

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
	)	No. 1:96CV01285
Plaintiffs,	)	(Judge Lamberth)
v.	)	
	)	
DIRK KEMPTHORNE, Secretary	)	
of the Interior, et al.,	)	
	)	
Defendants.	)	
_____	)	

**DEFENDANTS' NOTICE TO THE COURT OF  
RESTORATION OF BLM'S NATIONAL TRUST SYSTEMS  
TO THE INTERNAL NETWORK FOR OPERATIONAL USE**

Subsequent to the "Notification of Potential Finding and Recommendation" issued by the Office of the Inspector General for the Department of the Interior ("OIG") on April 6, 2005, the Bureau of Land Management ("BLM") took actions to mitigate risks to the BLM network and to ensure the integrity of Individual Indian Trust Data maintained by BLM. By this notice, Defendants advise the Court that, as a result of progress made in developing and implementing its plan to address the issues identified in the OIG report, BLM restored its National Trust Systems to BLM's internal network for operational use on June 2, 2006. BLM's National Trust Systems consist of the Indian Automated Fluid Minerals Support System ("IAFMSS") and the Alaska Land Information System ("ALIS").

As described in the attached declaration and enclosures submitted by Ronnie Levine, Chief Information Officer for BLM, BLM has implemented the substantive actions set forth in Ms. Levine's April 18, 2005 declaration (Items 4 through 9), filed with Defendants' Opposition to Plaintiffs' Consolidated Motion for Temporary Restraining Order and Preliminary Injunction (Docket # 2933), to ensure that the OIG's findings were adequately addressed.

Dated: June 2, 2006

Respectfully submitted,

PETER D. KEISLER  
Assistant Attorney General  
STUART E. SCHIFFER  
Deputy Assistant Attorney General  
J. CHRISTOPHER KOHN  
Director

/s/ Robert E. Kirschman, Jr.  
ROBERT E. KIRSCHMAN, JR.  
(D.C. Bar No. 406635)  
Assistant Director  
GLENN D. GILLET  
Trial Attorney  
JOHN WARSHAWSKY  
(D.C. Bar No. 417170)  
Trial Attorney  
Commercial Litigation Branch  
Civil Division  
P.O. Box 875  
Ben Franklin Station  
Washington, D.C. 20044-0875  
Telephone: (202) 616-0328  
Facsimile: (202) 514-7162

CERTIFICATE OF SERVICE

I hereby certify that, on June 2, 2006 the foregoing *Defendants' Notice to the Court of Restoration of BLM's National Trust Systems to the Internal Network for Operational Use* was served by Electronic Case Filing, and on the following who is not registered for Electronic Case Filing, by facsimile:

Earl Old Person (*Pro se*)  
Blackfeet Tribe  
P.O. Box 850  
Browning, MT 59417  
Fax (406) 338-7530

/s/ Kevin P. Kingston  
Kevin P. Kingston

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, etc al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 1:96CV01285
	)	(Judge Lambert)
DIRK KEMPTHORNE, Secretary of the Interior,	)	
et al.,	)	
	)	
Defendants	)	
<hr/>		

DECLARATION OF RONNIE LEVINE

1. I, Ronnie Levine, am the Assistant Director, Information Resources Management, and Chief Information Officer for the Bureau of Land Management, United States Department of the Interior (“BLM”). In this capacity, I oversee management of the Information Technology (“IT”) systems under the control and custody of BLM in accordance with applicable Department of the Interior policies and directives. I also coordinate with the Denver National Information Resources Management Center (“NIRMC”) on IT security and other matters concerning BLM IT resources. In performing my duties, I rely upon information from BLM management and staff to make management decisions and to prepare communications with the Court, as is the case with this Declaration.
2. This Declaration references “Declaration of Ronnie Levine, BLM Chief Information Officer (CIO) of April 18, 2005.” BLM has implemented all of the actions contained in that

Declaration under Items 4 through 9, which include multiple architectural and procedural changes to enhance overall network security.

