Excise and Taxation Technical Services Agency

Report on review of Network Security Architecture

December 2007

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 3

2 ENGAGEMENT SCOPE 4

3 LIMITATIONS 5

4 APPROACH & METHODOLOGY 6

5 DETAILED REPORT 7

6 ANNEXURE A - BASIS FOR RISK RATINGS 9

1 Executive Summary

Ernst & Young was engaged by Excise and Taxation Technical Services Agency (henceforth referred to as "ETTSA") to perform a security architecture review of its IT infrastructure. This review was performed on the basis of discussions with the IT infrastructure management team and based on the observations of the threat & vulnerability review performed in November, 2007.

2 Engagement Scope

The scope of work is governed by Task 11 mentioned under Clause 5 of the Agreement dated 20th January 2004 between ETTSA and E&Y relating to the Review of COVIS application deployed by ETTSA, and is as follows:

"E&Y shall perform a security and controls review of the technology components related to the COSTISP and COVIS application environment available at Main Site, DR Site and remaining types of sample sites limited to maximum of 12 sites (covering each type of site) as mutually agreed between the parties. E&Y shall submit Security and Controls Review Report to ETTSA".

3 Limitations

This report is solely for the information of ETTSA management and should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

The gaps identified in this report are based on the technical assessment conducted by us. We made specific efforts to verify the accuracy and authenticity of the information gathered only in those cases where it was felt necessary.

In carrying out our work and preparing the report, we have worked for ETTSA's purposes only. Consequently, we make no representation regarding the sufficiency of the procedures performed either for the purpose for which the report has been requested or for any other purpose.

The recommendations provided in this report should be tested in a test environment prior to implementing in the production environment.

Note:

The threat & vulnerability review was performed as an infrastructure security review without considering the applications hosted on the in-scope infrastructure components. Further, the review did not include the exploitation of any of the identified vulnerabilities to obtain access into the in-scope infrastructure components.

4 Approach & Methodology

The security architecture review of the IT infrastructure consisted of the following activities:

- Review of the network security architecture, domain architecture, and mail architecture.
- Discussions with the ETTSA / the IT infrastructure management team to understand the architecture as well as the flow of information.
- Identify architecture related issues (if any) based on the observations of the infrastructure threat & vulnerability assessment.

5 Detailed Report

S.no.	Priority	Observation	Risk/implication	Recommendation
1.	High	The Local Area Network (LAN) is not segmented. Critical servers hosting sensitive applications reside in the same segment as user desktops.	A compromised desktop of a user puts the critical servers on the same network segment at risk. Malicious users can resort to packet sniffing through ARP spoofing attacks that may allow them to eavesdrop on plaintext server administration / management traffic.	Segment the LAN to ensure distinct segments for servers, management terminals, and user desktops / laptops.
2.	High	Access to critical servers and sensitive infrastructure components (including network devices) is not filtered to restrict access attempts from anyone connected to the LAN.	Any user on the LAN can target services running on critical servers and infrastructure components such as routers. This increases the attack surface exposed by critical servers and infrastructure components.	Access to services running on critical servers and infrastructure components must be restricted to administrators and highly privileged users. Non administrators must not be able to initiate communication with sensitive infrastructure components such as routers. Use host Access Control Lists to restrict access to hosts to specific IP addresses only.
3.	Low	Intrusion Prevention / Detection Systems (IPS / IDS) are not deployed to protect critical servers.	Attack attempts targeting critical servers will go undetected. Hostile traffic directed at critical servers will not be detected and truncated in a timely manner.	Deploy Host IDS on critical servers. Segment the network into zones of differing security. And deploy Network based IDS / IPS to protect sensitive network segments.

S.no.	Priority	Observation	Risk/implication	Recommendation
4.	Low	Servers hosting critical applications and containing sensitive data are part of the corporate domain itself.	Connections between the corporate users and the Internet or possible remote access through modem pools may potentially render critical servers to attacks direct from the Internet. Further, internal threats from malicious users cannot be completely ruled out. Virus and worm outbreak in the corporate network may pose a serious challenge as well.	Sensitive applications and associated data must be moved out of the corporate domain that serves the users / employees of the organization.

6 Annexure A - Basis for risk ratings

"Risk Rating" provides an indication of the level of severity associated with the corresponding observation. In general, the following factors are considered to arrive at the risk rating for a vulnerability:

- *Impact* – The extent to which an attacker may gain access to a system and the severity of it on the organization
- *Popularity* – Describes the existing or potential frequency of exploitation of the vulnerability
- *Simplicity* – The amount of effort required to exploit the vulnerability.

Table 1: Risk Rating Criteria

Risk Rating	Level of severity
High	➢ ***Impact:*** Vulnerability noted on the affected IT asset can be exploited to • Obtain remote privileged or unprivileged access, and/or • Cause severe impact to system operations. ➢ ***Popularity:*** Exploit techniques are well known and the circumstances under which the attack may occur are very common. ➢ ***Simplicity:*** Exploit techniques can be easily obtained and executed by unskilled attackers.
Medium	➢ ***Impact:*** Vulnerability noted on the affected IT asset can be exploited to obtain limited user privileges or network level access. ➢ ***Popularity:*** Exploit techniques are fairly well known and the circumstances under which the attack may be successful are common. ➢ ***Simplicity:*** Exploit techniques can be easily obtained and executed by persons with general computer security knowledge.
Low	➢ ***Impact:*** Vulnerability noted on the affected IT asset provides little or no chance for exploitation. ➢ ***Popularity:*** Exploit techniques are not widely known and the circumstances under which the attack may be successful are rare. ➢ ***Simplicity:*** Exploit techniques are difficult to obtain and/or execute, and requires detailed computer security knowledge and experience.

In addition to the above, the following factors were also considered for grading the risk:

- Risk(s) perceived by generally accepted leading practices and/or software vendor for non-conformance to the recommended practice / security settings
- Existence and adequacy of compensating controls.

ERNST & YOUNG PVT. LTD.