CONSULTATION PAPER ISSUED BY THE

INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

SECURITY REQUIREMENTS FOR RESIDENTIAL GATEWAYS

13 March 2020

Consultation on Security Requirements for Residential Gateways

Background

1. The increasing proliferation of computing devices in residential homes nowadays translate to heightened risks of cyber-attacks that leverage on these devices. Many of these edge devices, Internet-of-Things (IoT) sensors and network infrastructure today may have minimal basic protections, weak credentials or are based on outdated firmware versions. Hence, such devices, including residential gateways and their connected IoT devices in homes are vulnerable to unauthorised access by actors and perpetrators for malicious activities, such as in the use for Distributed Denial of Service (DDoS) attacks.

2. IMDA is working with the Cybersecurity Agency ("CSA") to look into initiatives to better protect Singapore's telecom networks and IoT devices, such as establishing cybersecurity standards and guides. To this end, IMDA, with the CSA's support, plans to publish a new Technical Specification ("**IMDA TS RG-SEC"**), specifying minimum security requirements and stronger credential settings for Residential Gateways (RG), commonly known as home routers, that are sold and used in Singapore. RGs are network devices that connect the local home network, such as personal computers and other connected home IoT devices, to the Internet. Figure 1 below shows a typical home network connection with an RG:

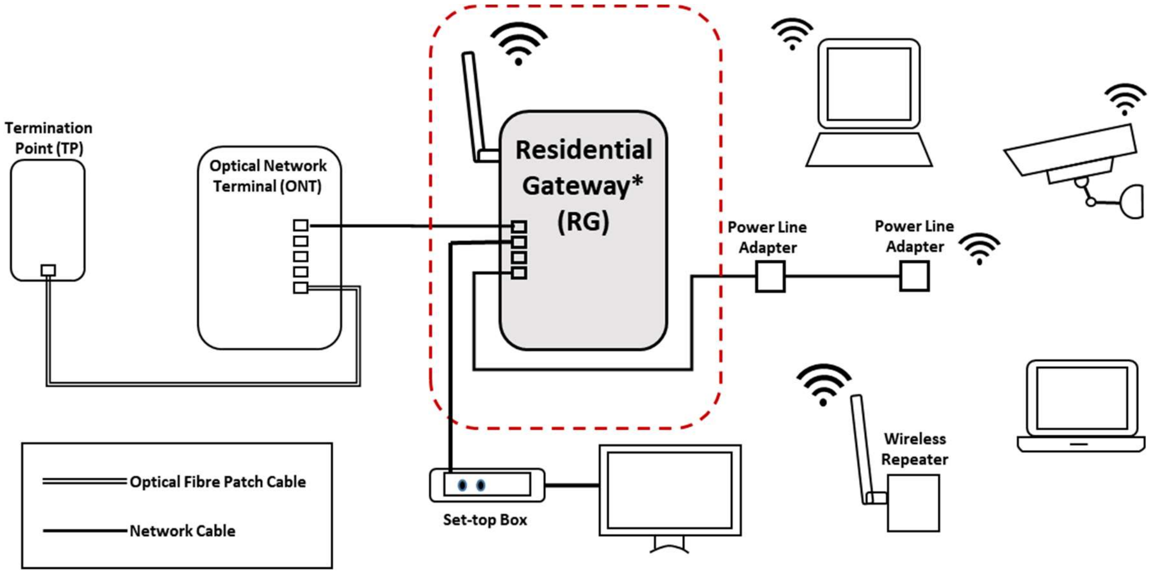


Figure 1: Typical Home Network Connection with Residential Gateway

3. The IMDA TS RG-SEC aims to minimise the risk of unauthorised access of the RGs and thus, mitigate the associated cybersecurity threats.

