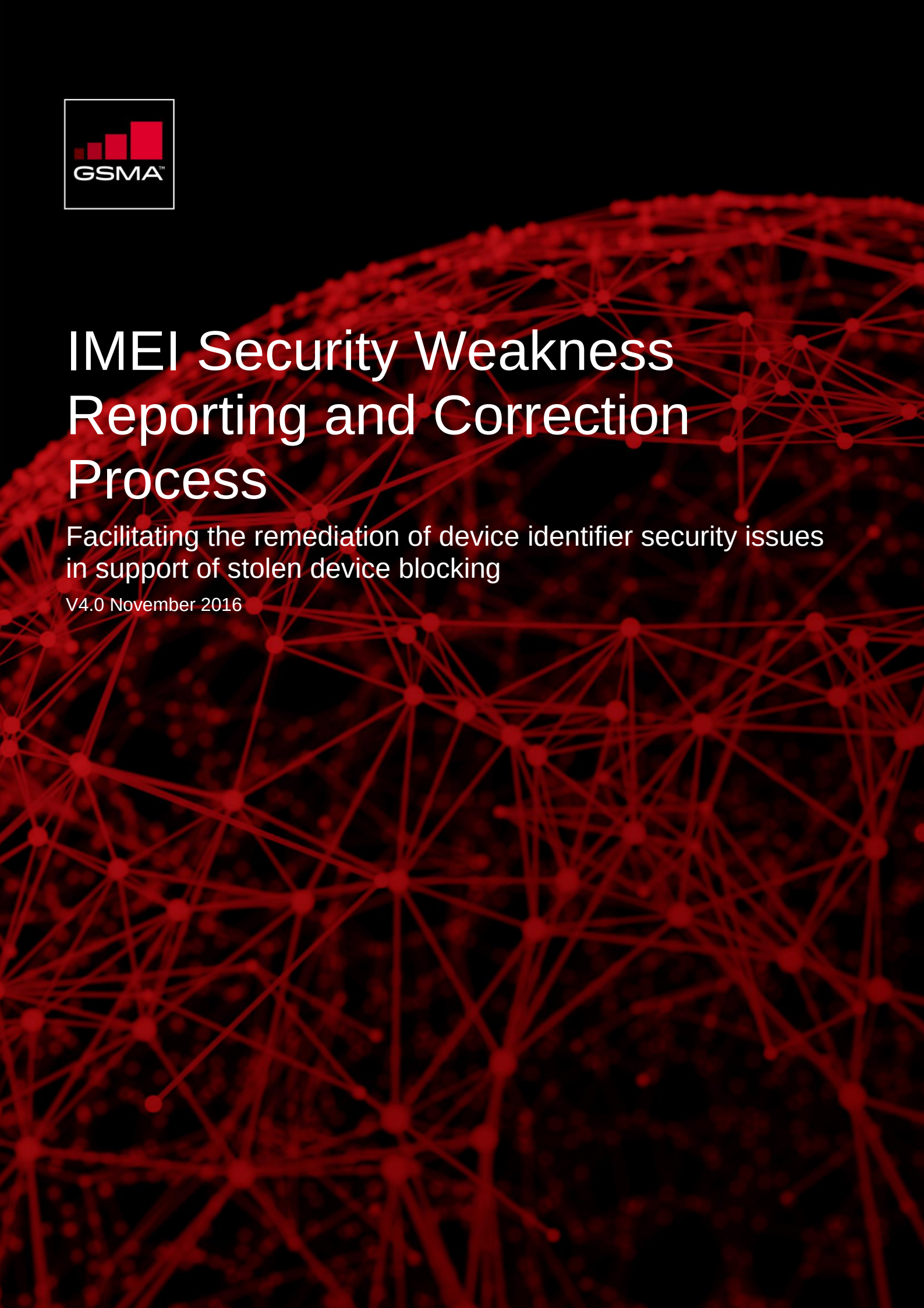

IMEI Security Weakness Reporting and Correction Process

Facilitating the remediation of device identifier security issues in support of stolen device blocking

V4.0 November 2016

Table of Contents

1. Introduction

The IMEI was originally introduced, as a unique terminal identity, for type approval reasons, in order that non-type approved terminals could be prevented from connecting to GSM networks. Subsequently, IMEIs of stolen terminals were used to stop them from working on some networks.

