INSPECTOR GENERAL

IG-V-101

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

December 24, 1998

MEMORANDUM

TO: Director, Office of Information Services

FROM: Inspector General Janet Altenhofen

SUBJECT Inspection Report 01-99, Evaluation of the Commission's *Passport* System's Security

The Office of Inspector General (OIG) initiated this inspection in October 1998 at the request of the Director of the Office of Information Services (OIS). The OIS Director requested this assessment because the Commission introduced a new remote-access facility called *Passport* in August 1998.

The objective was to evaluate the security of the *Passport* system and identify potential security risks. We found that, within the limited parameters of this assessment, we were unable to penetrate into the *Passport* system or the system protected by *Passport*. However, certain vulnerabilities were identified that could potentially be exploited to obtain such access.

Passport lets Commission employees who may be working at home or on travel access their e-mail and documents and files that are stored in areas protected by password security. *Passport* also provides access to other selected "internal" computing resources. The application's technical security controls are mainly encryption of all transactions containing password or password protected data. The OIS Director has determined this application secure for data other than National Security Information.

The OIG contracted with the Computer Sciences Corporation (CSC) to conduct a limited vulnerability assessment of the Commission's *Passport* system. Between October 26 and 28, 1998, CSC assessed the vulnerability of the Commission's *Passport* system. From its commercial laboratory site in Maryland, a CSC engineer used proprietary scanning tools and other auxiliary tools to scan the web site and associated firewall to evaluate the general level of security. CSC then attempted to isolate and penetrate the network via *Passport* and obtain access via the *Passport* modem.

Although CSC found no vulnerabilities on *Passport*, CSC identified a number of vulnerabilities on computers in the vicinity of the firewall. CSC suggested that OIS remove the employee names found on the public servers, disable a system and two services, prevent the download of certain files, and remove an option for mail service. The technical results of the inspection are presented in the passport application security evaluation report transmitted with this memorandum.

A draft of this report was sent to the OIS Director on November 24, 1998. The OIS Director, upon reviewing the report in draft form, disabled the system as recommended, and will disable one service. The other suggestions cannot be implemented because the names must be made available, the files are public information, and one system with low risk cannot be separated from the service.

The above procedures constitute an inspection made in accordance with the President's Council on Integrity and Efficiency Standards for Inspections.

If you have any questions, please contact me at 205-2210.

Attachment

cc:. Commission
Office Directors

International Trade Commission
Passport Application Security Evaluation Report

December 14, 1998

Computer Sciences Corporation
Systems Engineering Division
7459A Candlewood Road
Hanover, MD 21076

ITC Sensitive