Proposed Security Requirements for Residential Gateways

Login Credentials (Ref: IMDA TS RG-SEC Paragraph 4.1)

4. Many of the RGs today come pre-loaded with default login credentials, such as usernames and passwords, for access to the RGs' administration page[1]. These factory pre-loaded default login credentials are often weak, not unique and almost never require any changes throughout their use, and hence can be easily compromised by actors and perpetrators, to gain and take control of the RGs for malicious cyber activities. IMDA TS RG-SEC will thus require that these factory pre-loaded login credentials be randomised and unique for each RG, with minimum password strength as specified. If factory pre-loaded default login credentials are provisioned, users will be required to change these credentials before the RGs can be used.

Question 1: IMDA invites comments relating to the requirements on pre-loaded credentials and password strength for RGs as set out in paragraph 4.1.

Device Setup & Administration (Ref: IMDA TS RG-SEC Paragraph 4.2)

5. With technology advancements, RGs today come with many additional features and functions. An example would be Universal Plug and Play (UPnP), which allows devices connected to the RG to seamlessly discover each other's presence and establish functional network services for data sharing. Although such features and functions could be useful, they also provide openings for cybersecurity attacks if users are unaware that they have been activated. Considering that many users do not use these functions, the IMDA TS RG-SEC will require that these interfaces be turned off by default. In addition, the IMDA TS RG-SEC will also require the preloaded settings of RGs to disable some protocols/mechanisms that could be exploited, such as Home Network Administration Protocol (HNAP) and IPv6 tunnelling.

6. In addition to having secure preloaded settings for RGs, it is also important for RGs to be set up properly, such as ensuring that only authorised personnel can configure them. Hence, the IMDA TS RG-SEC will specify the handling of authentication and passwords. The IMDA TS RG-SEC will also require the device management interface to be secure, thereby preventing communication channels from being sniffed by unauthorised actors.

Question 2: IMDA invites comments relating to the requirements on pre-loaded settings for RGs as set out in paragraph 4.2.1.

Question 3: IMDA seeks feedback on the requirements on RG administration as set out in paragraph 4.2, in particular the applicability of maintaining secure communication protocols such as SSH or HTTPS for device management interfaces to the RG as indicated in paragraph 4.2.5.

[1] RG's administration page allows the RG's configurations and settings to be changed.

Firmware Updates (Ref: IMDA TS RG-SEC Paragraph 4.3)

7. The updating of the RGs' firmware with latest security patches is just as critical as any of the above mentioned security measures. Frequent timely updates will help to ensure that the RGs are protected against newer threats or newly found security lapses. However, it is noted that users may not update their RGs' firmware, even if security patches have been made available, thus making the RGs vulnerable. Hence, the IMDA TS RG-SEC will require the RGs to download and update the latest available firmware versions automatically. Nonetheless, IMDA is mindful that if the updating of firmware is disrupted or not done properly, it could affect the RGs' proper functioning subsequently. Thus, the IMDA TS RG-SEC does not specify the minimum period for the RG to be updated with the latest firmware.

Question 4: IMDA seeks feedback on the feasibility for RG to be updated automatically with the latest firmware as outlined in paragraph 4.3. IMDA welcomes suggestions on possible implementation of automatic updates of RG's firmware, including the management of disrupted update processes.

Question 5: While IMDA does not specify any timeline for security patches to be made available upon the finding of new vulnerabilities, IMDA seeks views on the typical duration for patches to be made available, and whether there is a need to impose such a timeline for patches to be applied.

Wireless Access & Data Protection (Ref: IMDA TS RG-SEC Paragraphs 4.4 & 4.5)

8. In addition to securing the access to the RG and having updated firmware, the RG should also ensure that its communication with connected devices in the home is secure. The IMDA TS RG-SEC will specify default encryption algorithms for such communications and the storage of data that they use. The RG shall also allow the user to set up guest networks with separate login credentials for authorised guest users of the home network.

Question 6: IMDA seeks comments on the requirements on the protection measures set out in paragraphs 4.4 to 4.5, in particular the requirement to display warning(s) of the higher security risk should weaker encryption algorithms be chosen.

Validation of Data Inputs (Ref: IMDA TS RG-SEC Paragraphs 4.6)

9. IMDA notes that RGs will remain vulnerable if the data inputs are executed without being validated, exposing attached devices to known security vulnerabilities, such as Information leakage, remote code execution and cross-site scripting. The IMDA TS RG-SEC will thus require the RG to validate data inputs via all interfaces.

