INSPECTOR GENERAL

IG-W-021

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

April 1, 1999

MEMORANDUM

TO: Director, Office of Information Services

FROM: Inspector General Jane E. Altenhofen

SUBJECT: Inspection Report 03-99, Review of the Electronic Dockets Information System's Security

The Office of Inspector General (OIG) initiated this inspection in March 1998 at the request of the Director of the Office of Information Services (OIS). The Director OIS requested this inspection because the Commission plans to implement a new system commonly referred to as EDIS On-Line.

EDIS On-Line is a component of the Electronic Dockets Information System (EDIS) which the Secretary of the Commission uses to manage the intake and dissemination of Commission public and non-public documents. EDIS On-Line will allow the general public (external users) to access the pubic documents contained in the docket via the Internet while allowing Commission employees (internal users) access to public and non-public documents in the docket via the Commission's Intranet.

The objective was to confirm that external users are restricted to public areas of the EDIS On-Line system and identify potential security risks. We found that, within the limited parameters of this assessment, external users were properly limited to information in the public directories. However, the testing revealed several potential security-related considerations that would enhance the security of EDIS On-Line.

The OIG contracted with the Computer Sciences Corporation (CSC) to conduct a vulnerability assessment of EDIS On-Line. In March 1999, a CSC engineer inspected the network architecture and configuration of EDIS On-Line, and from its commercial laboratory site in Maryland, used proprietary scanning tools and other auxiliary tools to perform several tests on EDIS On-Line. The testing was comprised of initial port scanning, Hydra vulnerability scanning, access control testing, and web site mapping.

CSC suggested changes that would enhance the security of EDIS On-Line. These include limiting the number of unsuccessful authentication attempts, separating public and non-public data on separate servers, increasing access controls, upgrading a software no longer in production to an active one, considering the use of a commercial product to control access to information, implementing a checking mechanism for all external variables, and limiting access to internal printers to internal users.

A draft of this report was sent to the Director OIS on March 22, 1999. The Director OIS implemented three of CSC's suggestions immediately on limiting authentication attempts, checking external variables and limiting printer access. He is planning to incorporate the suggestions on separating data and purchasing software in active development as a part of planned upgrades. He is evaluating the feasibility of the remaining two suggestions.

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