IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,

Plaintiffs,

v.

GALE A. NORTON, Secretary of the Interior, et al.,

Defendants.

Case No. 1:96CV01285
(Judge Lamberth)

NOTICE OF ACTIONS TAKEN BY THE DEPARTMENT OF THE INTERIOR TO COMPLY WITH DECEMBER 5, 2001 TEMPORARY RESTRAINING ORDER

On December 5, 2001, the Court entered a Temporary Restraining Order, as amended on December 6, 2001, requiring the Department of the Interior ("Interior") to "immediately disconnect from the Internet all information technology systems that house or provide access to individual Indian trust data" and to "immediately disconnect from the Internet all computers within the custody and control of the Department of the Interior, its employees and contractors, that have access to individual Indian trust data." In carrying out the terms of that Order, Interior has applied the following definitions:

> *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. (Source: ITMRA 5002(3)).
>
> *Individual Indian trust data*- information in a digital format, stored in a computer or other electronic information retrieval system that is a Federal Record as defined in 44 U.S.C. § 3301 and that evidences the existence of individual Indian trust

assets (e.g., as derived from ownership data, trust patents, plot descriptions, surveys, jacket files, statement of accounts), the collection of income from individual Indian trust assets (e.g., as derived from deposit tickets, journal vouchers, schedule of collections), use or management of individual Indian trust assets (e.g., as derived from leases, sales, rights-of-way, investment reports, production reports, sales contracts), or the disbursement of individual Indian trust assets (e.g., as derived from transaction ledgers, check registers, transaction registers, or lists of canceled or undelivered checks).

Individual Indian trust assets- Lands, natural resources, monies, or other assets held by the Federal government in trust or that are restricted against alienation for individual Indians.

House- The storage of data such that the data is retrievable by electronic means.

Access- The ability to gain electronic entry into systems, networks, personal computers, or application service providers;

Interior has taken efforts to ensure that it is in compliance with the Court's Temporary Restraining Order. Those efforts include:

1. On December 5, 2001, Interior verbally directed its senior management officials to disconnect their systems from the Internet. See Ex. A (Meeting Notes of Sue Ellen Woolridge from December 5, 2001); Ex. B.

2. The Assistant Secretary – Indian Affairs ordered all regional directors and central office directors to "immediately disconnect/unplug all non-BIA network connections to the Internet." See Ex. C.

3. In the morning through early afternoon of December 6, 2001, Interior received responses on actions taken to comply with the order to disconnect from the Internet from the following agencies: NBC Denver, NBC Washington, Alaska ARTNET2, Inspector General, Solicitor, Office of Special Trustee for American

Indians, Office of Historical Trust Accounting, National Park Service, Fish and Wildlife Service, Bureau of Indian Affairs, Bureau of Land Management, Minerals Management Service, Office of Surface Mining, U.S. Geological Survey, Bureau of Reclamation, Office of Hearing and Appeals. See Ex. D.

4. Employees were also instructed to disconnect modems from PCs connected to the BIANet. See, e.g., Ex. E.

5. On December 7, 2001, Interior Chief Information Officer Daryl White wrote a memorandum to Associate Deputy Secretary James Cason stating that he had discussed in a meeting with Bureau or Office chief information officers, their deputies, or technology chiefs their compliance with the Temporary Restraining Order, and that he told the attendees that "[i]f I don't hear differently, I assume you disconnected from the Internet. Further, you are directed to remain disconnected until further notice." He reported that there was no disagreement. See Ex. F.

Beyond those steps required by the Temporary Restraining Order, Interior has taken additional action to address the deficiencies in its trust-related information technology systems. To provide additional security for individual Indian trust data in the short-term, Interior had previously entered into a contract with Predictive Systems, Inc. to install firewalls, intrusion detection systems, and near real-time monitoring at three Office of Information Resource Management facilities. A copy of this contract has previously been filed with the Court. Interior expects this installation to be complete by January 31, 2002.

Because each information technology system provides important or critical services for

individual Indians, Interior would like to re-establish system operations once it can provide reasonable protection for the individual Indian trust data. Interior has filed a proposed consent order that would permit it to reconnect to the Internet any information technology system that no longer houses individual Indian trust data and that does not provide access to individual Indian trust data. In addition, Interior also sought permission to reconnect to the Internet any information technology system that houses individual Indian trust data if the external communications system is designed to deny access to the data and identifies unauthorized attempts to access the data (e.g., if it has a firewall, is subject to intrusion detection, and if system activity logs are available and routinely reviewed). For each information technology system that does not fit into either of these categories, Interior, in consultation with external experts, developed the following criteria that must be met before that system would be reconnected to the Internet:

1. Interior has implemented ingress and egress filtering on all internetwork connection routers bordering that system to prevent unauthorized access to the system;

2. Interior has first disabled all user IDs and then enabled only those IDs for users for whom the responsible program official has (1) verified the need of the user to access the system; and (2) issued a new, alphanumeric password to the verified user;

3. Interior has required all users to use complex (at least alphanumeric) passwords of at least 6 characters. Interior will communicate this requirement to users through written memoranda and oral communication at the time of user ID reactivation;

4. Interior has trained personnel who will examine system and router logs daily to identify malicious system activity; and

5. Interior has delivered to the Special Master: (1) router configuration text files showing the implementation of ingress and egress filtering technology; (2) certifications from the relevant responsible program officials for the management

of user IDs; (3) a computer program used to generate complex passwords, and a copy of the written memorandum and help desk oral script used to communicate new password policy to users; and (4) the identification of the trained personnel who will examine the system and router logs and a description of the mechanism by which they will monitor the logs.

Interior recognizes that, although these short-term steps will increase security for its individual Indian trust data located in the systems in this last category, more needs to be done to rectify the deficiencies identified in the Special Master's November 14, 2001 Report and Recommendation. After each system is brought on-line, Interior intends to task a qualified independent contractor to perform on each system as it is brought on-line an evaluation of the requirements to bring that system into compliance with OMB Circular A-130. Interior contracted with Science Applications International Corporation ("SAIC"), a leading information technology consulting firm, "to begin services to design, implement and manage an information assurance infrastructure and information security management program" with respect to Interior's information technology systems. See Ex. G. Within one month of receiving the independent contractor's evaluation, Interior will file with the Court a long-term security action plan to bring each system into compliance with OMB Circular A-130.

Upon completion of one or more long-term security action plans, Interior plans to seek from a recognized accreditation entity, independent accreditations of the covered systems as compliant with OMB Circular A-130. If the independent accreditation entity accredits the covered information technology system, Interior proposes to request that the Court's oversight of that system would end. If the independent accreditation entity were to decline to accredit the covered information technology system, Interior would produce and implement an action plan to correct any identified deficiencies.

