CONSULTATION PAPER ISSUED BY

THE INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ON

IMDA IoT Cyber Security Guide
Annex C: Case Study on Smart Buildings

29th July 2022

CONTENTS

1. INTRODUCTION

1.1 The Internet of Things ("**IoT**") paradigm is one where devices are connected to one another and are able to either convey information about the surroundings or themselves or be controlled by others to perform certain actions. As people and devices become more connected, issues relating to the safeguarding of IoT information and management of cyber security threats become increasingly important.

1.2 In building a more digitally connected Singapore, it is important to secure our infrastructure and the IoT devices and networks deployed. While many users and/or vendors are aware of the need to implement security for their IoT devices and networks, they may not know where and how to start.

1.3 In March 2020, the Infocomm Media Development Authority ("IMDA") launched an IoT Cyber Security Guide ("Guide") to offer enterprise users and their vendors better guidance on deploying IoT technology. The Guide aimed to provide a practical document to help enterprise users and their vendors address the cyber security aspects of IoT systems in the acquisition, development, operation and maintenance of these systems. In support of this objective, the Guide introduced foundational concepts and provided a set of baseline recommendations & checklists for users and vendors.

1.4 In support of the Real Estate Industry Transformation Map (ITM), BCA, with the support of IMDA, works towards transforming the Facilities Management (FM) industry through the adoption of smart FM systems, which would help to enhance building facilities management and maintenance capabilities. The use of smart FM systems will help the FM industry in raising productivity and efficiency, reducing labour intensity and enhancing FM services delivery. According to the "Guide to Smart FM" launched in October 2019, it has become more common for FM service and solution providers to develop smart solutions to complement their products and services through the enabling of added features such as remote monitoring, fault detection, diagnostics and system optimisation.

1.5 While leading technology providers have already developed smart IoT solutions (connected services) for FM application such as remote chiller plant monitoring and predictive maintenance, one key concern remains which is the trust and security of such IoT solutions. In order to help the FM industry in the implementation of security requirements of these smart IoT FM systems, there is a need to enhance the Guide with a new annex ("Annex C"), with a case study

on Smart Buildings. We believe this case study will be helpful in demonstrating the application of the recommendations by the Guide.

1.6 IMDA would like to seek views and comments from members of the public and the industry on the proposed Annex C, of IMDA IoT Cyber Security Guide, which is enclosed with this Consultation Document.

1.7 This consultation will be open for a period of six weeks, and will close by 12 noon on 9th Sep 2022.

2. ANNEX C: CASE STUDY ON SMART BUILDINGS

2.1 Annex C provides a case study on the use of IoT devices for Smart Buildings that demonstrates the application of the Guide recommendations. The case study includes:

- A "General architecture of Smart Building" to help scope the case study;
- Derivation of the "Security objectives" according to the Guide; and
- Application of the Guide "Vendor disclosure checklist" to identify applicable security requirements and recommended mitigations.

Question 1: *IMDA would like to seek views and comments on the Figure C-1 "General architecture of Smart Building" given in the Annex C, and whether it is adequate and relevant. What other asset(s) of Smart Buildings, do you think should be included in the architecture?*

Question 2: *IMDA would like to seek views and comments on the usefulness, as well as the clarity and adequacy of "Security Objectives" proposed in the Annex C. What additional objective(s) do you think should be included in the checklist?*

Question 3*: IMDA would like to seek views and comments on the usefulness and adequacy of the applied vendor disclosure checklist, on Smart Buildings security, in the Annex C and the items listed within. For example, which checklist item is most, least or not applicable to you. What other supporting material(s), do you think should be included in the applied checklist?*

Question 4*: IMDA would like to seek views and comments on the usefulness and the clarity of the Annex C as a whole, and whether the coverage of the Guide is sufficient. What other area(s) do you think the Annex C should also cover, which would further help the industry to better secure IoT solutions for Smart Facilities.*

3. INVITATION TO COMMENT

3.1 IMDA would like to seek views and comments from members of the public and the industry on the issues outlined in the above sections.

3.2 Parties that submit comments on the issues identified in this Consultation Document should organise their submissions as follows:

i. Cover page (including their personal/company particulars and contact information);
ii. Table of contents;
iii. Summary of major points (structured to follow the individual Parts of the Consultation Document);
iv. Statement of interest;
v. Comments (in response to the Questions set out in the Consultation Document and any other comments); and
vi. Conclusion.

Supporting material may be placed in an Annex.

3.3 Where feasible, parties should identify the specific sections of the Consultation Document on which they are commenting and provide reasons for their proposals.

3.4 All submissions must reach IMDA by 12 noon on 9th Sep 2022. Softcopy of submissions in both Microsoft Word and Adobe PDF format should be provided. Parties submitting comments should include their personal/company particulars as well as the correspondence address, contact number and email addresses on the cover page of their submission. All comments should be addressed to:

Ms Aileen Chia
Deputy Chief Executive / Director-General (Telecoms & Post)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Please submit your softcopy via email to: Consultation@imda.gov.sg

3.5 IMDA reserves the right to make public any written submissions and to disclose the identity of the source. Commenting parties may request confidential treatment of any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive, with supporting

justification for IMDA's consideration. In such cases, the submission must be provided in a non-confidential form suitable for publication, with any confidential information redacted as necessary and placed instead in a separate annex.

3.6 If IMDA grants confidential treatment, it will consider, but will not publicly disclose the information. If IMDA rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider the information as part of its review. As far as possible, parties should limit any request for confidential information submitted. IMDA will not accept any submission that requests confidential treatment for the entire, or a substantial part of, the submission.