Office of the Inspector General
Notification of Potential Finding and Recommendations

SENSITIVE BUT UNCLASSIFIED INFORMATION

Sensitive-But-Unclassified Information. Protect From Unauthorized Disclosure. This document requires Administrative Control. This is not a classified document, however it warrants physical protection and control.

Warning

The enclosed document(s) is (are) property of the United States Government. Release of or disclosure of the contents is prohibited. Contents may be disclosed only to persons whose official duties require access hereto. Remove this cover prior to external transmission or destruction of the document. Copying, dissemination, or distribution of these materials to unauthorized users is prohibited.

FOR OF
Sensitive-But-

Office of the Inspector General
Notification of Potential Finding and Recommendations

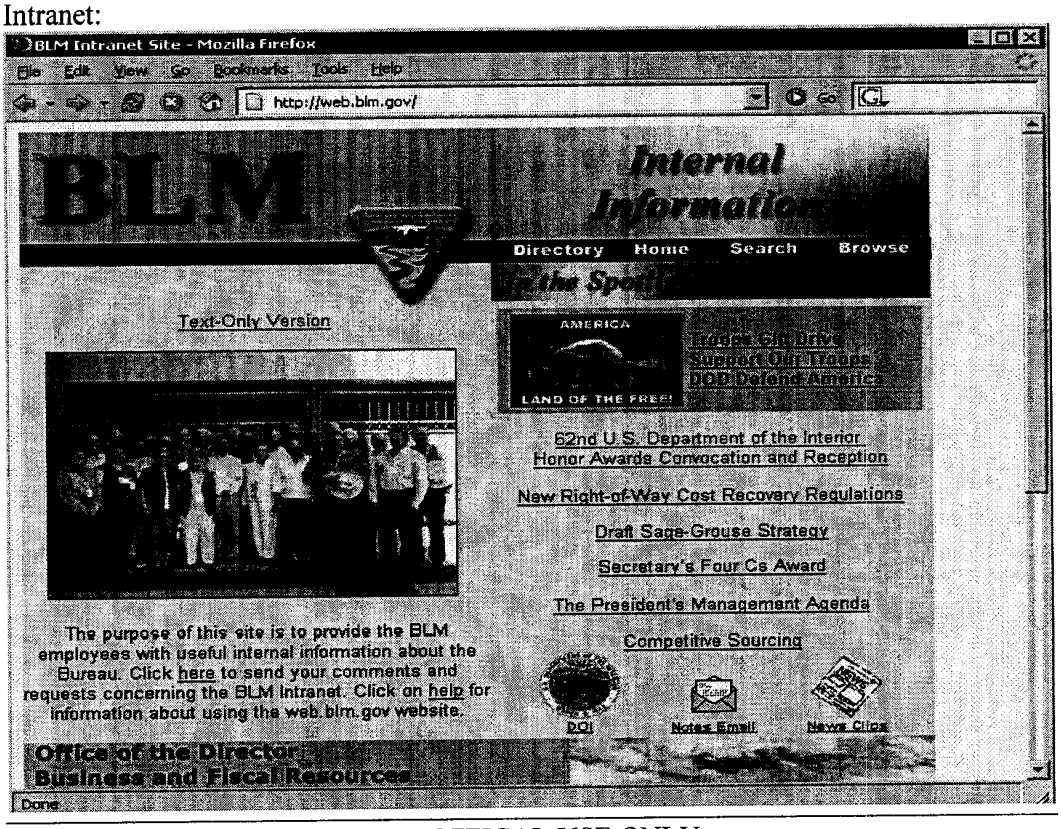
Finding: BLM Indian Trust Systems Vulnerable to Unauthorized Internet Access

Date Finding Provided: April 5, 2005

Date Response Due: April 15, 2005

Summary: As part of the Inspector General's Federal Information Security Management Act responsibilities, penetration testing was conducted on the Bureau of Land Management's (BLM) networks from February 21 through March 11, 2005. The OIG was able to penetrate BLM's internal networks from the Internet and masquerade as authorized users to discover and establish connections to servers purporting to contain Indian Trust data. 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. We did not validate the existence of any Indian Trust data on these systems.

