSCs in accordance with national laws and regulations;
- Permission and need-to-know for access to classified information;
- Imposing access restrictions;
- Maintaining and segregation of appropriate security records;

4.2 SUBJECTS OF PERSONNEL SECURITY VETTING

- All personnel, having access to classified information, including as appropriate:
- Owners
- Members of Management Board;
- Members of Supervisory Board;
- FSO;
- Staff of sub-registry;
- INFOSEC staff;
- Courier who is involved in the delivery of official documents;

CHAPTER 5: PHYSICAL SECURITY

- Supervising the physical security arrangements in Administrative and Security Areas, including:
- Implementing and monitoring all security measures or criteria that may be required,
- Overseeing of the company's security systems (perimeters, lighting, securing of walls, ceilings, doors, gates, windows, ventilation ducts etc.);
- Monitoring of security guards, intrusion detection systems, badge system, entry and exit control, vehicles;

- Ensuring protection and changing of combinations to security containers, cabinets, vaults, etc.;
- Establishing emergency procedures (e.g.: securing or removal of classified information, co-operation with police, fire-department);

CHAPTER 6: ADMINISTRATIVE SECURITY

General principles, including:

- Classification markings;
- Preparation and receipting;
- Reproduction, destruction of classified information;
- Transmission of classified information (documents) within facility.
- Transmission classified information (document) outside facility;
- Classification downgrading;
- Packaging;
- Discussion of classified information at conferences, meetings;
- Presentations;
- Disclosure of classified information;
- List of personnel granted with access to classified information

CHAPTER 7: INFORMATION SYSTEM SECURITY

Approving/accrediting of systems handling classified information, including:

- Specific INFOSEC responsibilities;
- Communications security;
- Security of cryptographic products;

- TEMPEST requirements;
- Security of computer storage media;

CHAPTER 8: PROJECT SECURITY

SECURITY OF CLASSIFIED CONTRACTS

- Definition and purpose;
- Prime- and subcontractors;
- Co-operation with NSA/DSA;
- Co-operation with subcontractors;
- PSI or SAL and Security Classification Guide;
- Classified transportation;
- RFV procedures;
- Courier procedures.

CHAPTER 9: TRANSPORTATION OF CLASSIFIED INFORMATION

9.1 DOMESTIC TRANSPORTATION OF CLASSIFIED INFORMATION

- Transportation plan;
- Shipping documents;
- Government agency arrangements;

- Commercial arrangements;
- Packaging;
- Hand-carrying classified material;
- Classified material receipts;
- Transportation by road, rail, sea, and aircraft.

9.2 INTERNATIONAL TRANSPORTATION OF CLASSIFIED INFORMATION

- Transportation plan;
- Shipping documents;
- Government agency arrangements;
- Commercial arrangements;
- Packaging, customs,
- Hand-carrying classified material;
- Classified material receipts;
- Transportation by road, rail, sea, and aircraft.

CHAPTER 10: VISIT PROCEDURES

10.1 DOMESTIC VISIT PROCEDURES

- Definition, types and purpose of domestic visits;
- Domestic RFV procedures.
- Government approved visits;
- Request formats;
- Visitor records;

10.2 INTERNATIONAL VISIT PROCEDURES

- Definition, types and purpose of international visits;
- International RFV procedures;
- Government approved visits;
- Request formats;
- Visitor records;

PART III: REFERENCES (to national laws and regulations)

PART IV: ACRONYMS

PART V: LIST OF POSSIBLE ANNEXES

- Personnel Security Questionnaire forms;
- Application form for Personnel Security Clearance;
- Personnel Security Clearance Certificate
- Facility Security Questionnaire form;
- Facility Security Clearance Information Sheet;
- Facility Security Clearance Certificate;
- Project Security Instructions template;
- Security Acknowledgement (for Hand Carriage);
- Courier Certificate;
- Request for Visit form (RfV);
- Processing times for international RfVs;
- International Transportation Plan;
- Notice of Classified Consignment;
- Authorization for Security Guard;
- Appointment of the Facility Security Officer form;
- Instruction sheet on foreign travel.
- Multinational Classification Markings Equivalents;
- Security Area Control Instruction;
- Facility Security Plan template;
- Facility Emergency Plan template.