Respectfully submitted,

ROBERT D. McCALLUM, JR.
Assistant Attorney General
STUART E. SCHIFFER
Deputy Assistant Attorney General
J. CHRISTOPHER KOHN
Director

SANDRA P. SPOONER
Deputy Director
JOHN T. STEMPLEWICZ
Senior Trial Attorney
MATTHEW J. FADER
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
(202) 514-7194

OF COUNSEL:

Sabrina A. McCarthy
Department of the Interior
Office of the Solicitor

CERTIFICATE OF SERVICE

I declare under penalty of perjury that, on December 7, 2001, I served the foregoing Notice of Actions Taken by the Department of Interior to Comply With December 5, 2001 Temporary Restraining Order, by facsimile only, in accordance with their written request of October 31, 2001, upon:

Keith Harper, Esq.
Lorna Babby, Esq.
Native American Rights Fund
1712 N Street, NW
Washington, D.C. 20036-2976
202-822-0068

Dennis M Gingold, Esq.
Mark Brown, Esq.
1275 Pennsylvania Avenue, N.W.
Ninth Floor
Washington, D.C. 20004
202-318-2372

by facsimile and by U.S. mail upon:

Alan L. Balaran, Esq.
Special Master
1717 Pennsylvania Ave., N.W.
12th Floor
Washington, D.C. 20006

by U.S. Mail upon:

Elliott Levitas, Esq.
1100 Peachtree Street, Suite 2800
Atlanta, GA 30309-4530

and by hand delivery upon:

Joseph S. Kieffer
Court Monitor
420 7th Street, NW
Apt 705
Washington, DC 20004

Erin Langsdorf

1000 am - 800 am cell: 202 441-0326

SEW - 1800-508-0027 * 4539

OFFICE OF
THE DEPUTY SECRETARY OF THE INTERIOR

630 pm:

① Contacted Darryl White – Began check of status of shut down

McCaleb White Capon SEW

① Instr's to BIA – has gone out; – Neal McCaleb – Ed Socks

② Directed Rob McKenna – OST all programs shut down all – kill it at Router level and all PCs

③ Directed Ed Socks to call Delphic McLeod at TAAMS / Fannie to call TAAMS – direct shut down. – Chet Mills, too.

② Call DOJ – touch base

③ OCW ~~[redacted]~~ Susan Ottley, Bill Rosales; Darryl White; Sharon Blackwell – Tex Cas

④ Ed Socks' ~~[redacted]~~ message went out;

⑤ Sharon Blackwell – Told people to get them down. period.

⑥ NBC – cut SSA checks, not beneficiary checks;

⑦ Darryl White – called Scott McPherson – will make intranet connection for BLM – AFMS (Leslie Cone) (Fred Nicholas) shut down.

⑧ Darryl Call – BLM re Tulsa Dist office – Std Mineral appraisals electronic;

⑨ David White – ELRIS – NBC – AS 400 system – Being shut down per Ed Socks – Sharon

⑩ Bruce Muzzy – Tell ATS know shut down.

OFFICE OF
THE DEPUTY SECRETARY OF THE INTERIOR

Daugh + Jim Cason told

) Bob Brown ✓ – Lucy Denett / Bob Brown – MMS shut down systems

) Bob Moore – OHA – told them to shut down
Daugh

) OSM? Jim Cason called Carol ___ shut down

) USGS? Bennett Raley will call USGS BOR

) USPS?

Sol – Bill will call re Tulsa + MMB

OST

United States Department of the Interior

OFFICE OF THE SPECIAL TRUSTEE FOR AMERICAN INDIANS
Washington, D.C. 20240

Memorandum

December 6, 2001

To: Associate Deputy Secretary

From: Principal Deputy Special Trustee James Thompson

Subject: Internet Disconnection Actions by the Office of the Office Special Trustee for American Indians

A December 5, 2001 Court Order instructed Interior to:

- Disconnect from the Internet Information technology systems that house or provide access to individual Indian trust data.

- Disconnect from the Internet all computers within the custody and control of the Department of the Interior, its employees and contractors, that have access to individual Indian trust data.

Following discussions late yesterday among senior Interior, BIA, CIO and OST management staff, at approximately 6 p.m. Eastern time on December 5, OST gave a "stand-by" order to the Albuquerque IT staff to prepare to effect the required disconnection. OST senior managers then awaited definitive guidance and clarification of the Court Order, remaining in contact with the IT staff over the next 1½ hours. At about 7:30 p.m., I learned that Mr. James Cason and Mr. Daryl White had telephoned the IT staff directly and instructed them to effect the disconnection. (Subsequently, I received a contemporaneous voice mail message from the Deputy Chief of Staff to contact her, or Mr. Cason, on this issue).

As of noon, December 6, 2001, OST has completed the following:

- On Wednesday evening, December 5, 2001, at approximately 7 pm Mountain Time, the OST router Access Control List (ACL) was modified to restrict access. No http traffic is allowed presently either in or out of OST's router.

- On Wednesday evening, December 5, 2001, at approximately 7 p.m. Mountain time, all modems (approximately 15) have been removed from PC's that had potential access to the LAN. Two modems on dedicated, stand alone PC's were not removed; these machines do not have access to the LAN and service GOALS, CashILink and ECS connections direct to Treasury. OST will isolate and closely monitor these applications on stand alone and dedicated PC's so we can continue to process ACH's and retrieve information from the Federal Reserve. OST will

examine other such applications (PACER, Polaris, etc.) with a view to establishing a work around not based on Internet technology.

- On Wednesday evening, December 5, 2001, at approximately 7 p.m. Mountain time, SEI was notified to discontinue access to StrataWeb, an internet-based system enabling Tribes to view Tribal account status.

- On Wednesday evening, December 5, 2001, at approximately 5 p.m. Mountain time, The Remote Access System Server (RAS) was shut down. With regard to impact, Wyondotte and Cherokee Tribes performing contracted/compacted IIM trust accounting functions are not able to access TFAS as normal through the Internet. Tribes who normally access Tribal account information through RAS will not be able to access TFAS to examine Tribal trust account status.

- On Wednesday evening, December 5, 2001, at approximately 7 pm Mountain time, OST's Lotus Notes Server was shut down, but brought back up at approximately 8 am Mountain time on Thursday, December 06, 2001, for OST intranet service only. A call has been placed to Lotus to determine how OST could encrypt all mail sent from the Lotus Server.

- The ACL was modified on OTFM's Cisco 7507 router. The RAS runs on a Dell Server running NT 4 service pack 6.