3. BLM has continued to investigate risk mitigation strategies to further protect IITD and Trust Systems. BLM has two Trust systems. These are the Automated Fluid Minerals Support System (AFMSS) and the Alaska Land Information System (ALIS). BLM has undertaken systems development efforts to effectively split the AFMSS application into two physically and functionally separate systems. Due to the original design considerations used in constructing AFMSS, the geographical location of the Field Offices allowed for a partitioning of the structural database into two distinct systems. These are the Indian AFMSS, hereinafter referred to as IAFMSS, and non-Indian AFMSS, hereinafter referred to as AFMSS, application data processing systems. Essentially, any field office which has Trust responsibilities will utilize IAFMSS. The remaining BLM offices which have no Trust responsibilities will utilize AFMSS. Due to the design of the ALIS application, it is not practical to segregate Trust information; therefore, ALIS will retain its current form as one system.
4. BLM has acquired and placed into service high end, state-of-the-practice network and application security intrusion detection system devices specifically to protect and monitor IAFMSS and ALIS. This adds another layer of security and protection to those applications. BLM has also, as of the date of this Declaration, established and tested a new De-Militarized Zone (DMZ) for all external web services in operational status.
5. BLM acquired the services of the firm SPI Dynamics to perform a Web application assessment of [www.blm.gov](http://www.blm.gov) for the purpose of determining whether or not its Web application contains vulnerabilities that could be exploited by unauthorized parties. SPI

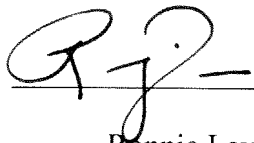
Dynamics rated the web site with its highest rating of “Secure.” They note in a cover letter of February 6, 2006, that: “This is the highest rating that SPI Dynamics can recommend.”

6. Item 10 of my Declaration of April 18, 2005 states: “The Trust Servers will not be allowed to reconnect to the BLM internal network until the new DMZ has been successfully established, tested, (and) the OIG determines that potential vulnerabilities have been adequately addressed.”
7. Accordingly, on February 23, 2006, BLM’s Director sent a Memorandum to the Inspector General inviting that Office to inspect and test the implementation of BLM’s IT security improvements to determine that the potential vulnerabilities identified in their previous penetration testing were in fact adequately mitigated. Attached hereto as Exhibit A is a true and correct copy of that Memorandum.
8. By Memorandum dated March 2, 2006, OIG declined to conduct that review due to ongoing workloads. OIG did offer to: “independently review the penetration test results of any qualified IT contractor.” Attached hereto as Exhibit B is a true and correct copy of that Memorandum.
9. BLM contracted the services of Sword and Shield Enterprise Security Inc., (<http://www.sses.net>) to perform additional IT security testing of the external network perimeter and national Trust applications security implementation. BLM provided Sword and Shield with IP addresses of the target hosts to test if they could access specified hosts from the untrusted (public) Internet. BLM's externally facing Information Technology Security Architecture is composed of the Intrusion Prevention Systems (IPS), the Cisco PIX firewalls, the Cisco routers, and the Net Continuum application layer gateways. This is also referred to as the BLM Exterior Perimeter Network (EPN).

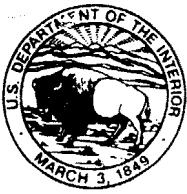
10. SSES testing was initiated May 5, 2006. SSES was quickly detected and completely blocked by the DOI Enterprise Services Network (ESN) Internet facing security systems. BLM worked with DOI to have the ESN blocks removed so the third party (SSES) testing could continue. After being passed through the DOI ESN perimeter, SSES was detected and quarantined twice by the BLM's DOI ESN facing security systems in the EPN. After an adequate period of testing, SSES determined they were completely shutout and requested that BLM have all of the quarantines removed. SSES then continued to attack without success the BLM EPN, with all blocks removed, until they had determined that they could get no further into the BLM network and declared that the external tests were completed with no weakness or vulnerabilities. SSES then conducted internal penetration testing on IAFMSS and ALIS. The internal test consisted of multiple attempts to gain access to target hosts in accordance with the Rules of Engagement authorized by the BLM. This included performing penetration tests and scans on target hosts containing Trust Data. Sword and Shield has concluded their testing. No weaknesses or vulnerabilities were found.
11. A copy of the SSES test report was provided to DOI-OIG. Thereafter, Scott MacPherson (Acting Deputy CIO and Indian Trust Program Manager) and I met with DOI-OIG representatives on Friday May 19, 2006 and discussed their review of our penetration testing. OIG indicated in that meeting that they plan to conduct significant testing on BLM's Information Technology (IT) security in FY 2007.
12. Due to the mission critical needs of implementing the Energy Policy Act, BLM will re-connect IAFMSS and ALIS to the Internal Network and re-establish operational use of those systems.

