UNITED
NATIONS

E

Economic and Social Council

Distr.
GENERAL

TRANS/WP.30/AC.2/2004/1
27 February 2004

ENGLISH ONLY

ECONOMIC COMMISSION FOR EUROPE

INLAND TRANSPORT COMMITTEE

Administrative Committee for the TIR Convention, 1975
(Thirty-sixth session, 5 and 6 February 2004,
agenda item 4 (a) (ii))

ACTIVITIES AND ADMINISTRATION OF THE TIR EXECUTIVE BOARD (TIREXB)

Activities of the TIRExB

Access and use of the International TIR Data Bank (ITDB)

Note by the TIR Secretary

A.   BACKGROUND

1.   At its thirty-first session, the Administrative Committee was informed by the TIR Secretary on the current operation of the ITDB and on progress made in providing on-line access to authorized Customs TIR Focal Points for inquiry procedures. It noted that the secretariat has finalized the development and testing of the system, and was now awaiting a security audit of the system to be conducted, as requested by the Committee. Pending the outcome of the audit, the Committee decided to postpone the decision to launch the system until its thirty-sixth session in February 2004 (TRANS/WP.30/AC.2/71, para. 27).

B.   SECURITY AUDIT

2.   The security audit of the system allowing on-line access of authorized Customs TIR Focal Points for inquiry procedures to the ITDB, the so-called ITDBonline, has taken place from 12 to 14 January 2004. The report of the audit has been made available on 30 January 2004. The

complete report can obviously not be made public without compromising the security of the system. Therefore, the following paragraphs summarize the results of the audit.

3.   The mandate of the auditors was to estimate the robustness of the ITDBonline application and the risk factors identified for application such as the ITDBonline are:

- The probability that data could be read by non-authorized 3rd parties, either directly, or in transit;
- The probability of data editing;
- The resistance of the system against denial of service attacks.

4.   The following paragraphs (from 5 to 13) are extracted from the management summary of the audit report and are presented as such:

(a)   <u>Probability of data read by non-authorized 3rd parties, either direct, or in transit</u>

After carefully analyzing the output from the report, the current risk of this occurring is very small. The risk will be even further reduced as soon as a few identified issues will be solved.

(b)   <u>Probability of data editing</u>

When the suggestions made in the report are applied, this issue becomes also a very low-risk factor.

(c)   <u>Resistance of the system against denial of service attacks (i.e. probability that users cannot get access to the system after an attack)</u>

There are no issues regarding Denial of Service attacks. The way the system is set-up, especially the firewall configuration, is a good protection against such attacks.

The ITDB-Online application is in its current state ready to be connected to the Internet with a security level which can withstand today's internet climate.

The system's strong security features, like the scratch lists, are comparable to the measures taken by banks for their online banking applications.

Various security enhancements can be put in place to protect the system even more against attacks. Please see the paragraph "Trouble Areas identified" for more details on these enhancements.

Furthermore, suggestions are made in the paragraph "Other Suggestions" to increase even more the robustness of the system.

During the audit, it became clear that great care had been taken to develop a secure and robust system. From our point of view we are confident that after our suggestions are implemented (as far as possible within the scope of the project), the system will be secure and stable.

Care should be taken to re-examine the level of security on a regular basis to assure that the system is still up-to-date with regard to the ever changing climate of attacks and new vulnerabilities.

C.   FURTHER CONSIDERATIONS

5.   In the light of the conclusions made by the auditing company, the Administrative Committee may wish to endorse the launching of the ITDBonline on the Internet, if the secretariat takes the appropriate measures to amend the few issues identified before the launching of the system.

6.   Moreover, the Administrative Committee may wish to take note that a security level that is considered today as sufficient, might become obsolete in the future. Therefore, it is important to regularly enhance the security features to maintain a high security level. These enhancements should, in addition, be followed by security audits in order ensure that security standards are maintained. As a consequence, the Administrative Committee may also consider making appropriate funding available for such tasks in future TIRExB budgets.

7.   Finally, the Administrative Committee may wish to reiterate the importance of Contracting Parties to comply with the provisions of Annex 9, part II of the TIR Convention. Providing updates of the data on TIR carnet holders, if possible on a daily or on a weekly basis, will make the ITDBonline application a tool enhancing the overall sustainability of the TIR procedure. In this respect, the Committee may consider the possibility of further enhancing the ITDBonline by enabling Customs authorities to update their date in the ITDB and mandate the secretariat to present a first feasibility study at one of its future sessions. Once the ITDB would be updated on a real time basis, then the Administrative Committee may wish to enable the consultations of the ITDBonline at Customs offices, directly via the Internet or through their national computer system.

———————————