- OST's contractors DataCom, SEI, CDL, KPMG, and EDS have been notified and instructed to disconnect all linkages from the Internet to trust databases in their control. Follow up confirmation to validate these actions by the contractors is being initiated.

- OST's Office of Trust Records and Trust Risk Management have removed all modem connections to PC's that can access trust data or information. Likewise, servers containing trust data have been locked down. OST field staff are co-located with BIA elements and receive processing support through BIANET channels. BIA action to disconnect from the Internet covers OST field staff, with three exceptions. OST staff in Billings, Muskogee and Shawnee have been instructed to disconnect Internet access.

Impacts include:

- Inability to transfer funds from BIA to TFAS (IPAC).

- No lease processing until the NX comes back on line.

- No Per Capita processing until the NX comes back on line.

- Likely delays in processing trust check payments to allottees.

Update to items discussed in the December 6, 2001 memo.

OTFM continues to block all internet traffic flowing to or from OTFM's router in Albuquerque.

The Remote Access Server (RAS) continues to be disabled.

In accordance with the telephone conversation held on 5 December, Lotus Notes was enabled after making the modifications discussed on the conference call and consultation with the OS Notes Administrator.

The SEI Relationship Manager has confirmed that StrataWeb has been disabled.

The Electronic Certification System continues to be a stand alone system isolated from the LAN. This system uses a secure dial up connection to the Regional Disbursing Office in San Fransisco. This system was never hooked up to the OTFM LAN, nor does it have internet access.

Cash Link is a dial up system that was previously housed on a PC that was connected to the LAN and therefore the PC had internet access. This system has been moved to a PC isolated from the LAN. The system being accessed does not contain Individual Indian Trust data.

Polaris is a dial up system that was previously housed on a PC that was connected to the LAN and therefore the PC had internet access. This system has been moved to a PC isolated from the LAN. The system being accessed does not contain Individual Indian Trust data.

Pacer is a dial up system that was previously housed on a PC that was connected to the LAN and therefore the PC had internet access. This system will not be used until further clarification from Treasury about the security of the dial up connection and confirmation for senior management is received that access is OK. Pacer would show negotiated check information for individuals. The system being accessed is not a DOI system, rather it is a Treasury system and apparently not covered under the restraining order.

Bloomberg continues to be disabled.
IPAC continues to be disabled.
FFS continues to be disabled.
FPPS continues to be disabled.

Note: We have received a call asking whether or not the restraining order pertains to PL638 tribes?

OPTIONAL FORM 99 (7-90)

FAX TRANSMITTAL # of pages ► 1

To: Dona Erwin	From: Bob McKenna
Dept./Agency: OST	Phone #: 505-816-1001
Fax #: 202-208-7545	Fax #: 505 816-1267

NSN 7540-01-317-7368 5099-101 GENERAL SERVICES ADMINISTRATION

United States Department of the Interior

BUREAU OF INDIAN AFFAIRS
Washington, D.C. 20240

DEC 05 2001

IN REPLY REFER TO:

To: All Regional Directors
All Central Office Directors

From: Assistant Secretary-Indian Affairs

Subject: Order to Immediately Disconnect Computers

You are hereby ordered to immediately disconnect/unplug all non-BIA network connections to the Internet. This includes:

Networked Workstations with separate phone lines to the outside Internet;

Any connection via RAS to a BIA and/or AS-IA organization networked computer;

Any outside connection to an ISP by a server or individual workstation in all BIA/AS-IA offices.

Please be advised that any employee who may attempt to circumvent this order by connecting to the internet via an outside line for any reason will be subject to disciplinary action up to and including termination of employment.

All Regional Directors and Central Office Directors are required to certify that all computer connections to the internet located within your administrative organization have been disconnected and that each employee has received a copy of this memorandum and the penalty for violation was explained.

This certification should be emailed to debbieclark@bia.gov with the following information:

Office location
Computer location
User name, Phone number and Email address.

Please respond in your email the effect this action will have on your capability to perform your assigned duties. Should you have any questions, please contact Bill Roselius at 405/205-7119 or Debbie Clark at 202/208-6087.

EFFORTS WITHIN THE DEPARTMENT TO FOLLOW THE COURT ORDER ISSUED 12/5/01

AGENCY	YES	NO
Office of the Secretary:		
NBC Denver	X	
NBC Washington	X	
Alaska ARTNET2	X	
Inspector General	X	
Solicitor	X	
Office of Special Trustee for American Indians	X	
OHTA	X	
National Park Service	X	
Fish and Wildlife Service	X	
Bureau of Indian Affairs	X	
Bureau of Land Management	X	
Minerals Management Service	X	
Office of Surface Mining	X	
U.S. Geological Survey	X	
Bureau of Reclamation	X	
Office of Hearings and Appeals	X	

NBC- DENVER

I, Robert L. Scheibel, certify that the attached information has been verified to be true and correct.

Signature Robert L Scheibel

Title Chief Information Officer

Organization National Business Center

Date December 6, 2001

Attached is the document "Description of your Organization's Efforts to Disconnect Trust Systems from the Internet."

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to
Disconnect Trust Systems from the Internet

Who called you to request : John Curran, BIA It Security Manager

When did they call: Initial informational call at 3:00 p.m. MST; official request to bring the system down at 4:25 p.m. MST

Name of system(s) affected: IBM OS/390, SYSH LPAR

Where (H/W) system(s) located: Denver, Colorado

Type of H/W: IBM Multiprise 3000 (7060-H30) mainframe

What Indian Trust data is housed there? Land title information showing and tracking Indian ownership, including all System rights conveyed or changed over time.

What Indian Trust system(s) is run there? Land Records Information System (LRIS)

Name and telephone number of person who shutoff the Internet access:
Walter Jones 303-969-7256

Time they accomplished the shutoff: 7:43 p.m. MST

How did they accomplish the shutoff: System was backed up; all system tasks and initiators were drained; the system was then deactivated.

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2360
Voice: 202/208-5444 (Julia)

202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

Date: 12/6/01

Time: 8:22

FAXOGRAM

Department of the Interior
Office of the Secretary
National Business Center
Products and Services
ADP Services Division
7301 W. Mansfield Avenue
Lakewood, Colorado 80235-2230

To: Julia Laws

Telephone No.:

FAX No.: (202) 501-2360

From:

Telephone No.: (303) 969-7070

FAX No.: (303) 969-7102

Number of pages including this cover sheet 4

Remarks and Special Instructions:

OS
NBC WASHINGTON

I, John R. Short certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature John R. Short

Title Computer Specialist

Organization OS/NBC Washington

Date Dec 6, 2001

Attached is the description of the organizations efforts.

