



Communications  
Security Establishment

Centre de la sécurité  
des télécommunications

# CANADIAN CENTRE FOR **CYBER SECURITY**

## COMMON CRITERIA MAINTENANCE REPORT

### RICOH IM 370 version E-1.00-H

### 26 September 2024

## 627-LSS

## v1.0

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada 

# FOREWORD

This Maintenance Report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The IT product identified in this report has been previously evaluated at an approved Common Criteria testing lab established under the Canadian Common Criteria program using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5.

This report is not an endorsement of the IT product by the Canadian Centre for Cyber Security, and no warranty of the IT product by the Canadian Centre for Cyber Security is expressed or implied.

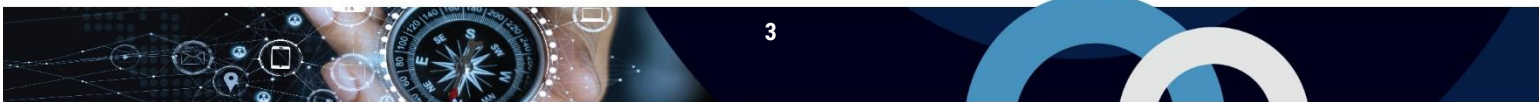
If your organization has identified a requirement for this maintenance report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security  
Contact Centre and Information Services  
[contact@cyber.gc.ca](mailto:contact@cyber.gc.ca) | 1-833-CYBER-88 (1-833-292-3788)



# TABLE OF CONTENTS

- 1 Introduction..... 4
- 2 Description of Changes..... 5
  - 2.1 Affected Developer Evidence ..... 5
- 3 Conclusions..... 6
- 4 References..... 7



# 1 INTRODUCTION

An Impact Analysis Report was submitted to the Canadian Common Criteria program to extend the validity of the Common Criteria certificate previously awarded to **RICOH IM 370 version E-1.00-H** from **Ricoh Company, Ltd.**

The process to achieve this under mutual recognition is described in [Assurance Continuity: CCRA Requirements](#), version 3.1, February 2024. In accordance with the requirements of this process, the Impact Analysis Report describes all changes made to the product and/or its IT environment, all resulting changes made to the evaluation evidence, and the security impact of the changes.

The purpose of this document is to summarize and present the Canadian Common Criteria program's findings regarding the assurance maintenance of **RICOH IM 370 version E-1.00-H**, hereafter referred to as the maintained Target of Evaluation, or maintained TOE.



## 2 DESCRIPTION OF CHANGES

The following characterizes the changes implemented in the maintained TOE and/or the environment. For each change, it was verified that there were no required changes to the security functional requirements in the Security Target.

**Table 1: TOE Identification**

<b>Original TOE</b>	<b>RICOH IM 370 version E-1.00-H</b>
<b>Maintained TOE</b>	<b>RICOH IM 370 version E-1.00-H</b>
<b>Developer</b>	<b>Ricoh Company, Ltd.</b>

### 2.1 AFFECTED DEVELOPER EVIDENCE

Modifications to the following developer evidence that was previously submitted in support of the original evaluation is as follows:

- The TOE ST has been corrected to show that RSA rather than ECDSA is used for trusted update of the Operation Panel software and applications.
  - ST version, date and document history updated.
  - Table 5 updated to remove ECDSA from RICOH Cryptographic Library 3
  - Table 30 rows updated as follows:
    - Operation Panel Software: Replace ECDSA with RSA 186-4
    - Operation Panel Applications: Remove ECDSA

### 3 CONCLUSIONS

As all the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance maintenance and re-evaluation is not required.

The assurance maintenance of the TOE has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions are consistent with the evidence adduced. This is not an endorsement of the IT product by the Cyber Centre or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the Cyber Centre or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.



## 4 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, V3.1, February 2024
Certification Report RICOH IM 370 version E-1.00-H, 8 December 2023, v1.0
Security Target RICOH IM 370 version E-1.00-H, 16 September 2024, v1.1
Impact Analysis Report RICOH Luffy MF-1 (626-LSS, 627-LSS) and Metis MF-4 (617-LSS), 26 September 2024, v1.0