Despite the need for mobile devices to have unique identities, in practice, IMEIs have been tampered with. The GSM specifications were changed in Nov 1999 to provide that, with effect from June 2002, IMEIs should not be capable of being changed outside the control of the original manufacturer of the terminal.

2. IMEI Security Weakness Detection and Correction Process

It is acknowledged that security is not absolute and GSMA and the world's leading device manufacturers agreed to establish a formal process to centralise the reporting of newly identified IMEI security weaknesses. The overall objective of this initiative is to improve device security levels during the remaining manufacturing life cycle of the product.

GSMA envisaged that an improved communication process would greatly enhance the exchange of intelligence and accelerate co-operation between the manufacturer and network operator communities.

The reporting process outlined in this document, (the Process), recognises the need to facilitate the reporting and correction of product security weaknesses. The process engages with manufacturers centrally rather than locally to ensure there is increased awareness and visibility of any problems that may arise.

The reporting process relates to existing and future devices over their product lifetime. It addresses the security compromise of IMEIs in mobile devices, which means cases in which the IMEI signaled to the network is not that which was set by the manufacturer during device production. The process consists of the following steps, which are also represented in the diagram below;

1. Once a stakeholder (notifying party) detects compromised IMEIs in a specific mobile device model, it notifies GSMA. All parties, including the notifying party, hold the information in confidence and acknowledge that information notified in this manner is commercially sensitive to the manufacturers. As a result, notifying parties commit to communicate this information responsibly within their organisations, restricting distribution to those with a need to know and respecting commercial confidentiality.

2. The report is assessed by GSMA and the weight of evidence and the feasibility of the breach on a commercially significant scale is considered to avoid referring spurious claims to manufacturers.

3. Where deemed appropriate, GSMA formally addresses a notice to a single point of contact, previously advised to GSMA by the relevant manufacturer for this process. The report shall include all available information, evidence, tools or software available to the notifying party, or its agent, required to support the alleged breach. Where none of this information is available a hacked device, (to be replaced), will be provided to the manufacturer, at the same time as the report is initiated, to enable the necessary investigation and analysis to be conducted. It is recognised that in the latter case the 42 days time period referred to in clause 4 below shall not commence until the device is received by the manufacturer's appointed contact, but in any event will commence no later than 10 working days from the date the initial report was furnished to the relevant manufacturer.

4. In the event that the notifying party is unable to provide any physical evidence of IMEI compromise it may refer reports based on symptomatic evidence to GSMA. Such evidence will generally be based on observations of multiple instances of the same IMEIs in use by different subscribers. These cases will be reported to the relevant manufacturers for information and intelligence purposes only and a detailed investigation or analysis is not

required on the part of the manufacturer. However, should the manufacturer have information available regarding the vulnerability and/or any associated remedial action it may submit this to GSMA. It is also recognised that devices with a duplicate IMEI may not be of the model or manufacturer to which the original IMEI was allocated.

5. The manufacturer assesses the validity of the alleged breach and responds to GSMA within 42 calendar days to acknowledge receipt of the report, propose remedial action to be taken, and provide estimated dates that an improved IMEI implementation will be available. The manufacturer also advises of any other of its device models, utilising the same IMEI implementation that may be affected by the alleged hack, if proven.

6. For economic reasons, device manufacturers are not obliged to undertake remedial action or to propose technical solutions where production of the compromised device has already ceased or is due to cease within a period which is reasonable considering the nature of the fix required.

   It is acknowledged that a manufacturer may initially inform GSMA that production of a particular model or platform is due to cease but at a later stage a decision may be made to extend the production life of that model. In such cases, the manufacturer should proactively inform GSMA and if the revised production life extends beyond the three (3) month 'reasonable period' the original report will be re-opened and treated in accordance with the agreed Process.

7. Where it is agreed by the manufacturer and GSMA that no remedial action is required due to a non-proven breach GSMA will advise the notifying party that no further action will be taken and the report will be rescinded.

8. In the event of there being evidence of a breach, the manufacturer response is sent by GSMA to the notifying party and also notified to GSMA operator members to avoid the generation and submission of duplicate reports pertaining to the same device model. The response information shall be limited to the information necessary to identify the manufacturer's software or hardware upgrade or additional information agreed between GSMA and the manufacturer.