Office of the Secretary / NBC - Washington

I, Roberta Heintz certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Roberta A. Heintz

Title Acting Chief, NBC Technology Services

Organization OS/NBC Washington

Date December 6, 2001

Attached is the description of the organizations efforts.

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to
Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White): Roger Mahach
When did they call: 9:30am, December 6, 2001
Name of system(s) affected: OS/NBC Washington electronic mail, local area network, Internet services and access to departmental administrative systems

Where (H/W) system(s) located: Room 1559, Main Interior Building

Type of H/W: Various local area network servers

What Indian Trust data is housed there? Electronic mail and documents related to Indian Trust data and systems, Document Management System containing Cobell litigation-related documents
What Indian Trust system(s) is run there? N/A

Name and telephone number of person who shutoff the Internet access: John Short, 202-208-5148
Time they accomplished the shutoff: 12:30pm, Thursday, December 6, 2001
How did they accomplish the shutoff: Disconnected public connection from firewall to Internet

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

Dan Healey - ARTNET 2

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to
Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White): Daryl White
When did they call: 12-6-01 10AM
Name of system(s) affected: ARTNet2

Where (H/W) system(s) located: Anchorage

Type of H/W: Routers - Switches

What Indian Trust data is housed there? NONE
What Indian Trust system(s) is run there? NONE

Name and telephone number of person who shutoff the Internet access:
Time they accomplished the shutoff: N/A
How did they accomplish the shutoff: NA

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

I, Bob W [illegible] certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Bob W [illegible]

Title Comm. Manager

Organization OCIO

Date Dec 6, 01

Attached is the description of the organizations efforts.

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

OIG 5:30pm Update restored Internet access & simply removed access to Trust systems

DEC - 6

Memorandum

To: Earl E. Devaney
Inspector General

From: Kimberly Elmore-Butterfield Kimberly Elmore-Butterfield
Acting Deputy Inspector General for Audits

Subject: Temporary Restraining Order Regarding Cobell v. Norton

In response to a December 6, 2001 10:30 am EST request from Steve Griles, Deputy Secretary for the Department of the Interior, the Office of Inspector General (OIG) determined that it does not own or maintain systems which manage Indian Trust Fund data and hand-carried this information to Julia Laws in the Office of the Secretary. (Attachment 1) Further review revealed that both OIG and Klynveld Peat Marwick Goerdeler (KPMG) staff have "read only" internet access to the subject data.

On December 6, 2001 at 11:00 am EST, the OIG held a meeting to prepare a plan of action for ceasing the internet access to Bureau of Indian Affairs (BIA) Indian Trust Fund records by OIG and KPMG staff. We verified that the OIG and KPMG staff do not have direct access to the three systems that maintain Indian Trust Fund data – TAAMS, IRMS and LRIS; however, we do have access to Indian Trust Fund data through FFS and Infopack. FFS is housed and accessed through the server in Reston, Virginia. Infopack is housed and accessed through the National Business Center (NBC), Albuquerque, NM. At this time we informed OIG and KPMG employees not to attempt to access Indian Trust Fund data and told them that further instructions would be forthcoming.

At 12:15 pm EST, OIG and KPMG employees were again advised not to access Indian Trust Fund data. In addition, they were instructed that all Indian Trust Fund information containing account holder names, account numbers, dollar amounts or any related information stored on their computer's hard or shared drives should be transferred to a disk. OIG and KPMG employees downloaded these records to disks, labeled them "Proprietary Data" and secured them in locked file cabinets. Additionally, other Indian Trust Fund information in hard copy/paper form has been appropriately labeled and secured in locked cabinets.

At 2:00 pm EST we prepared a list of all OIG and KPMG staff with FFS and Infopack access. These names are at Attachment 2.

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

DEC - 6

Memorandum

To: Earl E. Devaney
Inspector General

From: Kimberly Elmore-Butterfield
Acting Deputy Inspector General for Audits

Subject: Temporary Restraining Order Regarding Cobell v. Norton

In response to a December 6, 2001 10:30 am EST request from Steve Griles, Deputy Secretary for the Department of the Interior, the Office of Inspector General (OIG) determined that it does not own or maintain systems which manage Indian Trust Fund data and hand-carried this information to Julia Laws in the Office of the Secretary. (Attachment 1) Further review revealed that both OIG and Klynveld Peat Marwick Goerdeler (KPMG) staff have "read only" internet access to the subject data.

On December 6, 2001 at 11:00 am EST, the OIG held a meeting to prepare a plan of action for ceasing the internet access to Bureau of Indian Affairs (BIA) Indian Trust Fund records by OIG and KPMG staff. We verified that the OIG and KPMG staff do not have direct access to the three systems that maintain Indian Trust Fund data – TAAMS, IRMS and LRIS; however, we do have access to Indian Trust Fund data through FFS and Infopack. FFS is housed and accessed through the server in Reston, Virginia. Infopack is housed and accessed through the National Business Center (NBC), Albuquerque, NM. At this time we informed OIG and KPMG employees not to attempt to access Indian Trust Fund data and told them that further instructions would be forthcoming.

At 12:15 pm EST, OIG and KPMG employees were again advised not to access Indian Trust Fund data. In addition, they were instructed that all Indian Trust Fund information containing account holder names, account numbers, dollar amounts or any related information stored on their computer's hard or shared drives should be transferred to a disk. OIG and KPMG employees downloaded these records to disks, labeled them "Proprietary Data" and secured them in locked file cabinets. Additionally, other Indian Trust Fund information in hard copy/paper form has been appropriately labeled and secured in locked cabinets.

At 2:00 pm EST we prepared a list of all OIG and KPMG staff with FFS and Infopack access. These names are at Attachment 2.

At 2:30 pm EST Mr. Chris Krasowski called Ms. Kim Marchant at the NBC in Denver (303-969-7780) and asked that all the FFS passwords for OIG and KPMG employees with access to Indian Trust Fund data be revoked immediately.

At 3:30 pm EST AIG-M&P drafted an e-mail that informed employees passwords for OIG and KPMG employees working on Indian Trust Fund activities have been revoked. The e-mail states that the OIG internet system is in operation, however, OIG employees may experience difficulty in reaching Interior bureaus via the internet. (Attachment 3)

At 4:00 pm Mr. Chris Krasowski called Ms. Kim Marchant at the NBC in Denver (303-969-7780) and asked that the Infopack password for OIG employees with access to Indian Trust Fund data be revoked immediately.

If further action is taken, I will inform you immediately.

