INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY

CONSULTATION PAPER ISSUED BY THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

CONSULTATION ON THE IOT CYBER SECURITY GUIDE

13th March 2020

PART I: INTRODUCTION

1. The Internet of Things ("**IoT**") paradigm is one where devices connect to one another, and are able to either convey information about the surroundings or themselves, or be controlled to perform certain tasks. There has been growing industry and business use of IoT sensors and actuators, e.g. asset tracking in logistics and industry automation. The use of IoT has also become more pervasive in our daily lives, which include health monitoring, tracking of public transport, and controlling home appliances remotely.

2. While the deployment of these large number of devices could help enhance business productivity and improve convenience in our daily lives, any disruption to their designed operation, either intentionally or unintentionally, will likely bring inconveniences and possibly monetary losses and reputational damages to users and providers of IoT technology. If not managed well, these IoT devices could also be exploited, causing cyber security threats such as distributed denial of services. Data (including any personal data) collected and stored in the devices will also need to be protected against unauthorised access.

3. In building a more digitally connected Singapore, it is thus important to secure our infrastructure and the IoT devices and networks deployed. The Infocomm Media Development Authority ("**IMDA**") has thus developed an IoT Cyber Security Guide (hereafter refer to as the "**Guide**") to provide recommendations and guidance to IoT users and vendors in securing their IoT devices and networks.

4. To solicit feedback on the Guide, IMDA issued a public consultation ("**Public Consultation**") on 25 January 2019. The Public Consultation was open for a period of six weeks, and IMDA received comments from 20 respondents (individually referred to as a "**Respondent**" and collectively, the "**Respondents**"):

- Booz Allen Hamilton International Pte Ltd
- BSA The software alliance
- Cetome
- Cisco Systems (USA) Pte Ltd
- Cyber Security Agency (CSA)
- Mr Cyril Tan, Individual
- EVVO Labs Pte Ltd
- Government Technology Agency (GovTech)
- Housing & Development Board (HDB)
- ioXt Alliance
- Internet Society (ISOC) Asia-Pacific Regional Bureau
- Internet Society (ISOC) Singapore
- Privasec Pte Ltd
- Seagate Singapore International Headquarters Pte Ltd
- Singapore Telecommunications Limited (SingTel)
- StarHub Ltd
- UK Department of Digital, Culture, Media & Sport
- UL Singapore
- V-Key Pte Ltd
- VIBE Cybersecurity International LLC

5. 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 as well as provides IMDA's responses and decisions on these issues.

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

6. IMDA sought comments on the specific proposals in the Guide, the overall clarity of the Guide, and the concept of having a certification program based on the checklists. The Respondents are generally positive and supportive of the Guide, and provided suggestions to enhance the Guide.

Baseline Recommendations

7. Some Respondents suggested providing more examples in the Guide so that the content could be better understood. The additional examples suggested included recommendations for non-IP protocols that are used by technologies such as LoRa, Zigbee, etc. Examples of newer technologies and protocols were also suggested to be added. One Respondent had also suggested adding a summary before each of the listed cybersecurity principles for clarity. IMDA agrees that examples could help users better understand the baseline recommendations and has thus revised the Guide to include a few additional examples as suggested. However, IMDA would like to highlight that it is impossible to provide examples for all various technologies and protocols, and that the examples are provided as illustrations only, which are not meant to be exhaustive or prescriptive. IMDA also agrees that users could better understand the principles introduced with more explanations provided. However, IMDA is mindful of the need to keep the main document succinct to facilitate adoption. The additional examples provided for each of the principles in Annex A are self-explanatory, and will enhance the clarity of the Guide to users.

8. Some Respondents suggested that more details could be included, such as the minimum version of protocols to be used, the approved algorithm and random number generator, and examples on how to harvest and correctly use random numbers in common systems. On these suggestions, IMDA would like to highlight that the Guide is not meant to be prescriptive on the choice of technologies. As such, IMDA avoids providing specific details in the Guide. Users are in a better position to decide on the specific technologies and detailed configurations that meet their business needs and the respective regulatory requirements.

