

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

<b>ELOUISE PEPION COBELL, <u>et al.</u>,</b>	)	
	)	
<b>Plaintiffs,</b>	)	
	)	
v.	)	<b>Civil Action Number 96-1285 (RCL)</b>
	)	
<b>GALE A. NORTON, Secretary of the Interior, <u>et al.</u>,</b>	)	
	)	
<b>Defendants.</b>	)	
	)	
<hr style="border: 0.5px solid black;"/>		

**PRELIMINARY INJUNCTION**

For the reasons stated in the Court’s memorandum opinion issued this date, the Court now enters a preliminary injunction in this matter. This Preliminary Injunction (“Order”) supersedes and replaces the Preliminary Injunction entered by this Court on July 28, 2003.

A. Definitions

For purposes of this Order only, the following terms are defined as follows:

1. **Information Technology System.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, including computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
  
2. **Individual Indian Trust Assets.** Particular lands, natural resources, monies, or other assets held in trust at a particular time by the Federal Government for a

Tribe, Alaskan natives, or that are or were at a particular time restricted against alienation, for individual Indians.

3. **Management.** Actions that control, govern, administer, supervise, or regulate the use or disposition of Individual Indian Trust Assets.
4. **Federal Record.** This term is defined in 44 U.S.C. § 3301, and includes all documentary materials, regardless of physical form or characteristics, made or received under Federal law or in transaction of public business and preserved or are appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities or because of the informational value of the data in them.
5. **Individual Indian Trust Data.** Information stored in any Information Technology System that evidences, embodies, refers to, or relates to — directly or indirectly and generally or specifically — a Federal Record that reflects the existence of Individual Indian Trust Assets, and that either (1) was used in the Management of Individual Indian Trust Assets, (2) is a title or ownership record, (3) reflects the collection and/or disbursement of income from Individual Indian Trust Assets, (4) reflects a communication with a beneficiary (Individual or Tribe), or (5) was (a) created for the Bureau of Indian Affairs (BIA), Office of the Special Trustee (OST), or for a Tribe to use in the Management of Individual Indian Trust Assets; (b) provided to BIA, OST, or to a Tribe for use in the management of Individual Indian Trust Assets; and (c) used by the bureau or agency that created the record to manage Individual Indian Trust Assets.
6. **House.** The storage by electronic means of Individual Indian Trust Data.

7. Access. The ability to gain electronic entry into Information Technology Systems.

B. Substantive Provisions

In accordance with the foregoing, it is hereby ORDERED that:

1. All Information Technology Systems within the custody or control of the U.S. Department of the Interior, and its employees, agents, and contractors, that House or Access Individual Indian Trust Data and are currently disconnected from the Internet must remain disconnected from the Internet and cannot be reconnected until such time as this Court approves their reconnection to the Internet.
2. All Information Technology Systems essential for the protection against fires or other threats to life or property may remain connected to the Internet. Interior shall, within 5 days of this date, provide declarations, sworn or in compliance with 28 U.S.C. §1746 and LCvR 5.1(h) specifically identifying any and every such Information Technology Systems that has remained connected to the Internet and setting forth in detail the reasons Interior believes such Information Technology System to be essential for the protection against fires or other threats to life or property. The Court will review such declarations, but absent a contrary order from the Court, such systems shall remain connected to the Internet.
3. The Office of Inspector General, the Minerals Management Service, the Bureau of Land Management, the Bureau of Reclamation, the Office of the Special Trustee, Fish and Wildlife, the Bureau of Indian Affairs, the Office of Surface Mining, and the National Business Center shall disconnect all Information Technology Systems within their respective custody or control from the Internet forthwith, whether or not such Information Technology Systems House or Access Individual

Indian Trust Data. Any other bureau within the U.S. Department of the Interior that has custody or control over an Information Technology Systems that Houses or Accesses Individual Indian Trust Data must disconnect all of their Information Technology Systems from the Internet, except as provided in paragraph 4, infra.

4. As the Court is satisfied the Information Technology Systems in the custody and control of the National Park Service, the Office of Policy Management and Budget, and the United States Geological Survey do not House or Access Individual Indian Trust Data, these agencies do not have to disconnect any currently connected systems from the Internet.
5. Interior may, at any time, submit a proposal to the Court for connecting the systems disconnected by this Order or any prior order of this Court to the Internet. Any such proposal must include all of the following: (1) a uniform standard to be used to evaluate the security of all Information Technology Systems within the custody or control of the U.S. Department of the Interior, its bureaus, its agents, and its contractors; (2) a detailed process whereby the uniform standard will be applied to each Information Technology System; (3) a proposed entity external to Interior and having no existing relationship with Interior that will perform the following functions: (a) evaluate the security of each Information Technology System that has completed the process set forth in (2); (b) submit a report to the Court setting forth its independent evaluation of the security of each Information Technology System; (c) monitor, on an ongoing basis, the security of the Information Technology Systems that the external entity determines House or Access Individual Indian Trust Data; and (d) submit monthly reports to the Court

concerning the status of the Department of the Interior Information Technology Systems; (4) a budget and plan of action for the proposed external entity to fulfill the requirements in (3). Any such proposed external entity must not have any existing or proposed relationship or contract of any kind with the Department of the Interior or any of its bureaus. The external entity must not take on any other work for the Department of the Interior outside of the tasks set forth in this injunction. The external entity can function under the supervision of the Court or operate as a contractor to the Department of the Interior.

6. Plaintiffs may submit the names and proposed plans of up to three entities that they submit can fulfill the requirements outlined in paragraph 5 (3).
7. Plaintiffs may, within ten (10) days of receipt, submit comments on any proposal submitted by the Department of the Interior in accordance with paragraph 5.
8. After the Court receives a proposal from the Department of the Interior and comments from Plaintiffs, the Court will either approve or deny the proposal. Once the Court has approved a proposal and has chosen the external entity the Department of the Interior may commence the process outlined in paragraph 5(2). Upon completion of that process the Department of the Interior will submit a report on its actions to the Court and the external entity. Such report will be sworn or in compliance with 28 U.S.C. §1746 and LCvR 5.1(h). The external entity will then evaluate the report and conduct an independent evaluation of the security of the Information Technology system proposed for reconnection to the Internet and submit reports to the Court on each. Plaintiffs may then submit comments within 15 days on the reports. If the Court is then satisfied that the

