TD P 15-71

# Controls Over the LexisNexis Connection Should Be Improved to Better Deter and Detect External Attacks

**March 2002**

**Reference Number: 2002-20-063**

TD P 15-71

INSPECTOR GENERAL
for TAX
ADMINISTRATION

**DEPARTMENT OF THE TREASURY**
WASHINGTON, D.C. 20220

March 28, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION & CHIEF INFORMATION OFFICER

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Controls Over the LexisNexis Connection Should Be Improved to Better Deter and Detect External Attacks (Audit # 200120038)

This report presents the results of our review of the effectiveness of controls to deter and detect external computer attacks at the Internal Revenue Service's (IRS) LexisNexis connection. We performed this review to comply with the IRS Restructuring and Reform Act of 1998,[1] which requires the Treasury Inspector General for Tax Administration (TIGTA) to assess the security of IRS technology.

In summary, the IRS provides its employees direct electronic access to the LexisNexis[2] research service. This connection enables authorized employees, without Internet capabilities, to access the research service's collection of reference libraries. Because the connection links the IRS network with a private vendor, there is an external risk that an unscrupulous employee from LexisNexis or a hacker who had access to the LexisNexis computer system could gain access to the IRS network. There is also an internal risk that a contractor or IRS employee could gain access to sensitive data. We found that the IRS had not taken sufficient actions to secure the LexisNexis connection.

---

[1] The IRS Restructuring and Reform Act, Pub. L. No. 105-206, 112 Stat. 685 (1998).

[2] The LexisNexis Group provides information to legal, corporate, government and academic markets and publishes legal, tax and regulatory information, via online, hardcopy print and CD-ROM formats.

The IRS had not installed a comprehensive firewall system at the LexisNexis connection to *deter* unauthorized accesses. The Telecommunications Division had determined that a firewall was needed, but had not implemented it. The only protection device at this connection was an external router. The primary function of a router is to direct electronic traffic to the appropriate destination (i.e., an employee's workstation or the LexisNexis data network). Although the router can provide some protection, a router by itself is generally not considered an effective control against intruders.

Also, contractors operating the router had not documented configuration changes. When configuration changes are not tracked, an unauthorized person who gained access to the router could access sensitive systems then change the configurations back without being detected. We also found no documentation of background investigations of contractors or employees who had access to the router.

In addition, an intrusion detection system had not been installed at the LexisNexis connection to *detect* unauthorized accesses. The IRS was in the process of installing intrusion detection on external connections, but had not decided if the LexisNexis connection warranted the placement of intrusion detection sensors in the immediate future.

Because of these weaknesses, the IRS was unnecessarily vulnerable to attack through the LexisNexis connection, and the IRS cannot state with confidence that its sensitive data had not been compromised. If unauthorized persons had gained access to the internal network, they could have caused damage in many ways, such as obtaining confidential taxpayer information, planting virus programs, or hindering network performance by causing a denial of service.

Findings similar to the documentation of configuration changes and background investigations discussed in this report have been presented in a previous TIGTA report titled, *Controls Over the Internet Gateway Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2001-20-101, dated June 2001). If recommendations in that report are implemented at the LexisNexis connection, these conditions we cite will be corrected. As such, we have not restated those recommendations. To address our other findings, we recommend that the Director, Telecommunications, implement a comprehensive firewall and intrusion detection system at the LexisNexis connection.

Management's Response: The Deputy Commissioner for Modernization and Chief Information Officer temporarily transferred responsibility of firewall and intrusion detection infrastructure from the Office of Telecommunications to the Office of Mission Assurance within Security Services. Also, a firewall computer has been installed at the connection between the IRS and LexisNexis.

Office of Audit Comment: Management's response did not address the implementation of intrusion detection at the LexisNexis connection, as recommended in our report.

However, an IRS Cyber-Security official verbally informed us that intrusion detection has been installed at this connection in addition to the firewall computer.

TIGTA has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within TIGTA's Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs) at (202) 622-8510.

# Table of Contents

Background ..... Page 1

The LexisNexis Connection Was Not Protected by a Firewall ..... Page 1

Access Controls Need Strengthening at the LexisNexis Connection ..... Page 2

An Intrusion Detection System Had Not Been Installed at the LexisNexis Connection ..... Page 3

Recommendation 1: ..... Page 4

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 6

Appendix II – Major Contributors to This Report ..... Page 7

Appendix III – Report Distribution List ..... Page 8

Appendix IV – Management's Response to the Draft Report ..... Page 9

# Controls Over the LexisNexis Connection Should Be Improved to Better Deter and Detect External Attacks

## Background

The Internal Revenue Service (IRS) created a dedicated connection between its network and the LexisNexis research service in 1999 at the Detroit Computing Center (DCC). This connection allows authorized employees, without Internet access, the ability to use the LexisNexis service. The LexisNexis Group provides information to legal, corporate, government and academic markets and publishes legal, tax and regulatory information via online, hardcopy print and CD-ROM formats. The IRS uses this service to access a variety of reference libraries pertinent to tax administration (e.g., tax code and tax-related legislation).