9. The efficacy of remedial technical measures proposed by device manufacturers is critical to the success of the industry initiative. At its discretion, GSMA may request an appointed agent to evaluate the fixed device once the manufacturer has implemented the countermeasures. In the event that a solution put forward to correct an acknowledged breach is compromised the original report should be re-opened until it is properly remedied in accordance with the agreed Process.

10. In the event that the manufacturer fails to respond within the 42 days, or fails to take the stated remedial action, GSMA will inform its operator members of the product compromise.

Once informed of the compromise, network operators may take action, proportionate to the breach but in the event that a satisfactory solution is put forward by the manufacturer the notification will be withdrawn.

Statistics available from this reporting scheme may be made available periodically to third parties as deemed appropriate and necessary by GSMA. Such information to be held in confidence by third parties.

GSMA agrees to continue to review the reporting process to measure its success and to propose any enhancements that may be deemed appropriate and mutually beneficial. Changes proposed by any Ad-Hoc or Working Group are only valid when approved by GSMA’s Device Security Group.

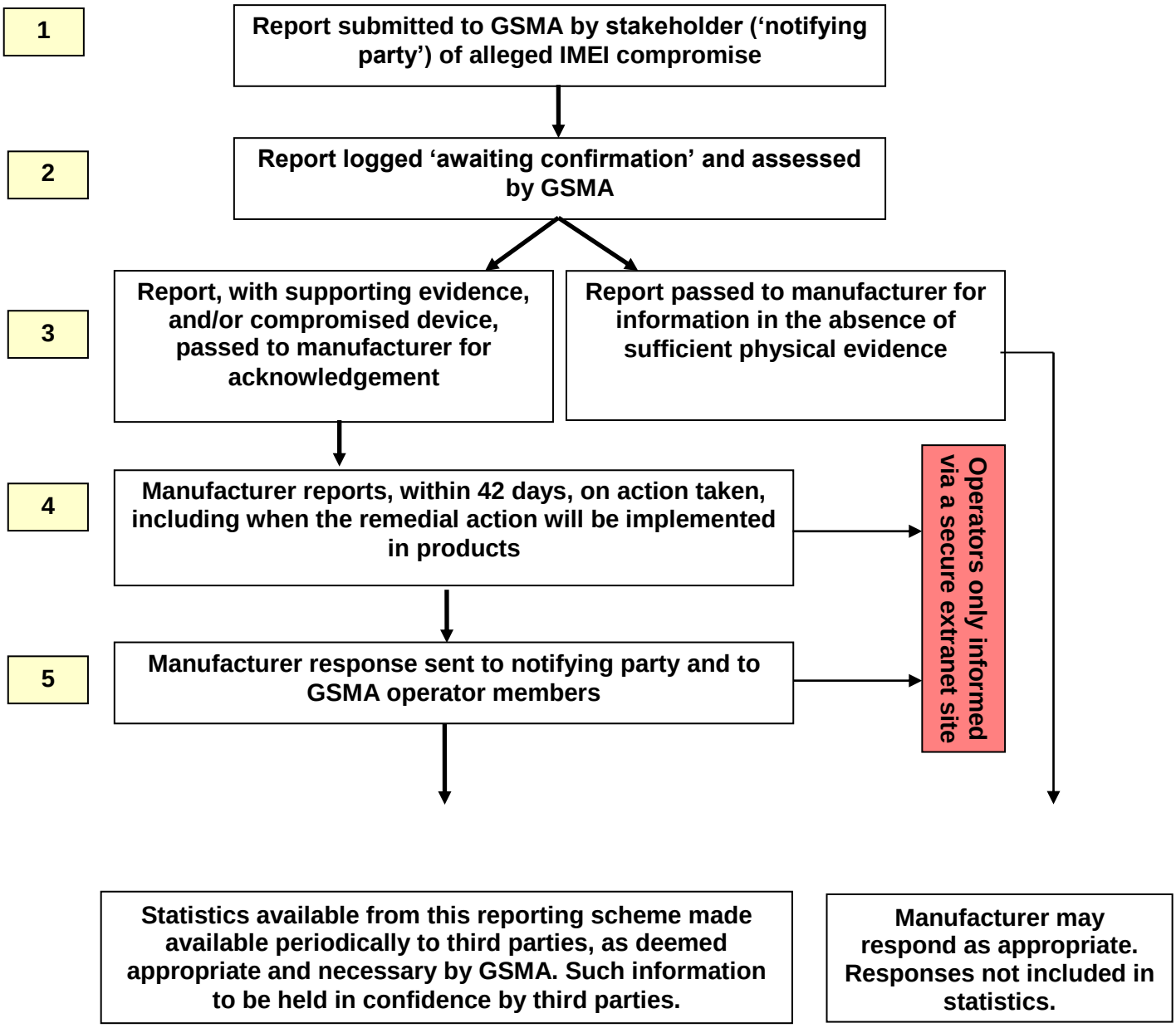

Fig 1. Pictorial representation of IMEI Security Weakness Reporting and Correction Process

Annex 1 – Declaration of Participation

The undersigned have agreed to participate in the scheme outlined in the attached document “IMEI Security Weakness Reporting and Correction Process” as may be amended from time to time upon agreement of GSMA and its members and manufacturers agreeing to sign this declaration. The current version of the document is referenced in GSMA as IMEI Security Weakness and Correction Process 4.0.

The undersigned agrees to enter into a Non-Disclosure Agreement substantially, but not exclusively, based upon the NDA Template with the GSM Association for the express purpose of the captioned scheme. However, for the avoidance of doubt nothing in the agreed Non-Disclosure Agreement shall conflict with the “IMEI Weakness Reporting and Correction Process”. It is understood that this Declaration of Participation has no legally binding effect and that any legal obligations arising are subject to other contractual arrangements that may exist.

Agreed by

Company name:

Address:

Signed:

Name:

Position:

Date:

And acknowledged by

GSM Association

