

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELOUISE PEPION COBELL, et al.,)

Plaintiffs)

v.)

GALE NORTON, Secretary)

Defendants.)

Case No.1:96CV01285 (RCL)

NOTICE OF RULE 30(b)(6) DEPOSITION

To: J. Christopher Kohn
United States Department of Justice
Civil Division
1100 L Street, NW, Room 10036
Washington, DC 20005

Attorneys for Defendants

PLEASE TAKE NOTICE that pursuant to Rule 30(b)(6) of the Federal Rules of Civil Procedure plaintiffs' will take the deposition of the Mineral Management Service ("MMS") of the Department of the Interior on **May 10, 2005**. The deposition shall commence at 9:30 am at plaintiffs counsel's offices, the Native American Rights Fund, 1712 N Street, NW, Washington D.C. 20036, and shall continue on consecutive days until completed.

On or before May 5, 2005, the Interior defendants shall provide to plaintiffs the name, title, and grade level of each deponent who has actual knowledge of the facts and who is most qualified to testify on the matters stated below. At such time, the Interior defendants shall also disclose the specific matters that each such designated deponent will testify to. Further, the Interior deponents shall produce for deposition at the time and place specified by plaintiffs the deponent or deponents who are most qualified to testify on the following matters:

(1) The adequacy of security of information technology systems and applications, from

1984 through March 31, 2005, owned, controlled, or operated by MMS (“MMS IT Systems”) that house or access Individual Indian Trust Data (“Trust Data”).

(2) The adequacy of security of information technology systems and applications, from 1984 through March 31, 2005, owned, controlled, or operated by third parties that house Trust Data or interface with and access MMS IT Systems that house or access Trust Data (“Third-Party Systems”). Such Third-Party systems shall include without limitation systems owned, controlled, or operated by agents, contractors, corporations, state governments, agencies of states, agencies of the federal government, and Tribes under contract, compact, or cooperative agreement, whether or not such systems are under the control of MMS.

(3) Any and all steps taken to assess the risk of, and correct deficiencies and vulnerabilities in, the security of MMS IT Systems and applications that house or access Trust Data from 1984 through March 31, 2005.

(4) Any and all steps taken to assess the risk of, and correct deficiencies and vulnerabilities in, the security of Third-Party IT Systems and applications from 1984 through March 31, 2005.

(5) Any and all steps taken to undertake a certification and accreditation process for each IT System referenced in ¶¶ 1-2 above since December 5, 2001.

(6) Any and all steps taken to undertake a certification and accreditation process for each IT System referenced in ¶¶ 1-2 above from 1984 through December 5, 2001.

(7) Each material deficiency or vulnerability identified in the security of each IT System and application referenced in ¶¶ 1-2 above from December 5, 2001 through March 31, 2005.

(8) The trustworthiness of each IT System and application referenced in ¶¶ 1-2 above from 1984 through December 5, 2001 and the nature, scope, and location of documentation related thereto.

(9) The trustworthiness of each IT System and application referenced in ¶¶ 1-2 above from December 5, 2001 through March 31, 2005 and the nature, scope documentation related

thereto.

(10) The integrity of Trust Data housed in or accessed by each IT System referenced in ¶¶ 1-2 above and the impact of identified security deficiencies and vulnerabilities on the integrity of Trust Data housed in or accessed by each such system from 1984 through June 10, 1996.

(11) The integrity of Trust Data housed in or accessed by each IT System referenced in ¶¶ 1-2 above and the impact of identified security deficiencies and vulnerabilities on the integrity of Trust Data housed in or accessed by each such system from June 10, 1996 through December 5, 2001.

(12) The integrity of Trust Data housed in or accessed by each IT System referenced in ¶¶ 1-2 above and the impact of identified security deficiencies and vulnerabilities on the integrity of Trust Data housed in or accessed by each such system from December 5, 2001 through March 31, 2005.

(13) The process and procedures developed and implemented to ensure the preservation of all Trust Data housed in or accessed by each IT System referenced in ¶¶ 1-2 above, including without limitation all Trust Data created or stored in any electronic format since June 10, 1996.

Testimony will be recorded by stenographic means.

Respectfully submitted,

/s/ Dennis Gingold

DENNIS M. GINGOLD
D.C. Bar No. 417748
P.O. Box 14464
Washington, D.C. 20044-4464
202 824-1448

Of Counsel:

JOHN ECHOHAWK
Native American Rights Fund
1506 Broadway
Boulder, Colorado 80302
303-447-8760

/s/ Keith Harper

KEITH HARPER
D.C. Bar No. 451956
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
202 785-4166

Attorneys for Plaintiffs

April 13, 2005