Attachments 3

cc: Darryl White/DIO/CIO
Eddie Saffarinia/OIG/CIO
Julia Laws/OS/CIMD

Attachment 1

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to
Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White):
When did they call:
Name of system(s) affected:

Where (H/W) system(s) located:

Type of H/W:

What Indian Trust data is housed there?
What Indian Trust system(s) is run there?

Name and telephone number of person who shutoff the Internet access:
Time they accomplished the shutoff:
How did they accomplish the shutoff:

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

I, Ronald Malone certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Ronald Malone

Title Chief, IRM

Organization OIG

Date December 6, 2001

AIG/MP - Concur

Attached is the description of the organizations efforts.

Names of Employees With Access to Indian Trust Fund Data

OIG
202-208-5520

Gene Bratcher
Julene Theis
Dawn Eleice Pizarro
Julie Ford
Jamie Howard
Joaquin Carney
Ben Privitt
Karleen Hill
Scot Tilley
Clark Bullock
Tom Zwettler
Chris Krasowski
Melvin Skinner
Richard O'Brien

KPMG
202-208-5552

Scot Janssen
Carole Withers
Jeanine Miller
Tonya Diamond
Rod Filliban
Bruce Antiporowich
Rob Fuller
Paul Geraty
Jim Childers
Alan Klein
Robert Moore
Dwan Ranghel-Warner
Sharolynn Dewitt
John Hummel
Tom Boylan
Kathleen Ditcher
Gene Wichmann
Amy-Beth Evans
Adriana Yepes
Jerry Chow
Jennifer Tauser
Jatin Wahl
Margaret McKinney
Kevin Lowe
Ruby Reichel

Attachment 3

Sharon D Eller

12/06/01 04:53 PM

To: OIG Employees
cc:
Subject: Cobell v Norton court order re: Internet access for Indian Trust data

In response to a court order in the matter of Cobell v Norton, the Department of the Interior has been instructed to ".... immediately disconnect from the Internet all computers within the custody and control of the Department of the Interior, its employees and contractors , that have access to the individual Indian trust data." Signed Royce C. Lambert, US District Judge.

We have arranged for the immediate revocation of passwords for our auditors and the KPMG contractors working on Indian Trust matters. Information that has already been collected for audits regarding the Indian Trust data, will be moved off computer hard drives, and stored on CDs immediately.

Accordingly, all OIG employees are instructed to not attempt access to the Indian Trust Fund (ITF) data base and to protect all ITF data by removing the ITF data from any storage computer which can be remotely accessed, and copying the data to a CD-ROM or other storage media. Such copies should then be secured within your office. Employees who possess ITF data should make no disclosures of the data to any other party prior to consulting with the appropriate AIG.

In addition, you may be impacted in attempting to reach other bureaus via the Internet. The Office of the Secretary and some Bureaus have cancelled Internet access for their employees . The O/S webpage is now only available to Office of the Secretary employees. The Solicitors office in Albuquerque, has shut down their employees Internet access.

As of now, the OIG e-mail system has not been shut down. But, as other DOI bureaus are restricting e-mail exchange and Internet access, the OIG will be impacted in that we may not send and receive email messages from other DOI bureaus.

We will continue to keep you informed as we become aware of other Departmental actions that may affect your ability to perform your mission.

Sharon D. Eller
Assistant Inspector General for Management and Policy

OIG

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White): JULIA LAWS
When did they call: 12-6-2001 10AM
Name of system(s) affected: NONE

Where (H/W) system(s) located: NONE

Type of H/W: NONE

What Indian Trust data is housed there? N/A
What Indian Trust system(s) is run there? N/A

Name and telephone number of person who shutoff the Internet access:
Time they accomplished the shutoff: NA RONALD MALONE
How did they accomplish the shutoff: NA (202) 208-2406

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

I, RONALD J. MALONE certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks. THE OIG HAD NO SYSTEMS RELATED TO THE INDIAN TRUST FUNDS,

Signature Ronald J Malone / Aaron J. Ellen AIG/IMP

Title Chief, IRM

Organization OIG

Date 12-6-2001

Attached is the description of the organizations efforts.

12/6/01

TO: Jim Cason

FROM: Office of the Solicitor

Subject: Actions taken to comply with Order of the Court, dated December 5, 2001, in *Cobell v. Norton*

Between 9 p.m. and midnight EST on December 5, 2001, we telephoned all offices of the Solicitor not located in Washington, DC to advise them of the Order and to direct them to take certain actions. The telephone calls were placed by Tim Elliott (202-208-4813), acting Deputy Solicitor, and Susan Offley (202-208-4388), Attorney-Advisor. They were assisted by Stephan Graves (202-208-4331) from the MIS branch of the Office. Bill Roselius (405-205-7119) of the Bureau of Indian Affairs was present during the first few calls. The result of those call are as follows:

Summary

With the exception of the Sacramento Regional Office and the San Francisco Field Office, all offices were reached and reported back before 1 a.m. EST December 6, 2001 that they had followed the instructions. The instructions essentially were in line with the message Assistant Secretary McCaleb (202-208-7163) sent to the Bureau of Indian Affairs earlier in the day. That message indicated that all non-network connections to the internet were to be disconnected. Most offices have a Bravo computer that has a separate dial-up capability to access the internet. While we believe these are the only ones with that capability, we asked each office to verify that any other machines with a similar capability were disconnected from the internet.

Alaska - We reached Dennis Hopewell (907-271-4131), the Deputy Regional Solicitor, who advised that all access to the internet was disconnected in that office

Atlanta - We reached Patricia Courtelyou-Hamilton (404-331-4447), an Attorney-Advisor, who reached Horace Clark (404-331-4447 Ext. 225), the acting Regional Solicitor. Mr. Clark reported back that the office computers with independent access to the internet were disconnected.

Knoxville - Field Solcitor Begley (865-545-4315 Ext. 11) disconnected the Bravo machine.

Boston - We reached Jim Epstein, (617-527-3400)the acting Regional Solicitor, who advised that their office has no independent outside access to the internet.

Pittsburgh - We reached JoAnn Leshen (412-937-4001), a legal technician. Ms. Leshen advised that the office disconnected the Bravo machine and the internal modem from the other machine with one.

Twin Cities - The Field Solicitor, Priscilla Wilfahrt (612-713-7100)advised that the Fish and Wildlife Service has severed all connections from that office to the internet.

Tulsa - Alan Woodcock (918-669-7730), an attorney-Advisor, disconnected the Bravo machine.

Albuquerque - Tonianne Baca-Green (505-346-2700), an attorney-advisor, advised us she had disconnected the Bravo Computer, which is the only one in that office with independent access to the internet. The acting Regional Solicitor advised us that all external access to the system in Albuquerque.

