Organisation intergouvernementale pour les transports internationaux ferroviaires
Zwischenstaatliche Organisation für den internationalen Eisenbahnverkehr
Intergovernmental Organisation for International Carriage by Rail

INTERNATIONAL INSTITUTE FOR THE UNIFICATION OF PRIVATE LAW
INSTITUT INTERNATIONAL POUR L'UNIFICATION DU DROIT PRIVE

PREPARATORY COMMISSION FOR THE ESTABLISHMENT OF THE INTERNATIONAL REGISTRY FOR RAILWAY ROLLING STOCK PURSUANT TO THE LUXEMBOURG (RAIL) PROTOCOL

Prep. Comm. Rail/12/Doc. 6
Original: English/French
February 2024

12th session
Berne / remote, 7 March 2024

Information and discussion on documents related to the functioning of the Registrar: External Auditor Report

An "External Auditor Report" must be provided to allow the OTIF Secretariat to issue a certificate regarding the functioning of the International Registry as stipulated in Article XII (8) and Article XXIII (1) b) of the Luxembourg Protocol.

A summary of the External Auditor Report is attached. The report was based on test results from 6 February 2024, where testing was conducted from the perspective of an authenticated and unauthenticated user on the internet.

External Audit Summary Report

7 February 2024

DATE: 7 February 2024

TO: Preparatory Commission

FROM: Regulis S.A.

SUBJECT: External Audit Summary

Regulis and its prime subcontractor, ERS, engaged a CREST approved third-party provider to complete a technical security assessment and penetration test on the Registry application. The following memorandum provides summary information regarding the outcome of the assessment.

The provider, BCC Risk Advisory Ltd. (Edgescan) delivered a draft report of its test results on February 6, 2024. To complete the test, the provider followed its 'black-box' web application and server/network assessment approach using testing methodology based on leading industry practice. This uses a combination of automated tools and manual testing techniques to test the web application for security issues without assuming any special knowledge of the hosts or its supporting network.

Testing was conducted from the perspective of:

- An unauthenticated user on the Internet
- An authenticated user on the Internet

The draft report identified four items which will be addressed by ERS in advance of go-live. An additional six, low-risk informational items were also identified for awareness. These items will be integrated into the Registry's continuous improvement plan and be addressed through updates following go-live.

The results of this type of assessment are highly confidential and are not for wide (or public) distribution given the security-related content. As such, the report's executive summary has confidentially been shared with the Secretariat as evidence of the completion of the testing.