Question 7: IMDA seeks feedback on the requirement for RG to validate data inputs via all interfaces as outlined in paragraph 4.6. IMDA also seeks feedback on the possible documents/information to be submitted for IMDA verification of this requirement when performing equipment registration.

Vulnerabilities Reporting (Ref: IMDA TS RG-SEC Paragraphs 4.7)

10. IMDA notes that it is not uncommon for new vulnerabilities of RGs to be discovered by various research institutes, organisations and individuals over time. Hence, IMDA views that it is important for RG manufactures to provide contacts for the public to inform them of the discovered vulnerabilities, allowing the manufacturers to develop security patches to address these vulnerabilities. In addition, IMDA understands that RG manufacturers would typically establish vulnerability disclosure policies.

Question 8: IMDA seeks views on what standards or guidelines are being used by RG manufacturers in developing their vulnerability disclosure policies.

Other Recommendations

11. The industry concerned should assess the impact of the proposed security requirements on RGs registered with IMDA, to be deployed on broadband networks in Singapore.

Question 9: IMDA welcomes suggestions on other possible recommendations to secure the RGs.

Implementation Plan and Timelines

12. Following the close of the consultation, IMDA will review and assess all responses received prior to finalising the IMDA TS RG-SEC. The finalised IMDA TS RG-SEC will be in force 6 months from its publication date. IMDA considers that a 6-month duration will be sufficient for suppliers to bring in new RGs or refresh existing RGs to comply with the security requirements stipulated in the new IMDA TS RG-SEC.

13. Concurrently, IMDA plans to require the cessation of the sale of any previously registered RGs, which are not in compliance with IMDA TS RG-SEC, 1-year from the publication date of the IMDA TS RG-SEC. The timelines with the key milestones are shown in the attached **Annex A**.

Question 10: IMDA invites comments on the proposed implementation plan and timelines.

Proposed Registration Scheme and process for RG

14. Today, equipment suppliers seeking to import and sell RGs are required to register the RG with IMDA by making an online declaration of conformity to the IMDA TS SRD[2] via the Enhanced Simplified Equipment Registration (ESER)[3]. Once the device is successfully registered with IMDA it can be released for sale for local use. Following the publication of the finalised IMDA TS RG-SEC, registations for RGs can be submited via a fresh registration under the ESER by making the necessary online declaration of conformity to IMDA TS RG-SEC and IMDA TS SRD for the RG models, and with the relevant supporting documents.

Question 11: IMDA invites comments on the proposed equipment registration process for RGs.

[2] IMDA Technical Specifications for Short Range Devices

[3] ESER is a self-declaration scheme where approval can be based on a declaration of conformity that does not need prior verification by IMDA. No registration fee is required.

Invitation to Comment

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

16. 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.

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

18. All submissions must reach IMDA by **12 noon on 10 April 2020**. 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