Denver - Assistant Regional Solicitor Gerry O'Nan (303-231-5353) advised that their two machines with stand-alone access to the internet were shut down.

Billings - Garry Moore (406-247-7586), an attorney in the office advised all computers in the office were disconnected from the internet.

Boise - Ken Sebby (208-334-1911), an attorney in the office advised that Boise has no Indian trust data in the office, nor does it have a Bravo machine. The Bureau of Reclamation is sending a technical person to the office to review the system for other connections.

Phoenix - Dan Jackson (602-379-4523), an attorney in the office, advised that the office has no individual Indian Trust data on their machine, nor do they have a Bravo machine.

Palm Springs - Dan Shillito (760-416-8619), the Field Solicitor advised that the only computer in the office is shut off, in his absence. He will disconnect from the internet when he returns to his office.

Santa Fe - The Field Solicitor, Arthur Arguedas (505-988-6200), advised that their computers with independent access to the internet were unplugged.

Salt Lake City - the field Solicitor, John Steiger (801-524-5677), advised that their Bravo computer was unplugged and that their other access to the internet is through the Bureau of Reclamation. He called the Bureau and was told that his office did not have the ability to disconnect from the Bureau's local area network.

Portland - We reached Lynn Peterson (503-231-2125), the Regional Solicitor, who had Donna Barton (503-231-2126), a secretary in that office, call us to advise that the Bravo machine and one other machine in the office that might have independent connections to the internet was shut down.

San Francisco was reached the morning of December 6, 2001. They are sending someone to the

office before it opens to disconnect their Bravo computer.

Sacramento - Carolyn Brooks (916-978-5671), is at the Sacramento Office, working with the Bureau of Reclamation to disconnect the Bravo machine and any other machines with independent internet access.

Other Actions

1. Last night Stephan Graves, Susan Offley and Tim Elliott inspected all offices in the Division of Indian Affairs for separate connections to the internet. None were found.

2. This morning we have started calling all offices to determine if they have any Indian Trust data on computers able to access the internet through any means, including wide area networks.

3. We have shut down all electronic messaging capabilities for the Office, nationwide.

4. No divisions, except the Admin. Division in Washington have external internet access. All such access in Washington is being disconnected.

Effects

We now have no access to e-mail systems. In some offices, which number will increase, our PCs function only as wordprocessors.

United States Department of the Interior

OFFICE OF THE SPECIAL TRUSTEE FOR AMERICAN INDIANS
Washington, D.C. 20240

December 6, 2001

Memorandum

To: Associate Deputy Secretary

From: Principal Deputy Special Trustee

Subject: Internet Disconnection Actions by the Office of the Office Special Trustee for American Indians

A December 5, 2001 Court Order instructed Interior to:

- Disconnect from the Internet Information technology systems that house or provide access to individual Indian trust data.

- Disconnect from the Internet all computers within the custody and control of the Department of the Interior, its employees and contractors, that have access to individual Indian trust data.

Following discussions late yesterday among senior Interior, BIA, CIO and OST management staff, at approximately 6 p.m. Eastern time on December 5, OST gave a "stand-by" order to the Albuquerque IT staff to prepare to effect the required disconnection. OST senior managers then awaited definitive guidance and clarification of the Court Order, remaining in contact with the IT staff over the next 1½ hours. At about 7:30 p.m., I learned that Mr. James Cason and Mr. Daryl White had telephoned the IT staff directly and instructed them to effect the disconnection. (Subsequently, I received a contemporaneous voice mail message from the Deputy Chief of Staff to contact her, or Mr. Cason, on this issue).

As of noon, December 6, 2001, OST has completed the following:

- On Wednesday evening, December 5, 2001, at approximately 7 pm Mountain Time, the OST router Access Control List (ACL) was modified to restrict access. No http traffic is allowed presently either in or out of OST's router.

- On Wednesday evening, December 5, 2001, at approximately 7 p.m. Mountain time, all modems (approximately 15) have been removed from PC's that had potential access to the LAN. Two modems on dedicated, stand alone PC's were not removed; these machines do not have access to the LAN and service GOALS, CashILink and ECS connections direct to Treasury. OST will isolate and closely monitor these applications on stand alone and dedicated PC's so we can continue to process ACH's and retrieve information from the Federal Reserve. OST will

examine other such applications (PACER, Polaris, etc.) with a view to establishing a work around not based on Internet technology.

- On Wednesday evening, December 5, 2001, at approximately 7 p.m. Mountain time, SEI was notified to discontinue access to StrataWeb, an internet-based system enabling Tribes to view Tribal account status.

- On Wednesday evening, December 5, 2001, at approximately 5 p.m. Mountain time, The Remote Access System Server (RAS) was shut down. With regard to impact, Wyondotte and Cherokee Tribes performing contracted/compacted IIM trust accounting functions are not able to access TFAS as normal through the Internet. Tribes who normally access Tribal account information through RAS will not be able to access TFAS to examine Tribal trust account status.

- On Wednesday evening, December 5, 2001, at approximately 7 pm Mountain time, OST's Lotus Notes Server was shut down, but brought back up at approximately 8 am Mountain time on Thursday, December 06, 2001, for OST intranet service only. A call has been placed to Lotus to determine how OST could encrypt all mail sent from the Lotus Server.

- The ACL was modified on OTFM's Cisco 7507 router. The RAS runs on a Dell Server running NT 4 service pack 6.

- OST's contractors DataCom, SEI, CDL, KPMG, and EDS have been notified and instructed to disconnect all linkages from the Internet to trust databases in their control. Follow up confirmation to validate these actions by the contractors is being initiated.

- OST's Office of Trust Records and Trust Risk Management have removed all modem connections to PC's that can access trust data or information. Likewise, servers containing trust data have been locked down. OST field staff are co-located with BIA elements and receive processing support through BIANET channels. BIA action to disconnect from the Internet covers OST field staff, with three exceptions. OST staff in Billings, Muskogee and Shawnee have been instructed to disconnect Internet access.

Impacts include:

- Inability to transfer funds from BIA to TFAS (IPAC).

- No lease processing until the NX comes back on line.

- No Per Capita processing until the NX comes back on line.

- Likely delays in processing trust check payments to allottees.