9. A few Respondents provided recommendations to enhance the Guide, such as having all software and firmware upgrades and updates digitally signed and verified, continuous monitoring of devices and traffic flow, and secure key deployment. IMDA has reviewed these recommendations and has revised the baseline requirements and checklist to incorporate relevant recommendations.

10. Some Respondents viewed that it might not be necessary to separate the baseline recommendations for implementation and operational phases because some

cybersecurity concepts would not fall neatly into either phase. While IMDA agrees that some cybersecurity concepts are common across the different phases, IMDA views that the segmentation of implementation and operational phases would provide clarity and ease of adoption to the different types of users (developers, providers & end-users).

11. There were suggestions from some Respondents to use and/or add different terminologies, concepts, principles and categorisations. IMDA notes that there is much published work on cybersecurity, advocating various best practices. As it is not possible to adopt all the differing practices, IMDA has developed the Guide based on the more commonly accepted practices and simplified them where necessary to ease user understanding, and set out the core principles. IMDA notes that there were suggestions to include principles that do not fall within the intended scope of this Guide, such as governance, risk, privacy requirements, incident management, gathering of digital forensic evidence, etc. IMDA will take these suggestions into consideration when planning for the development of new guidelines in the future.

12. One Respondent has suggested the inclusion of the logging of all system accesses to a central server. While IMDA views that having a centralised logging mechanism may not be applicable for all IoT systems, IMDA would like to clarify that the requirement for audit log capability was originally embedded within one of the baseline recommendations (6.5.1). IMDA agrees that having an audit log is relatively important and has thus formed a new baseline recommendation on its own. With this move, IMDA has also refined the original recommendation 6.5.1 to focus on guarding against threats on resource exhaustion.

13. Some Respondents shared the concern that some recommendations provided might not be suitable or applicable for all use cases and including them in the Guide might give the wrong impression that strict adherence by users would be required. One example shared was that the security requirement “employ secure versions of transport protocols” could not be effectively applied to, nor was it necessary for, IoT devices working with an infrared remote control. IMDA notes the concern and would like to highlight that the Guide is meant as a reference and is not for strict adherence for all use cases. IMDA has thus added a note to inform users that they ought to assess the relevance of the recommendations based on their specific systems’ needs.

14. One Respondent recommended to avoid stating password construction rules as such rules might conflict across different regulatory regimes. While IMDA views that it is important to ensure strong password is implemented, IMDA also notes that different regulatory requirements may define the construction rules differently. Hence, IMDA has revised the Guide to recommend the adoption of published international best practices for password construction rules and has also suggested the minimum requirement for constructing a strong password.

Threat Modelling Checklist

15. While most Respondents valued the importance of the threat modelling checklist, several Respondents also shared that the application of it could be challenging due to the wide variety of IoT devices available in the market. They suggested that this section be further simplified, and more examples and guidance be

provided. IMDA notes the comments and suggestions raised, and would like to highlight that threat modelling itself is a relatively complex process due to the many variables involved. Further simplification of the process could diminish its effectiveness. Hence, IMDA has illustrated the use of the checklist via a case study in Annex B of the Guide, with the aim of helping enterprise users to better understand how to conduct threat modelling.

16. One Respondent suggested to have more specific details on the appropriate person who would be filling the checklist. IMDA would like to highlight that it is for the organisation to decide on the appropriate person to fill the checklist as it depends on factors such as organisation structures, level of technical expertise, etc.

17. Some Respondents suggested additional items such as the detection of malicious software to be included in the checklist. IMDA would like to clarify that some of these suggested items are currently provided in the Vendor Disclosure Checklist. Other suggested items which Respondents would like to see, such as the identification of targets, assets and threats, are also provided in the case study in Annex B.

18. One Respondent commented that threat modelling was a continual process, subject to re-assessment when conditions, such as the environment, had changed. IMDA agrees and has thus revised the Guide to include threat modelling in the baseline recommendation of “conduct periodic assessments”.