with an office at 2nd Floor, The Walbrook Building, 25 Walbrook, London EC4N 8AF, United Kingdom (hereinafter referred to as "GSMA").

Signed:

Name:

Position:

Date:

Annex 2 – Non-disclosure Agreement Template

An NDA will be entered into as part of this reporting process but shall be subject to negotiations between GSMA and the manufacturer with regards to the details.

The following is a template for use by the parties and does not form part of this agreement. This template is subject to change following further discussions between manufacturers' legal representatives and GSMA Legal.

MUTUAL NON DISCLOSURE AGREEMENT DATED {} (THE "COMMENCEMENT DATE")

PARTIES

1. [***Please insert company name, registered office and company number]*** and

2. **GSM Association** with an office at 2nd Floor, The Walbrook, 25 Walbrook, London EC4N 8AF, United Kingdom (hereinafter referred to as "**GSMA**").

IN CONSIDERATION of the premises and mutual covenants and obligations contained herein **IT IS HEREBY AGREED** as follows:

1. For the purposes of this Agreement:-

   a) "Confidential Information" shall mean all information of the disclosing party, whether commercial, financial, technical or otherwise, disclosed to the recipient in connection with the Business Purpose specified in the Schedule hereto ("the Business Purpose") (whether disclosed orally, in documentary form, by demonstration or otherwise) which is contained in any form whatsoever (including without limitation data, drawings, films, documents and computer readable media) and which is marked or otherwise designated to show expressly or by necessary implication that it is by its nature deemed confidential or proprietary to the disclosing party
   b) "Disclosing Party" means the party furnishing Confidential Information.
   c) "Recipient" means the party receiving the Confidential Information in the particular case.
   d) "Final Report" means the report prepared by ***[insert company name]*** to address the issues raised by the Initial Confidential Information.
   e) "Initial Confidential Information" means the Confidential Information received by the GSMA from the Original Disclosing Party.
   f) "Original Disclosing Party" means any operator member or appointed agent of the GSMA that forwarded the Initial Confidential Information to the GSMA.

2. In connection with the Business Purpose it will be necessary for each party, to disclose to the other party Confidential Information of the Disclosing Party, which may be communicated orally, or in document form, by demonstration or otherwise.