OST

ATTACHMENT A
POTENTIALLY RESPONSIVE DOCUMENTS
Office of the Special Trustee

Classification & Document Type	OST
Basic Financial Documents	
Activity Allotment Program	
Advice of Allocation/Other Authorization	
Advice of Allotment	
Advice of Check Issue Discrepancy	
Advice of Collections	
Application and Account for Advance of Funds	
Application for Allotment or Change in Allotment	
Apportionment and Allotment Schedules Transmittal	
Apportionment and Reapportionment Schedule	
Authorization	
BIA/IIM Accounts Purchase Order or Other Purchase Orders	
Bill for Collections/Collection Voucher	
Cancelled Check	
Check Carbon	
Check Register	
Claim Form	
Claims Against US/Proceed for Government Check	
Claims Disposition Notice	
Daily Advice of Status Card	
Daily Disbursement Report IISSDA	
Debit Voucher	
Deposit Ticket/Certificate of Deposit	
Field Receipt	
Financial Accounting System Code Sheet	
Guaranteed Remittance	
IIA or ISSDA Change Orders	
IIAA One Time Authorization	
IIAA Permanent or Voucher/Automatic Authorization	
IIAA Programmed Authorization	
IIM Data Change Notice	
IIM Jacket File	
Individual Indian Account Ledger	
Individual Indian Accounts Application (IIAA)	
Intra-Bureau Transfers	
IRS 1099 Interest Statement	
Journal Voucher	
Letter of Advice	
Lot Sheet	
Multi-use Standard Requisitioning/ISD	
Negotiated Check Copies	
Other Transfers and Corrections	
Public Voucher for Purchases and Services & Memorandum	
Public Voucher for Refunds & Memorandum	
Receipt for Cash-Subvoucher	
Receipt Log	
Reconciliation Statement of Funded Checking Account Maintained	
Redemption Authorizations and Schedule of Withdrawals and Credits	
Reimbursement Voucher	
Request for Individual's Social Security Number	
Request for Issuance of Replacement Check	
Request for Removal of Stop Payment	
Request for Stop Payment	

ATTACHMENT A
POTENTIALLY RESPONSIVE DOCUMENTS
Office of the Special Trustee

Classification & Document Type	OST
Schedule of Canceled or Undelivered Checks	
Schedule of Collections	
Schedule of Disbursements from an Agency Depository	
Schedule of Unavailable/Undelivered Check Cancellations and Credits	
Statement, Voucher & Schedule of Withdrawals & Credits	
Treasury Check Agency Recertification Follow-up	
Treasury Check Claims Document	
Unavailable Check Cancellation	
Voucher and Schedule of Payments	
Other As Identified	
Basic Supportive Documents to Financial Documents	
Claims	
Interest Calculations, Distributions & Related Documents	
Notice of Hearing	
Notice to All Persons Having an Interest	
Order Determining Heirs or Order Approving Will	
Permits (Surface, Mineral, etc.)	
Probates (Order Determining Heirs)	
Range Unit or Lease Income Report	
Other As Identified	
Production Supportive Documents	
Copies of Fax Data Transmittals/Notifications	
Correspondence	
Direct Pay Authorization and Documentation	
Orders or Decrees	
Supervised Account & Hold Documentation	
Transmittal Letters to BIA/OST Forwarding Checks	
Other As Identified	
Global System Reports (To be provided for inspection on-site)	
90 Day or Older Report	
A-17 Interface Reports (TFAS)	
Account listing by Area	
Automated Daily Reconciliation Reports (ADR-IRMS/TFMS)	
Automated Treasury Reconciliations (Treasury/OMNI/TFMS)	
Batch Proof List	
Check Payment & Reconciliation Report	
Check Register	
Compressed General Ledger	
Control Account Reconciliation	
Dailies (99 report)	
Daily Mini ledger (TFAS)	
Disbursements and Adjustments - ISSDA	
End of Day Report (TFAS)	
File Maintenance Memo	
General Ledger Detail List	
Historical List of Transactions (IRMS-IIM)	
Hold Account List	
IIM Account Payout Report (TFAS)	
IIM ACH file-day/night (TFAS)	

ATTACHMENT A
POTENTIALLY RESPONSIVE DOCUMENTS
Office of the Special Trustee

Classification & Document Type	OST
IIM Ledger Cards & Reports	
IIM Pooled Fund Report (TFAS)	
Interest Posted (TFAS)	
Interface Pre-Edits	
Investment Pool Confirmations and Documentation of Investment Transactions	
Investment Reports Related to IIM Pool (BOLT System)	
Investment Subsidiary Ledger Reconciliations	
Investment Subsidiary Ledger Reports (MoneyMax, etc.)	
IRMS / IIM Verification List	
IRMS / RDRS Distribution Transaction Listing	
IRMS / RDRS Error Recycle Control Report	
IRMS / RDRS Error Recycle Exception Report	
IRMS / RDRS Interest Report	
IRMS / RDRS MMS Transaction Control Report	
IRMS / RDRS Pre-Check Register	
IRMS Distribution Batch Pre-Edit	
IRMS Range - Error Report	
IRMS Range - Lease / Own Match, Distribution / Reconciliation	
IRMS Range - Own-IIM Match Verification	
IRMS Range - Permittee Listing	
IRMS Range - Post / Non-Post	
IRMS Range - Range Listing	
IRMS Range - Summary Accounts	
IRMS to Finance System ADR Reports	
Lease Posted (TFAS)	
Master File List/Transaction File List	
Missing Social Security Numbers	
Monthly Journal of Transactions	
Oil & Gas Posted (TFAS)	
OPAC, Payment Over Cancellations or Reclamation Credits	
Other IRMS Reports Not Listed	
Other OMNI/TFMS/Finance System Reports Not Listed	
Other TFAS Reports Not Listed	
Other Treasury Reports Not Listed	
Per Capita Posted (TFAS)	
Range Posted (TFAS)	
RFM Audit report (TFAS)	
Statement of Account & Mailed Sealed Copy (IRMS-IIM)	
Statement of Accountability	
Statement of Differences	
Statement of Financial Condition	
Statement of Funds in Account	
Statement of Transactions (SF1219)	
Statement of Transactions (SF224)	
Statement of Transactions According to Appropriations, Funds and Receipt Accts	
Total Average Daily Balance Report by Area & Update	
Transaction Registers	
Undisbursed Appropriation Account Ledger	
Undisbursed Appropriation Account Trial Balance	
US Treasury Check (Magnetic Tape & Treasury Transmittals)	
Other As Identified	

ATTACHMENT A
POTENTIALLY RESPONSIVE DOCUMENTS

Office of the Special Trustee

Classification & Document Type	OST

OST-OHTA

United States Department of the Interior

OFFICE OF THE SECRETARY
OFFICE OF HISTORICAL TRUST ACCOUNTING
1951 CONSTITUTION AVENUE, N.W., MS 16-SIB
Washington, D.C. 20240-0001
Phone (202)208-3405
Fax (202)219-1139

Via Hand Delivery

Memorandum

To: James Cason
Associate Deputy Secretary

From: Bert T. Edwards BertEdwards
Executive Director, Office of Historical Trust Accounting

Subject: *Office of Historical Trust Accounting - Access to Internet - IIM Trust Fund Data*

This will confirm my earlier conversation with you and Steve Griles on OHTA's connectivity. The OHTA does not have active Internet or any other electronic connection to Indian Trust Records. The only digital IIM records in our possession is on a CD-ROM disk(s) containing the IRMS information analyzed by Arthur Andersen for the DOJ. The consultant who has been examining data on these disks is out of the office today and tomorrow. We do not know if any of the IRMS data has been placed on the consultant's computer, a PC connected to the DOI LAN and having Internet access. However, to comply with the Court's Order, at 10:30 a.m. today, we disconnected this trust computer from the LAN connection and the computer is turned off. A note has been left on the machine instructing the consultant not to use the computer AT ALL, until we can verify that there are no trust records on the machine. The computer is in a locked office of a separately locked room.

