CONSULTATION PAPER ISSUED BY THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

ON

IMDA IoT Cyber Security Guide Annex C Case study on Smart Buildings

1 December 2022

PART I: INTRODUCTION

1. The Internet of Things ("IoT") paradigm is one where devices are connected and can convey information about and/or interact with its surroundings. As people and devices become more connected, issues relating to the safeguarding of IoT information and management of cyber security threats become increasingly important.

2. In building a more digitally connected Singapore, it is important to secure our IoT systems, infrastructure and devices 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.

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.

4. In support of the Real Estate Industry Transformation Map (ITM), Building and Construction Authority (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.

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. 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**"), case study on Smart Buildings. We believe this case study will be helpful in demonstrating the application of the recommendations of the Guide.

6. To solicit feedback on the proposed Annex C, IMDA issued a public consultation ("**Public Consultation**") on 29 July 2022. The Public Consultation was open for a period of six weeks, and IMDA received comments from 5 respondents (individually referred to as a "**Respondent**" and collectively, the "**Respondents**"). They are:

- Housing & Development Board (HDB)
- JTC Corporation (JTC)
- Singapore Institute of Technology (SIT) and Firefense Pte. Ltd
- Mr Kang Meng-Chow, Individual
- Mr Yap Kai-Yeow, Individual

7. IMDA thanks all Respondents and has given careful consideration to the comments received. This document sets out the key issues raised in the Public Consultation and provides IMDA's responses and decisions on these issues.

PART II: SUMMARY OF INDUSTRY RESPONSES AND IMDA'S DECISIONS ON KEY RESPONSES

8. IMDA sought comments on the adequacy, clarity and usefulness of the general architecture, security objectives, applied vendor disclosure checklist and the coverage and usefulness of the Annex C. The Respondents are generally positive and supportive of the Annex C, and have provided suggestions to enhance the Annex C.

General architecture of Smart Building

9. One Respondent suggested to emphasize whether Annex C is applicable to building system/device connected to the internet. IMDA agreed with the comment and has revised the relevant paragraphs, to make it clearer that internet connectivity is an optional consideration for the building system/device covered in Annex C.

10. Some Respondents suggested to cover more assets of Smart Building, such as electrical monitoring & control devices, autonomous robots, access management system (physical gantry, card access, etc.), smart pump systems (including transfer, booster & sump pumps), mechanical ventilation systems (in carparks and building) and centralised / district-level cooling systems. One Respondent suggested to consider Advanced Message Queuing Protocol (AMQP) for backend integration and communication. IMDA agreed that examples could help users better understand the guidance and has revised the Annex C to include additional examples. However, IMDA would like to highlight that it is impossible to provide examples of all technologies and protocols, and the examples provided are for illustrations only, they are not meant to be exhaustive or prescriptive.

11. One Respondent enquired whether there are plans to include Smart Buildings with decentralized IoT systems (with separate networks). IMDA has added a note in Clause 2.3 to highlight that although not modelled in this case study, the reader may include considerations for smart buildings with decentralized IoT systems on separate networks.

Security objectives

12. One Respondent commented that the confidentiality, integrity and availability (CIA) triad provides a good impact assessment of targeted system / asset and can help to prioritise which system / asset to be better protected. The Respondent further suggested to include safety as an objective, as a compromised system / asset can be used to cause physical harm. IMDA would like to highlight that the relationship between safety and CIA triad is provided under Clause 2.4 of Annex C. This case study focuses on cyber security and safety is indirectly covered by the CIA triad.

13. Some Respondents commented that the CIA triad requires additional definitions to define the levels or impact criteria (,i.e., low, moderate, high) of CIA triad. IMDA would

like to highlight that the impact levels of CIA triad is defined in “ITSC TR 64: 2018 Guidelines for IoT security for smart nation”, which the IMDA IoT Cyber Security Guide document is based upon.

14. One Respondent suggested that for availability, it should cover dependencies (i.e., whether a system outage affect another system in the building). IMDA agreed with the comment and has added a note on page 12 of Annex C, that this may be a consideration but not illustrated in this case study.

15. There were suggestions from one Respondent to include: (i) difference between one device unit being compromised versus multiple being compromised, (ii) the need to detect compromised device promptly, (iii) the need to support fast isolation of a network segment, and (iv) the need for the edge gateway to monitor and response to a compromise of its connected devices. IMDA has revised the Annex C as appropriate. However, IMDA would like to highlight that it is impossible to cover all scenarios and mechanisms. Annex C illustrates a generic approach to identify security objectives based on user’s business needs.

<u>Applied vendor disclosure checklist</u>

16. One Respondent acknowledged that the applied vendor disclosure checklist items are applicable as security requirements for Smart Building.

17. One Respondent suggested for the Annex to highlight on the need to ensure that there is qualified and designated personnel, in the areas of information technology (IT) and operational technology (OT) security, to look after the procurement and maintenance processes. While IMDA agreed with the importance of personnel management, this is not in scope as defined by the Guide.