Vendor Disclosure Checklist

19. Respondents were generally of the view that the checklist was useful. Some Respondents remarked that they would like the Guide to distinguish between the mandatory and optional items as not all checklist items provided would be applicable to all use cases. Some other Respondents raised concerns that the description in the checklist might not be sufficiently clear, leading to misinterpretation by the vendor and thus resulting in inaccurate submission of compliance. IMDA would like to highlight that the vendor disclosure checklist provided is only a template of common security considerations. Users will need to determine the appropriateness and applicability of the checklist items so as to add on, remove, and/or adjust them according to the uses and businesses’ needs. IMDA would also like to clarify that the checklist allows the vendor to provide “supporting materials” to give evidence of compliance. If additional assurance is required, a third-party professional body could be engaged to validate the vendors’ submission. Noting the general concern on the use of the checklist as a definitive document, IMDA has updated the Guide to clarify that the checklist is to be considered as a template of sample questions, which should be tailored to the circumstances of the user as suggested by one Respondent.

20. Some Respondents suggested the inclusion of several security checklist items in the areas of data privacy, incident management, etc., which would not fall within the scope of the Guide. While IMDA notes the importance of these measures, IMDA is of the view that users could include these requirements in their checklist when they refine the checklist items for their adoption.

21. One Respondent suggested that different checklists be provided for different types of vendors, such as manufacturers, service providers and software suppliers. IMDA views that the different checklists will overlap considerably and it will be difficult for users to manage and maintain the different checklists. Hence, IMDA will continue to maintain a general checklist in the Guide for both buyers and vendors to adapt for their business cases.

22. One Respondent is concerned that the checklist would result in high cost for the deployment of voluminous IoT devices. While IMDA agrees that the adoption of the checklist may result in higher implementation cost, IMDA would like to emphasise that significant losses (monetary and reputational) may also occur due to insufficient cybersecurity measures. The user should thus assess the level of cybersecurity required for its IoT systems, depending on the use case.

Annex A: Foundational Concepts

23. Some Respondents commented that Annex A could be too short and suggested for more details to be included. They observed that many vendors found it difficult to conduct meaningful and comprehensive threat modelling and thus, requested that more assistance be rendered to these vendors via the Guide. One Respondent on the other hand suggested to simplify the content of Annex A and move it to the introduction segment of the main document. IMDA notes the challenges for vendors to conduct threat modelling and has thus added a reference to Open Web Application Security Project ("**OWASP**") as an example, which provides more resources and information on threat modelling. As for the suggestion to move Annex A to the main document, IMDA views that this could result in an overly-dense main document of the Guide.

24. One Respondent queried the basis on which TR64 would be used as a reference for the foundational concepts in Annex A. The Respondent believed that the foundational concepts should be more related to IoT protocols and networks. IMDA would like to clarify that TR64 is a published national technical reference on IoT security, which IMDA has developed together with industry members and other relevant government agencies. Its foundational concepts for cybersecurity are based on international best practices for system-level engineering. As the Guide covers general IoT systems, IMDA is of the view that the referencing to TR64 is appropriate and relevant.

25. One Respondent suggested that online references be provided instead of the Annex, given that concepts in the Annex could be outdated very quickly. IMDA agrees that the cybersecurity concepts and methodologies stated in Annex A could become less relevant over time due to the evolving threats and technologies. This also applies to online references if they are not adequately maintained and updated. Instead of providing only online references as suggested, which could inconvenient readers, IMDA has thus included references in Annex A in addition to the text. IMDA will continue to work closely with industry members to track the evolving cybersecurity risk, update the Guide, and ensure that the Guide remains relevant and adequate.

Annex B: Case Study on Home Control System

26. Many Respondents expressed that the case study provided in Annex B was useful and had suggested for more case studies to be included, considering that the IoT environment would be diversified and one specific example might not provide sufficient clarity to user. IMDA notes the comments and would work with interested parties to develop more case studies for specific application.

27. One Respondent raised the concern that no single party (such as Internet Access Service Providers and device manufacturers) other than the customer would have an oversight of the full end-to-end IoT ecosystem within the home and thus, threat assessment could not be properly carried out, especially when the customer is not technically savvy. IMDA would like to clarify that the Guide is meant for enterprise users/vendors of IoT systems, and not individual end customers. Nonetheless, IMDA notes that it is possible that enterprise users may not have strong cybersecurity capability and thus, the Guide is developed to provide them with basic cybersecurity knowledge as well as highlight the baseline requirements they should include when procuring and implementing IoT system. The users could engage independent third-party assessors to assist in reviewing and assessing the vendors' submissions against the checklist.