3. Each party undertakes in respect of Confidential Information for which it is the Recipient:-

(a) to treat such Confidential Information disclosed by the Disclosing Party as confidential;
(b) not without the Disclosing Party's prior written consent in each case to communicate or disclose any part of such Confidential Information to any person except:-
    (i) to those employees of the Recipient on a "need to know" basis who are concerned with the Business Purpose;
    (ii) the Recipient's auditors and professional advisers and any other persons or bodies only who have a legal right or duty to have access to or knowledge of the Confidential Information in connection with the business of the Recipient;
    (iii) where the Recipient is ordered by a Court of competent jurisdiction to do so or there is a statutory obligation to do so except that the Recipient shall use all reasonable endeavours to first inform the Disclosing Party in writing before any disclosure under such order or obligation is made;
    (iv) members of the GSMA, and those third parties only who have been expressly authorised in writing by the Disclosing Party to receive the Confidential Information prior to disclosure; and
    (v) to the Original Disclosing Party.
(c) to ensure that all persons and bodies mentioned in paragraph (b) above are made aware, prior to the disclosure of such Confidential Information, of the confidential nature thereof, that they owe a duty of confidence to the Disclosing Party and agree to hold such Confidential Information in confidence in accordance with the terms of this Agreement; and to use all reasonable endeavours, but for the avoidance of doubt, shall exercise no lesser security measures and degree of care of the Confidential Information than that which it applies to its own confidential information and hereby warrants to provide adequate protection against any unauthorised disclosure, copying or use to ensure that such persons and bodies comply with such obligations under this Agreement;
(d) not to use or circulate such Confidential Information within its own organisation except solely to the extent necessary for the purposes of the Business Purpose or any other purpose the Disclosing Party may hereafter expressly authorise in writing before any disclosure whatsoever is made;
(e) For the avoidance of doubt, the named parties entering into this Agreement only are solely responsible for maintaining all the legal obligations in accordance with this Agreement, including, but not limited to those of confidentiality, when disclosing to any named third parties under this Clause 3. The Disclosing Party warrants that it has the authority to disclose the Confidential Information covered by this Agreement.

4. The obligations of confidentiality in Clause 3 above shall not apply:-

(a) to any portion of Confidential Information where the Recipient can demonstrate that the Confidential Information concerned:-
    (i) is or has become publicly known through no fault of the Recipient, its employees, agents and sub-contractors whatsoever; or
    (ii) is lawfully received from an independent third party without any restriction and without any obligation of confidentiality; or
    (iii) is already known to the Recipient with no obligation of confidentiality at the date it was disclosed by or obtained from the Disclosing Party; or
    (iv) is disclosed without restriction by the Disclosing Party to any third party.
(b) to any development made by the Recipient which is independently developed by the Recipient without access to, use or knowledge of the Disclosing Party's Confidential Information.
(c) to the Final Report as prepared by ***[insert company name]***. In the absence of a Final Report, all Confidential Information shall cease to be treated as confidential and may

be treated as information available to GSMA Operator Members forty–two (42) days after disclosure by the GSMA to ***[insert company name]*** of the Initial Confidential Information.

5. All material containing Confidential Information furnished by or obtained from the Disclosing Party, including without limitation, magnetic tapes, documents, manuals, specifications, flowcharts, program listings and data file printouts ("the Materials"), shall be and remain the property of the Disclosing Party and shall not be reproduced in whole or in part without the Disclosing Party's express written consent. Any copies of the Materials shall become the Disclosing Party's property and shall contain such copyright and other proprietary rights notice or legend as appears on the original Materials.

6. Each party may disclose Confidential Information received from the other party to other members of the Recipient's Affiliate and Group Companies for use only in connection with the Business Purpose and each party named in the Agreement shall be solely responsible for observance of the provisions of this Agreement by such other members of its respective Affiliate or Group Companies.

7. Nothing contained in this Agreement shall be construed as granting to or conferring on the Recipient any rights by license or otherwise, expressly or impliedly, for any invention, discovery or improvement made, conceived or acquired prior to or after the date of this Agreement relating to the Confidential Information of the disclosing party.

8. The parties agree that the provision of Confidential Information hereunder and any discussions held in connection with the Business Purpose shall not prevent either party from pursuing similar or other discussions with third parties provided that no breach of this Agreement is so occasioned or oblige that party to take, continue or forego any action relating to the Business Purpose. Any estimates, forecasts or similar material provided by either party to the other shall not constitute any commitments. For the avoidance of doubt, the parties do not intend that any agency or partnership or exclusive relationship be created between them by this Agreement.