18. One Respondent suggested to (i) emphasize the management and maintenance of device, (ii) provide evidence of device operating system (OS) update and patching, (iii) ensure segregation of networks and (iv) prevent unauthorized devices from connecting. IMDA has studied the suggestions and revised items CK-LP-06, CK-LP-07, CK-NP-01 and CK-NP-04, as appropriate.

19. One Respondent suggested to rename the checklist as "Device Vendor Security Implementation Disclosure". IMDA would like to highlight that the checklist is also applicable for solution vendors and system integrators, thus the name “Vendor disclosure checklist” is more appropriate.

20. One Respondent suggested for the Annex to further recommend on (i) wireless protocol evaluation, (ii) physical security of devices, (iii) device verification at printed circuit board (PCB) level and (iv) awareness of Linux kernel & operating system (OS) in use. IMDA has studied the suggestions and revised items CK-NP-03, CK-AP-04, CK-LP-07 and CK-LP-06, as appropriate. The Respondent also suggested to recommend firmware protection analysis and awareness of supply chain. IMDA would like to highlight that these suggestions are already covered by items CK-DP-02, CK-LP-06, CK-LP-07 and CK-LP-03.

21. One Respondent suggested to include examples for items CK-DP-01, CK-DP-02, CK-DP-03, CK-RS-02 and CK-LP-02. IMDA has studied the suggestions and added examples for items CK-DP-01, CK-DP-02, CK-DP-03, CK-DP-04, CK-RS-02 and CK-LP-02.

22. One Respondent noted that CSA's Cybersecurity Labelling Scheme (CLS) was mentioned under CK-LP-07 and sought to clarify whether Annex C intended to recommend or mandate the usage of CLS-labelled products only. IMDA would like to highlight that CK-LP-07 had referenced CSA CLS scheme as an example. Also, it should be noted that the checklist is only a template of common security considerations. Users are required to determine the appropriateness and applicability of the checklist items to add on, remove, and/or adjust according to its uses and business needs.

Overall Coverage and Usefulness

23. Most Respondents found Annex C as a useful add-on to the IoT Cyber Security Guide. One Respondent commented that overall Annex C provides a good baseline to secure IoT solutions and has defined a list of controls in the different areas which can be applied onto IoT solutions. Another Respondent commented that Annex C provides a good baseline view of the different levels that organisations should consider when designing and evaluating the use of Smart Building solutions.

24. One Respondent suggested that there is a need to place emphasis of Annex C onto regulated entities especially the critical information infrastructure owners (CIIOs). IMDA noted the suggestion but would like to highlight that Annex C is a case study to illustrate good practices for voluntary adoption. Users of this case study will still need to customise the content according to their business needs, and check with the relevant regulatory bodies on the latest regulatory and statutory requirements, where applicable.

25. One Respondent suggested for the assessment scope to include operational technology (OT) aspect of Smart building solution, to compare the risk assessment approach for cyber physical systems to a traditional risk assessment for enterprise system and provide guidance to on engineering safeguards and the safety aspects as part of the risk assessment. IMDA noted the suggestions and would like to highlight that these are covered in Clause 2.4 of Annex C.

26. One Respondent suggested to furnish more details to guide the system owner's run through of each phase of the risk assessment and the considerations. IMDA would like to highlight that this is provided by table C-1 of Annex C.

27. One Respondent suggested that for the assessment on the attacker's capabilities, there should be guidance on how we define and identify the right asset that would be of interest from the attacker's point of view. IMDA noted the suggestion but would like to highlight that identifying an asset of interest from the attacker's point of view is context-sensitive and highly subjective. Our intention is to point out that an attacker's capability is a consideration for the readers of this case study.

28. One Respondent suggested to include examples for end-to-end encrypted communications in Smart Buildings, on specific principles and security mechanisms

mentioned. IMDA noted the suggestion and has added some examples for item CK-DP-01, CK-RS-02 and CK-LP-02, but it is impossible to be exhaustive.

29. One Respondent suggested to provide optional indicators for specific items on the vendor disclosure checklist, such as if they are not always applicable to all systems. IMDA noted the suggestion but would like to highlight that this is covered by the introduction to Clause 6 of Annex C: “Users must determine the appropriateness and applicability of the checklist items to add on, remove, and/or adjust according to the uses and business needs.”

30. One Respondent suggested to consider expansion to cover non-unified IoT network designs, and the associated security considerations and objectives for it. IMDA noted the suggestion and would consider this when the opportunity arises.

PART III: CONCLUSION

31. IMDA had carefully considered all the suggestions and comments provided by the Respondents and has revised the Annex C to incorporate the applicable inputs to enhance the clarity and applicability of the Annex C, while ensuring that the Annex C remains succinct to be useful.

32. IMDA understands that cyber security covers very broad aspects, and it notes that some suggestions received are not covered by the scope of the Annex C. IMDA will give due consideration to these suggestions when developing new guidelines or revising Annex C in the future.

33. The Annex C of IMDA IoT Cyber Security Guide has been finalised and published on 1st December 2022.