Background: We were able to penetrate two servers that provided us full, undetected access to BLM's internal networks and Intranet. See below for a screen shot of BLM's Intranet:



Using a [redacted] User id gathered from previous hacking activities, we were able to access [redacted] known as [redacted] shown below.

(b) (5)

[redacted]

Based on information provided in this database we were able to determine that there were presently 24 systems/servers identified that contained Indian trust data. We then looked [redacted] ablished connections from the [redacted] servers to the following BLM

[redacted]

See below for screen shots of the database-- [redacted] detailing which systems contain Indian Trust data:

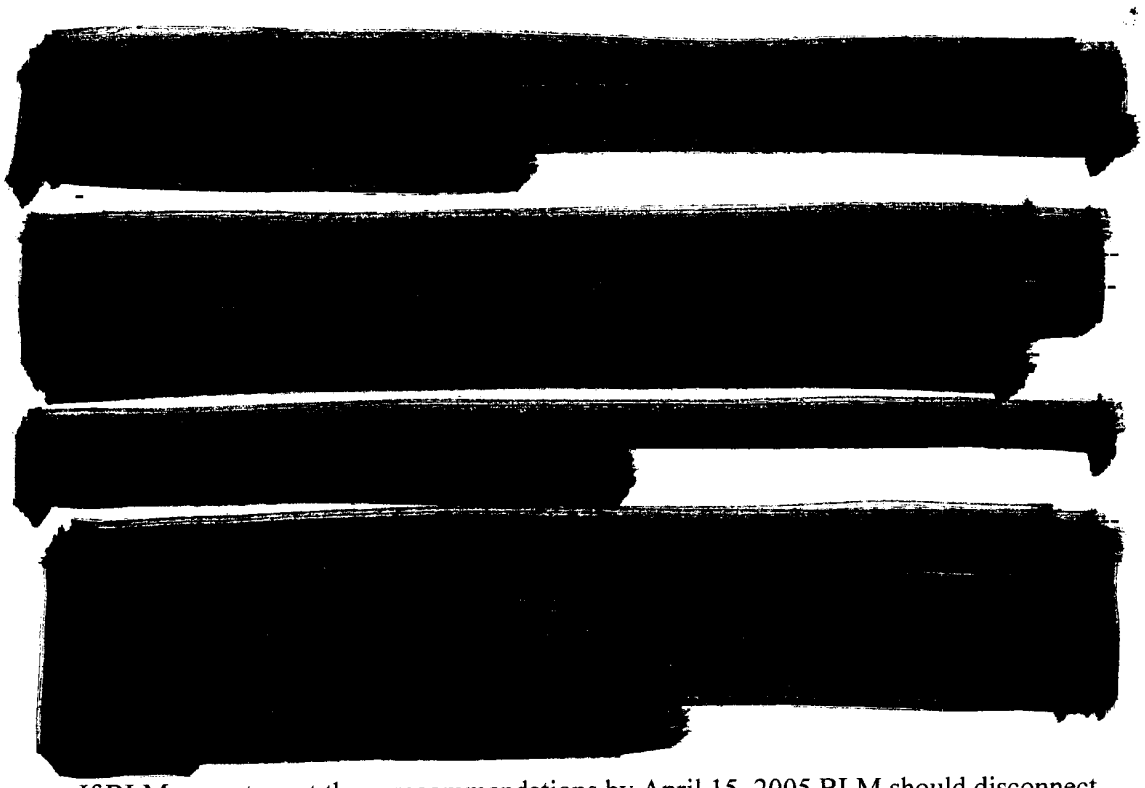
(b) (5) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]



If BLM cannot meet these recommendations by April 15, 2005 BLM should disconnect any existing network access to their Indian Trust systems.

Receipt

_____
DOI Official Signature

_____Date

Management concurs with the Notification of Finding and Recommendation:

Yes/No

MANAGEMENT'S RESPONSE