Because this connection links the IRS with a private vendor, it provides an entry point into the IRS' network. While this external risk is lessened because the connection is not readily accessible by anyone outside the IRS and LexisNexis, an unscrupulous LexisNexis employee or a hacker who had access to its computer system could gain access to confidential taxpayer information. There is also an internal risk that a contractor or IRS employee could gain access to sensitive data.

We performed this review to comply with the IRS Restructuring and Reform Act of 1998,[1] which requires the Treasury Inspector General for Tax Administration (TIGTA) to assess the security of IRS technology. This review was conducted at the DCC and the IRS office in New Carrollton, Maryland, from July to October 2001. This audit was performed in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

## The LexisNexis Connection Was Not Protected by a Firewall

To deter unwanted attacks, the National Institute of Standards and Technology (NIST)[2] recommends that a computer connection between two separate entities be

[1] The IRS Restructuring and Reform Act, Pub. L. No. 105-206, 112 Stat. 685 (1998).

[2] NIST is a Department of Commerce organization designed to provide guidance for federal agencies relating to Information Systems areas.

protected by a firewall system (routers and firewall computers). The firewall system serves as a barrier mechanism, barring entry to some kinds of network traffic and allowing others, based on a firewall policy.[3] In addition, the Department of the Treasury requires that any connection to Treasury systems must occur through a firewall system.

The IRS had not installed a comprehensive firewall system at the LexisNexis connection. The Telecommunications Division had determined that a firewall was needed at this connection, but had not implemented it. The only protection device at the LexisNexis connection was an external router. Generally, the primary function of a router is to direct electronic traffic to the appropriate destination (i.e., an employee's workstation or the LexisNexis data network). Routers can provide some level of protection because configuration tables in the router can be set to dictate how to handle various types of traffic.

The IRS configured its external router at the LexisNexis connection to generally deny all traffic unless specifically permitted. However, the router by itself does not provide sufficient traffic filtering to prevent hackers from gaining access into the IRS networks and, potentially, sensitive data and systems. As such, a router alone is generally not considered an effective control against intruders.

## Access Controls Need Strengthening at the LexisNexis Connection

IRS procedures require that router configuration changes be authorized and documented. This documentation helps provide assurance that only authorized changes are made to the router. In addition, if a router administrator resigns or is otherwise unavailable, this documentation enables an experienced individual to rapidly assume administration of the router.

We did not find any documentation of changes to the router at the LexisNexis connection. Without tracking changes to

[3] NIST provides two publications on firewalls and intrusion detection systems: *Special Publication 800-10: An Introduction to Internet Firewalls* and *Draft Special Publication on Intrusion Detection Systems.*

the router's configurations, the IRS has no assurance that only authorized changes had been made to the router configuration. If a hacker had gained access to the router, he or she could have changed the configuration settings to access sensitive files, and then changed them back without being detected.

The maintenance of router configuration change logs is the responsibility of the contractor assigned to administer the router. However, the contractor did not do so, and the Telecommunications staff did not provide oversight to ensure that logs were maintained.

In addition, IRS employees and contractors must have approved authorization forms and background investigations on file before they can access automated systems. The IRS was not able to provide authorizations for accessing the router nor was it able to provide evidence that background investigations had been conducted for individuals with access to the router. These individuals include the entire IRS Network Management Center staff and an administrator in DCC. Management did not ensure these forms were completed and retained. As a result, there was no assurance that access to the router was kept to a minimum and that those with access were not security risks.

If hackers had gained access to the internal network, they could have caused damage in many ways, such as accessing sensitive files from any system on the network, planting virus programs, or hindering network performance by causing a denial of service.

## An Intrusion Detection System Had Not Been Installed at the LexisNexis Connection

To detect unwanted attacks, the NIST recommends that each computer connection between two entities be protected by an Intrusion Detection System (IDS). An IDS serves as a monitoring mechanism. It watches activities occurring in a computer system or network and analyzes them for signs of intrusions.

The IRS had not installed an IDS at the LexisNexis connection. The IRS was in the process of installing intrusion detection on external connections, but had not

decided if this connection warranted the placement of IDS sensors in the near future.