13. Based upon these actions, I am providing this new Declaration with the District Court. This Declaration informs the Court of BLM's actions and intent to re-establish operational use of BLM's National Trust Systems as of June 2, 2006.

I declare under penalty of perjury that the foregoing is true and correct, to the best of my knowledge, information, and belief.

 6/2/2006  
Ronnie Levine CIO of BLM





# United States Department of the Interior

BUREAU OF LAND MANAGEMENT  
Washington, D.C. 20240  
<http://www.blm.gov>

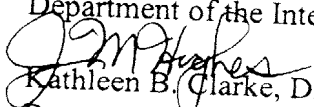
FEB 23 2006



In Reply Refer To:  
1260 (WO500) P

## Memorandum

To: Earl Devaney, Inspector General,  
Department of the Interior, Office of the Inspector General

From:   
Kathleen B. Clarke, Director  
Bureau of Land Management

Subject: Request for Penetration Testing

BLM has two national data processing systems which are critical to effective execution of our energy program. These are the Automated Fluid Minerals Support System (AFMSS) and the Alaska Land Information System (ALIS). Both of these systems include Native American Indian Trust components which have been offline since April 18, 2005 after the penetration testing conducted by your office.

In a Declaration submitted on April 18, 2005 to the Court in *Cobell v. Norton*, Chief Information Officer Ronnie Levine stated that "The Trust Servers will not be allowed to reconnect to the BLM internal network until the new DMZ (De-Militarized Zone) has been successfully established, tested, and the OIG determines that potential vulnerabilities have been adequately addressed."

Since that time BLM has established and tested a new DMZ for all external web services and implemented multiple enhancements to increase the security of the Bureau's IT infrastructure.

Due to the priorities of implementing the Energy Policy Act (EPAct) of 2005, it is imperative that BLM restore services to these two systems on an immediate basis.

Accordingly, we are formally requesting that the Office of Inspector General conduct penetration testing of our external and internal IT security implementation. The Solicitor's Office, in consultation with the Department of Justice, has advised us that the most prudent course of action from a litigation standpoint is to adhere to the intention stated in Ms. Levine's Declaration, that is, to have the testing done by the OIG. Because of the critical need for full use of the two systems, I am requesting that you initiate this testing and review as soon as possible.

**Exhibit A**

Please provide a written response to this Memorandum at your earliest convenience. If you have any questions or comments, please contact Scott E. MacPherson, Deputy (Acting) Associate Director, AD-500 at 202-208-4602.

**Exhibit A**



# United States Department of the Interior

OFFICE OF INSPECTOR GENERAL  
Washington, D.C. 20240

MAR - 2 2006

## Memorandum

To: Kathleen B. Clarke, Director  
Bureau of Land Management

From: Earl E. Devaney  
Inspector General

Subject: Request for Penetration Testing

This is in response to your memorandum of February 23, 2006, requesting that the Office of Inspector General (OIG) conduct penetration testing of the Automated Fluid Minerals Support System (AFMSS) and the Alaska Land information System (ALIS) as soon as possible.

The OIG has extensive information technology (IT) responsibilities throughout the entire Department, pursuant to the Inspector General Act and the Federal Information Security Management Act (FISMA), which we must carry out with extremely limited resources. In order to meet these responsibilities, we develop an annual IT plan that covers the broadest possible scope our small staff and contractors can realistically address. Penetration testing is only one aspect of our overall IT oversight responsibilities. In order to maximize our efforts, our penetration testing must extend beyond individual systems. Furthermore, our penetration testing for the 2006 FISMA reporting period is already well underway.

While the OIG may be the preferred entity to conduct penetration testing from the litigation perspective of the Office of the Solicitor and the Department of Justice, as a practical matter, we cannot suspend our broader IT activities simply to accommodate two BLM systems. In order to meet the time requirements, we would suggest that BLM hire an IT contractor to conduct penetration testing of ALIS and AFMSS. The OIG would be willing, however, to independently review the penetration test results of any qualified IT contractor.

The OIG will incorporate a broader view of BLM's IT security stance in our annual work plan for FY 2007. This effort would include a more in-depth evaluation of the corrective action plans you implemented as a result of our penetration testing in FY 2005, review and validation of the overall security architecture in place at BLM, including technical control assessments, as well as internal and external penetration testing.

Questions or comments should be directed to Michael Wood, Assistant Inspector General for Administrative Services and Information Management at (202) 208-5745.

**Exhibit B**