MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP

MISWG DOCUMENT Number 26

20 December 2013

CYBER SECURITY INCIDENT REPORT FORMAT

1. INTRODUCTION

1.1 This document provides a format for reporting cyber security incidents at contractor entities, when there is a national reporting requirement to do so.

2. SCOPE

2.1 The attached Cyber Security Incident Report format has been approved by the MISWG participants for reporting cyber security incidents at contractor entities. This form may also be used to document and triage INFOSEC and other related incidents.

2.2 The aim of this cyber security incident report is to be used by the security or other appropriate officers of industrial facilities to immediately document and report loss/compromise, suspected compromise, suspicious contact, or activity involving systems accredited to process classified information. It may be used as a preliminary response to supplement national reporting requirements and provide a resource to document initial or first response to a cyber security incident.

2.3 The responsibility solely rests on national security authorities to adopt or not a form to report cyber security incidents. The classification of the completed form depends on national regulations and therefore is required to be transmitted appropriately depending on the level of classification assigned to the report. The assumption is made that any security incident involving classified information and foreign government information, including assets and information stored, processed or generated, in relation to a contract or capability must be reported immediately to the appropriate national security authorities. In turn, they will collect initial details then advise who else should engage in the inquiry.

ANNEX 1
of Document no. 26

CYBER SECURITY INCIDENT REPORT

1.0 Reported By

1.1 Surname:		1.2 Forenames:	
1.3 Position:			
1.4 Name of organisation or company:			
1.5 Telephone No:			
1.6 E-mail:			

2.0 Organisation Details

2.1 Name of organisation:	
2.2 Type of organisation:	
2.3 Street Address:	
2.4 At this time, is it known that other organisations are affected by this incident? (If so, list names, addresses, telephone number, email addresses and contact persons):	

3.0 Incident Details including Injury and Impact Level

3.1 Date:		3.2 Time:	
3.3 Location of affected site:			
3.4 Brief summary of the incident (what has happened, where did it happen, when did it happen):			
3.5 Description of the project/programme and information involved, and, if applicable, the name of the			

specific program:	
3.6 Classification level of the information involved	
3.7 System compromise (detail):	
3.8 Data compromise (detail):	
3.9 Originator and /or Official Classification Authority of the information involved? (List name, address, telephone no., email and contact person).	
3.10 Is Foreign Government Information involved? Originating country or international organisation?	
3.11 Did the incident occur on an accredited system authorized to process and store the information in question?	
3.12 Estimated injury level/sector:	
3.13 Estimated impact level: (any compromise or disruption to service?)	
3.14 Incident duration:	
3.15 Estimated number of systems affected:	
3.16 Percentage of organization systems affected:	
3.17 Action taken:	
3.18 Supporting documents attached (describe if any)	
3.19 Multiple occurrence or first time this type of incident occurs within this location?	

3.20 Incident Status (resolved or unresolved)	
3.21 Has the matter been reported to other authorities? If so, list names, addresses, telephone no., email and contact person.	

4.0 Status of Mitigation Actions

4.1 Mitigation details to date: (List any actions that have been taken to mitigate incident and by whom)	
4.2 Results of mitigation:	
4.3 Additional assistance required?	

5.0 Computer Network Defense Incident Type (if applicable)

5.1 Malicious code: (Worm, virus, trojan, backdoor, rootkit, etc.)	
5.2 Known vulnerability exploit: (List the Common Vulnerabilities and Exposures (CVE) number for known vulnerability)	
5.3 Disruption of service:	
5.4 Access violation: (Unauthorized access attempt, successful unauthorized access, password cracking, Etc.)	
5.5 Accident or error: (Equipment failure, operator error, user error, natural or accidental causes)	
5.6 If the incident resulted from user error or	

malfeasance, identify reasons (training, disregard for policy, other) and responsible parties.				
5.7 Additional details:				
5.8. Apparent Origin of Incident or Attack	Source IP and port:		Protocol:	
	URL:		Malware:	
	Additional details:			

6.0 Systems Affected

6.1 Network zone affected: (Internet, administration, internal, etc.)	
6.2 Type of system affected: (File server, Web server, mail server, database, workstation (mobile or desktop), etc.)	
6.3 Operating system (specify version):	
6.4 Protocols or services:	
6.5 Application (specify version):	

7.0 Follow-on Activities

7.1 Has information contained in this report been provided to the authorities? When?	
7.2 Next steps as discussed by the security authorities (document here in the event that management or chain of command has not yet been informed of the incident, or that a status report is required).	