Without an IDS, the IRS has limited ability to recognize and respond to external intrusion events at the LexisNexis connection. It cannot detect and deal with preambles to attacks, including sharing such information with other government sources. The absence of intrusion detection can also hinder the IRS' ability to fully investigate intrusions. As a result of this deficiency, the IRS could not state with confidence that the LexisNexis connection has kept hackers out of its internal network.

## Recommendation

In the TIGTA report, *Controls Over the Internet Gateway Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2001-20-101, dated June 2001), we made recommendations to address the lack of external connection security policies and procedures and the need for better compliance with IRS procedures on computer access requirements and router configuration changes. The Director, Office of Security, agreed with our recommendations and proposed corrective actions to address those issues which will also correct the similar issues cited in this report. As such, we have not repeated the same recommendations.

1. The Director, Telecommunications, should implement a comprehensive firewall and IDS at the LexisNexis connection.

Management's Response: The Deputy Commissioner for Modernization and Chief Information Officer temporarily transferred responsibility of firewall and intrusion detection infrastructure from the Office of Telecommunications to the Office of Mission Assurance within Security Services. Also, a firewall computer has been installed at the connection between the IRS and LexisNexis.

Office of Audit Comment: Management's response did not address the implementation of intrusion detection at the LexisNexis connection, as recommended above. However,

an IRS Cyber-Security official verbally informed us that intrusion detection has been installed at this connection in addition to the firewall computer.

**Appendix I**

## Detailed Objective, Scope, and Methodology

The objective of this review was to evaluate the effectiveness of controls to deter and detect external attacks at the Internal Revenue Service's LexisNexis connection. To accomplish our objective, we conducted the following tests.

I. Reviewed background information on the establishment and use of the connection.

II. Determined whether a firewall, router, and intrusion detection system were appropriately deployed and distributed to ensure they were effectively providing the intended security protections.

III. Evaluated the component configurations to ensure only authorized traffic flowed through the component.

IV. Evaluated the logical access controls in place to ensure the components adequately identified and authenticated users.

V. Evaluated account controls in place to ensure the components were adequately protected by limiting access to users with a need to know.

VI. Evaluated the security surveillance controls in place to ensure the components adequately logged systemic activities and that logs were reviewed to identify any inappropriate access.

Appendix II

## Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Bret Hunter, Senior Auditor
Dave Hodge, Auditor

**Appendix III**

## Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Director, Telecommunications M:I:T
Director, Office of Security M:S
Director, Detroit Computing Center M:I:E:DC
Director, Servicewide Policy, Directives & Electronic Research N:ADC:R:SPDER
Deputy Chief Financial Officer, Department of the Treasury

Appendix IV

## Management's Response to the Draft Report

:PUTY COMMISSIONER

LIMITED OFFICIAL USE
DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
MAR 2 2 2002

March 20, 2002

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: John C. Reece
Deputy Commissioner for Modernization &
Chief Information Officer

SUBJECT: Response to Draft Report – Controls Over the LexisNexis Connection Should Be Improved to Better Deter and Detect External Attacks (200120038)

Thank you for the opportunity to review and comment on your draft report and report recommendation concerning our controls at the IRS LexisNexis connection.

It is our management goal to continually strive for an enhanced security program that effectively manages risks. In this regard, we have reorganized and have transferred responsibilities of the firewall and intrusion detection infrastructure from the Office of Telecommunications to the office of Mission Assurance, within Security Services. This became effective in a Memorandum of Understanding dated May 31, 2001, and is in effect until September 30, 2003, when responsibility will revert back. This change is reflected in our attached response to your report recommendation.

We appreciate your comments that will further assist us in strengthening our firewall system. If you have any questions and/or concerns, please feel free to contact me at (202) 622-6800 or Mr. Len Baptiste, Director, Security Services at (202) 622-8910.

Attachment

LIMITED OFFICIAL USE

**Management response to Draft Audit Report –Controls Over the LexisNexis Should Be Improved to Better Deter and Detect External Attacks**

**RECOMMENDATION #1:**

The Director, Telecommunications, should implement a comprehensive firewall and intrusion detection system at the LexisNexis.

**ASSESSMENT OF CAUSE:**

IRS did not have a comprehensive firewall and Intrusion Detection System.

**CORRECTIVE ACTION TO RECOMMENDATION #1:**

Effective May 31, 2001, firewall management and intrusion detection were transferred to the Office of Mission Assurance from the Office of Telecommunications. On March 7, 2002, a VelociRaptor firewalls was installed on the T1 connection between the IRS and Lexis-Nexis. The firewall is being centrally managed by Mission Assurance, and IRS is working with Lexis-Nexis to limit traffic to only those network/system services deemed absolutely necessary.

**IMPLEMENTATION DATE:**

June 1, 2002

**RESPONSIBLE OFFICIAL:**

Director, Office of Mission Assurance