

United States Department of Interior

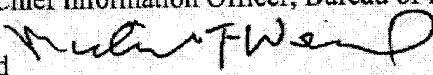
Office of Inspector General
Washington D.C. 20240

APR - 6 2005

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

Memorandum

To: W. Hord Tipton, Chief Information Officer, Department of the Interior
Ronnie Levine, Chief Information Officer, Bureau of Land Management

From: Michael F. Wood 
Assistant Inspector General
for Administrative Services and Information Management

Subject: OIG Report "NSM-EV-BLM-0020-2005-Penetration Testing" External
Penetration Testing of Bureau of Land Management

Background

As part of the Inspector General's Federal Information Security Management Act responsibilities, penetration testing was conducted on the Bureau of Land Management (BLM) from February 21, through March 11, 2005. The purpose of the testing was to identify, attempt exploitation, and document vulnerabilities that could be used to gain access to BLM's systems and to evaluate BLM's incident response capabilities. Our findings are presented in two reports. The first report is a high level summary for non-technical managers and the second is a detailed technical report for security officers, system and network administrators.

Summary of Testing

Testing was conducted under the protocols agreed to within the Rules of Engagement (ROE) between the Office of Inspector General (OIG) and the Department of the Interior (DOI) Office of the Chief Information Officer (OCIO). BLM was not advised of the testing. The OCIO provided the OIG test team with sensitive information that would not normally be available to an outside entity. However, the OIG chose not to utilize the information and conducted its testing to best resemble a real Internet based attack. As a result we identified seven additional network address ranges not included in the DOI provided list. Our testing identified a large network that could support 65,535 possible devices. Sixty-six different services, such as web browsing, email, and file

transfer protocol, are accessible from the Internet. Our Internet research revealed 50 web sites publishing some 450,000 pages intended for public use¹.

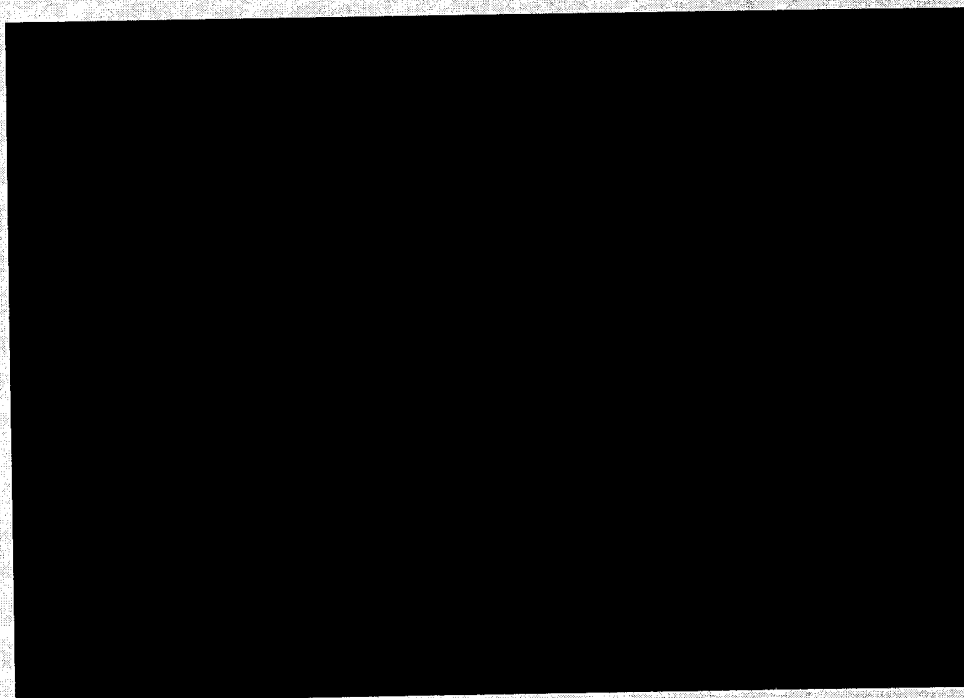
Findings

The OIG's penetration testing expanded on the SANS (SysAdmin, Audit, Network, and Security) Top 20 vulnerabilities. Our testing of BLM revealed a number of issues that place the BLM network at a fairly high risk of unauthorized access from the Internet. OIG's penetration testing of BLM's [REDACTED] resources uncovered [REDACTED]

[REDACTED] Consequently, the OIG was able to penetrate BLM's internal networks [REDACTED] to discover and establish connections to servers or systems purporting to contain Indian Trust data. Please reference the Potential Notice of Findings and Recommendations (NSM-EV-BLM-0020-2005-NFR) for more information. Given the sensitivity of Indian Trust systems, and court orders protecting data that resides within them, the OIG carried out no further testing that could jeopardize BLM's Indian Trust systems. No information was collected or manipulated, and no system was compromised. While we were detected twice by BLM [REDACTED]

The most critical vulnerabilities are noted below:

-
-
-
-
-
-
-



¹ See OIG Report 2003-I-0051, "Moving To a Customer-Centered Web Presence", for recommendations on improving and securing DOI's web presence.

-
-

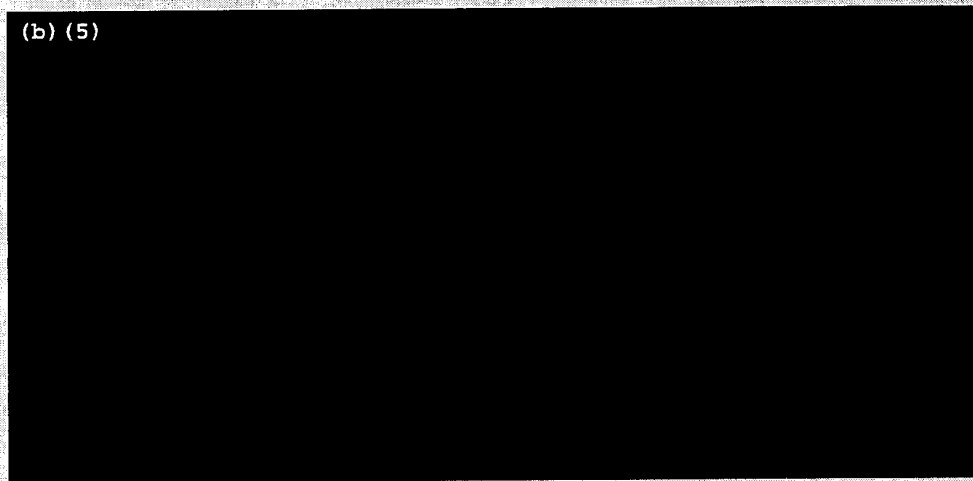


Extensive details, analysis and recommendations are provided in the accompanying technical report.

Recommendations

Implement all corrective actions and recommendations noted within the report, such as:

- (b) (5)



Please provide a report documenting what corrective actions have been taken to address the vulnerabilities detailed in the technical report. A copy of your response should be forwarded to this office by May 6, 2005. Vulnerabilities and their associated recommendations should be managed through the existing Plan of Actions & Milestones process.

Attachment

cc: Associate Deputy Security, James E. Cason
Bureau Director, Bureau of Land Management – Kathleen Clarke