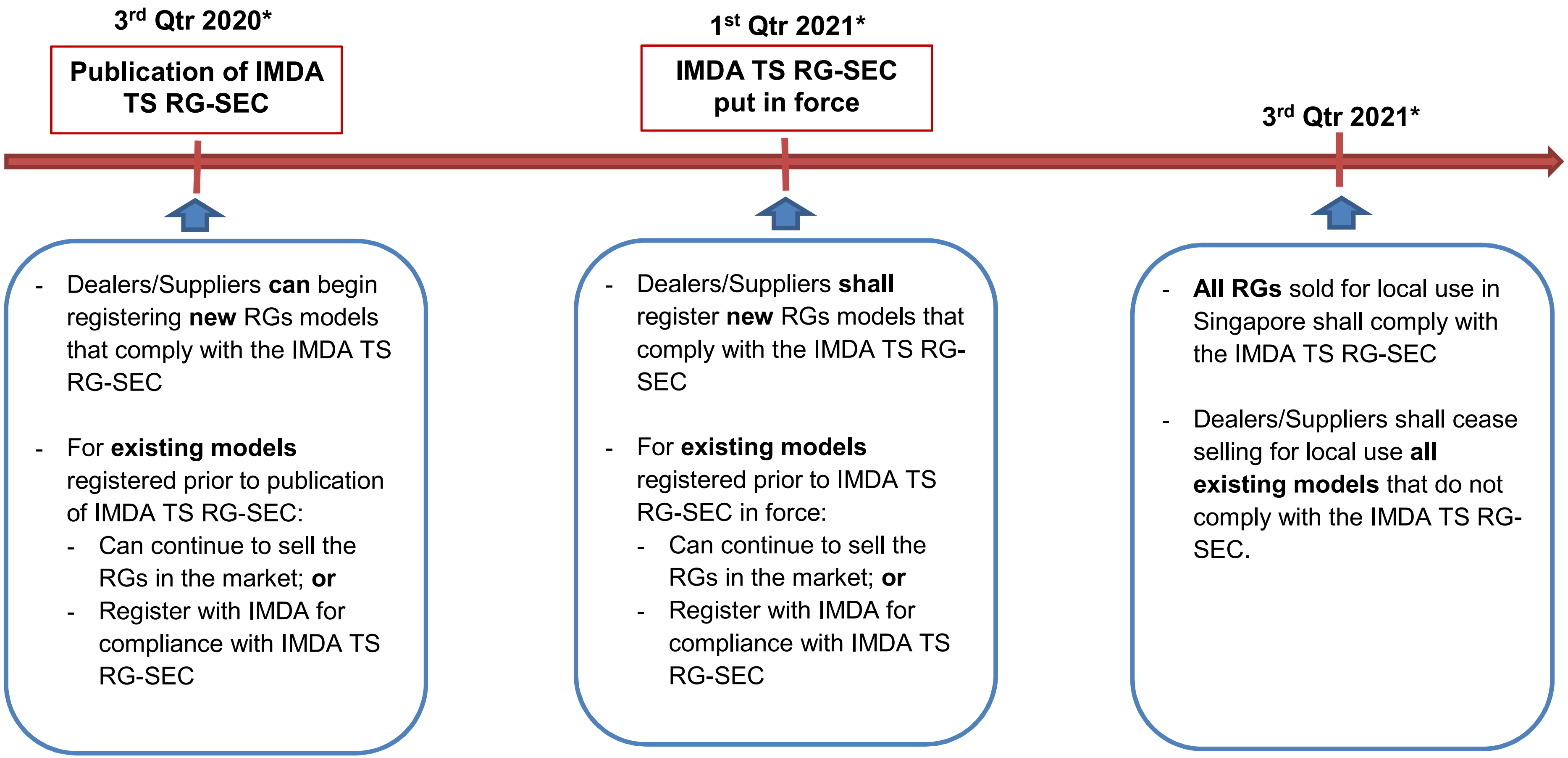
    Please submit your softcopy via email to: Consultation@imda.gov.sg

19. 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.

20. 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.

Security Requirements for Residential Gateways
Annex A: Implementation Timelines



3rd Qtr 2020*

Publication of IMDA TS RG-SEC

- Dealers/Suppliers **can** begin registering **new** RGs models that comply with the IMDA TS RG-SEC

- For **existing models** registered prior to publication of IMDA TS RG-SEC:
  - Can continue to sell the RGs in the market; **or**
  - Register with IMDA for compliance with IMDA TS RG-SEC

1st Qtr 2021*

IMDA TS RG-SEC put in force

- Dealers/Suppliers **shall** register **new** RGs models that comply with the IMDA TS RG-SEC

- For **existing models** registered prior to IMDA TS RG-SEC in force:
  - Can continue to sell the RGs in the market; **or**
  - Register with IMDA for compliance with IMDA TS RG-SEC

3rd Qtr 2021*

- **All RGs** sold for local use in Singapore shall comply with the IMDA TS RG-SEC

- Dealers/Suppliers shall cease selling for local use **all existing models** that do not comply with the IMDA TS RG-SEC.

***indicative dates**