9. Upon the completion or termination of the Business Purpose, each Recipient shall promptly deliver up to the disclosing party all Materials supplied by the disclosing party incorporating any Confidential Information of that party and all copies thereof and destroy or erase any Confidential Information contained in any Materials and documentation prepared by or on behalf of the Recipient or recorded in any memory device. Within fourteen (14) days of such request or completion of the Business Purpose the Recipient shall certify in writing to the disclosing party that it has fully complied with its obligations under this Clause. Notwithstanding the foregoing each Recipient may retain one copy of all Materials containing Confidential Information of the Disclosing Party received or made in connection with this Agreement for archival purposes only, subject always to strict compliance with the obligations of Clauses 3 and 5.

10. Neither party shall make or permit others to make any reference to the subject matter of the Agreement or the Confidential Information or use the name of the other party in any public announcements, promotional, marketing or sales materials or efforts without the prior written consent of the other party and such consent shall not be unreasonably withheld or delayed.

11. Nothing contained in this Agreement shall be construed as granting or conferring any intellectual property rights or any other such rights by license or otherwise by either party to the other.

12. The Disclosing Party does not:

    (a) make or give any representation, warranty, undertaking or other statement (express or implied) as to the accuracy or the completeness of the Confidential Information or any other information supplied by the Disclosing Party or as to the reasonableness of any assumptions on which any of the same is based
    (b) accept any duty of care in relation to the provision of such Confidential Information
    (c) accept any liability and hereby excludes any liability for any loss suffered by the Recipient or any other employee, assignee or subcontractor of the Recipient from the use of Confidential Information supplied by the Disclosing Party.
    (d) make or give any representation, warranty, undertaking or other statement (express or implied) that any Confidential Information it may disclose will not infringe any third party intellectual property rights, but agrees to make every reasonable effort to ensure that it will make the Recipient aware where it is itself aware of a third party intellectual property infringement.

13. This Agreement shall become effective as of the date any Confidential Information of a Disclosing Party is first made available to a Recipient Party, or the Commencement Date, whichever is sooner.

14. Except as stated in Clause 6 herein, nothing in this Agreement is intended to confer any benefit on any third party (whether referred to herein by name, class, description or otherwise) or any right to enforce any term of this Agreement.

15. This Agreement shall come into effect on the Commencement Date and shall continue in full force and effect until either party terminates this Agreement in writing with one (1) month's notice to the other party. The requirement and legal obligations of confidentiality of all Confidential Information disclosed under this Agreement shall continue after termination of this Agreement. The termination of this Agreement or the completion of the Business Purpose for any reason shall not affect the obligations set out in this Agreement.

16. This Agreement shall be governed by and construed in accordance with the laws of England and Wales and the parties shall be submit to the non-exclusive jurisdiction of the English Courts.

READ AND AGREED

On behalf of the GSMA		**On behalf of *[insert company name]***	
Signed:	_____	**Signed:**	_____
Print Name:	_____	**Print Name:**	_____
Title:	_____	**Title:**	_____
Date:	_____	**Date:**	_____

SCHEDULE

DESCRIPTION OF BUSINESS PURPOSE

The GSM Association (GSMA) and leading manufacturers including the signatory to the Declaration of Participation forming part of the mutually agreed IMEI Security Weakness and Reporting Process have agreed to establish a formal process to centralise the reporting of identified IMEI security weaknesses when devices, which are in the market, appear to have been compromised. The concept involves an Original Disclosing Party who identifies device security weaknesses reporting the Initial Confidential Information to GSMA, which then refers the report to the relevant device manufacturer. The manufacturer, under the agreed formal process will then investigate the report and will respond to GSMA acknowledging receipt of the report, proposing remedial action to be taken, and providing estimated dates from which equipment with an enhanced IMEI implementation will be available in the Final Report.

Annex 3 – Reporting Template

SUSPECTED IMEI SECURITY WEAKNESS REPORT

Status:

Discovery Date:

Issue Date:

Issue Ref:

Originator's Company:

Contact Name for Information:

Device Model and Relevant Version Numbers:

Description of weakness with supporting evidence e.g. any tests carried out, equipment used, internet sources, etc.:

Evidence Provided:

Initial Manufacturer Acknowledgement/Comments:

Remedial Action Taken by Manufacturer

Estimated date from when equipment with improved IMEI implementation will be available:

Other Device Models Affected by Platform Vulnerability:

Any other comments or information (please provide information on additional sheets if necessary):

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601