28. One Respondent suggested that an actual Smart Home case study could be used instead of a hypothetical one. IMDA agrees that this would be beneficial and would work with the relevant parties to develop case study that is based on actual implementation.

29. Another Respondent commented that the tiered approach might lead to "medium" and "low" risk levels being ignored, even though their combination could result into a higher tiered risk. IMDA agrees with the comment and would like to clarify that an illustration of such a scenario has been provided in the case study on smart socket device. IMDA would also like to highlight that the security assessor should consider the system holistically and assign the appropriate ratings.

Usefulness and Clarity of Guide

30. Most Respondents found the Guide useful, especially to companies that do not have strong security knowledge. Some Respondents commented that the Guide provides clarity, while others suggested that the scope be expanded to include security governance and management. IMDA notes the importance of the other security aspects that are not covered within the Guide. IMDA will review and consider the need to develop new guidelines or expand the Guide to cover these security aspects in future.

31. One Respondent suggested adding a section to map international standards to the baseline standards given in the Guide, so that readers/users can refer to them for more details. IMDA notes the suggestion and has added references to relevant international standards for each baseline recommendation.

32. One Respondent suggested that different requirements be applied for different types of devices. IMDA would like to highlight that this Guide provides system-level

recommendations, and will consider the suggestion if the Guide is revised to include recommendations for devices.

Need for Certification Scheme

33. Most Respondents commented that they did not favour a blanket mandatory certification scheme for all IoT devices/systems, citing high costs as the key reason for their disinclination. Some of these Respondents also shared their concerns that a mandatory certification scheme would hinder innovation and vendor's ability to respond in a timely manner to emerging threats.

34. A few Respondents had on the other hand shared their support for the use of mandatory scheme in specific sectors such as military, healthcare and transport, and also for critical infrastructure. One of the Respondents viewed that government agencies could take the lead in requiring certification for their IoT devices/systems, levelling up the industry as a whole, because both government agencies and the involved IoT device manufacturers (and solution providers) would be more willing to pay the additional cost for certification.

35. Many Respondents support the use of voluntary certification because doing so would encourage the use of trusted and security compliant devices to find its way into the market. One Respondent commented that the certification program should provide trustmark to certified products, informing consumers that these products carry a higher level of security than those without the trustmark. However, another Respondent raised concern on the validity of the certificate in view of the need for device firmware to be regularly updated and patched to address evolving threats.

36. Some Respondents suggested that IMDA could consider going through an extensive consultation with stakeholders to assess the practicality of a security certification scheme. One Respondent commented that the lack of a consultation before launching a certification scheme could result in a backlash from the industry.

37. IMDA notes the comments and concerns shared by the Respondents and understands that any certification scheme, voluntary or mandatory, if introduced, will need to ensure a balance of necessity and practicality. IMDA agrees that different types of devices require different certification schemes, i.e., mandatory or voluntary, depending on the potential impact should these devices be compromised. IMDA also agrees that consultation should be put in place if such certification schemes, in particular the mandatory ones, are to be launched. IMDA will take these suggestions into consideration and work with the Cyber Security Agency of Singapore ("**CSA**") should any certification scheme be introduced.

PART III: CONCLUSION

38. IMDA has considered all the suggestions and comments provided by the Respondents. IMDA has revised the Guide to incorporate those relevant and applicable to enhance the clarity and applicability of the Guide, while ensuring that the Guide remains succinct to facilitate adoption.

39. IMDA understands that cybersecurity covers very broad aspects and it notes that some suggestions received are not covered by the scope of the Guide. IMDA will give due consideration to these suggestions when developing new guidelines or revising the Guide in the future.

40. IMDA has consulted CSA in finalising the Guide, and CSA has given its support.

41. The finalised IMDA IoT Cyber Security Guide is published on 13th March 2020.