Our contractor, NORC in Chicago, has been called to inform its contract administrator. However, NORC has no IIM records, nor access to DOI systems and no access to any data systems containing Indian Trust Records.

The person taking the action is Jeffrey P. Zippin, Deputy Director of OHTA, 202-208-5966. The action has been verified by Bert T. Edwards, Executive Director of OHTA, by visually inspecting the computer and its connections.

FWS
NPS

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

December 6, 2001

Memorandum

To: Associate Deputy Secretary

From: Special Assistant to the Assistant Secretary for Fish and Wildlife and Parks

Subject: Elouise Pepion Cobell, et. al. v. Gale Norton, et. al.

A review of National Park Service and U. S. Fish and Wildlife Service major information technology systems did not identify any such systems that housed or provide access to individual Indian trust data. Additionally, no employees or contractors of those two bureaus have access to individual Indian trust data.

This information was derived through contact with the Associate Director-Administration, NPS, the Chief Information Officer, NPS, and the Assistant Director, Business Management and Operations, FWS. These individuals provide oversight and management of major financial and information technology systems in the two bureaus and advise that such systems do not contain the previously referenced data or access. Additionally, in all cases these individuals contacted select managers and field stations and did not identify any referenced systems or data at those locations.

BIA

Trust Systems Shutdowns (Electrical & Telecommunication Connections) Managed by OIRM

Name:	**Integrated Records Management System (IRMS)**
Located	Reston, VA
Hardware:	Unisys NX 5621
Function:	IIM, Owner, Lease, Lease Distribution, People, Oil & Gas Royalties, Per Capita Payments
Disconnected by:	Thomas Farrow - 703/390-6335
Telecomm. Disc.	12/05/01 10:10 p.m.
Electrical Disc.	12/06/01 11:11a.m.
Verified by:	Robert Thompson - 703/390-6342

Name:	**Integrated Records Management System (IRMS) - Disaster Recovery System**
Located	Albuquerque, NM
Hardware:	Unisys NX 4620
Function:	IIM, Owner, Lease, Lease Distribution, People, Oil & Gas Royalties, Per Capita Payments
Disconnected by:	Gerald Lucero - 505/248-7150
Telecomm. Disc.	12/05/01 3:00 p.m.
Electrical Disc.	12/06/01 9:10 a.m.
Verified by:	Robert Thompson - 703/390-6342

Name:	**Remote Access Server (RAS)**
Located	Albuquerque, NM
Hardware:	3 Com Net Server
Function:	Remote access to all BIA systems
Disconnected by:	Gerald Lucero - 505/248-7150
Telecomm. Disc.	12/05/01 3:00 p.m. (approx.)
Electrical Disc.	12/06/01 9:00 a.m. (approx.)
Verified by:	Robert Thompson - 703/390-6342

Name:	**Trust Assets and Accounting Management System (TAAMS)**
Located	Dallas, TX
Hardware:	IBM AS400
Function:	Trust system management
Disconnected by:	Debbie McCloud - 817/360-5893
Telecomm. Disc.	12/05/01 7:05 p.m.
Electrical Disc.	12/05/01 7:05 p.m.
Verified by:	

Name:	**Land Records Information System (LRIS)**
Located	Denver, CO
Hardware:	IBM Multiprise 3000 (7060-H30) mainframe
Function:	Land title information showing and tracking Indian ownership, including System rights
Disconnected by:	Walter Jones - 303/969-7256
Telecomm. Disc.	12/05/01 7:43 p.m.
Electrical Disc.	12/05/01 7:43 p.m.
Verified by:	

Name:	**Lotus Notes (Webmail & SMTP Internet Mail)**
Located	Reston, VA
Hardware:	Dell servers
Function:	Electronic messaging
Disconnected by:	Eric Eskam - 703/390-6343

Internet Disc. 12/06/01 11:51 a.m.
Verified by: Kym Burns

Name: **Lotus Notes (Webmail & SMTP Internet Mail)**
Located Albuquerque, NM
Hardware: Dell servers
Function: Electronic messaging
Disconnected by: Eric Eskam - 703/390-6343
Telecomm. Disc. 12/06/01 11:51 a.m.
Verified by: Kym Burns

Name: **Data Cleanup for TAAMS**
Located Albuquerque, NM and coordinated with DataCom & BIA personnel at remote locations
Hardware: Servers, PCs
Function: Data Cleanup for TAAMS
Disconnected by: Frank White - 505/344-0072
Telecomm. Disc. 12/05/01 yesterday afternoon
Electrical Disc. 12/05/01 yesterday afternoon
Verified by:

Name: Management Accounting and Distribution System (MAD)
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.
Electrical Disc.
Verified by:

Name: Management Accounting and Distribution System (MAD)
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.
Electrical Disc.
Verified by:

Name: Management Accounting and Distribution System (MAD)
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.
Electrical Disc.
Verified by:

Name: Management Accounting and Distribution System (MAD)
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.

Electrical Disc.
Verified by:

Name: Management Accounting and Distribution System (MAD)
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.
Electrical Disc.
Verified by:

Name:
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.
Electrical Disc.
Verified by:

Name:
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.
Electrical Disc.
Verified by:

Name:
Located
Hardware:
Function:
Disconnected by:
Telecomm. Disc.
Electrical Disc.
Verified by:

Name: Osage Annuity System
Located Pawhuska, OK

Hardware:	Router & Power supply
Function:	Generates royalty disbursements for Oil & Gas at the Osage Reservation only
Disconnected by:	Melanie Quinton - 918/287-1032
Internet Disc.	12/06/01 10:30 a.m.
Verified by:	

Name:	
Located	
Hardware:	
Function:	
Disconnected by:	
Telecomm. Disc.	
Verified by:	

BLM

I, Michael Howell certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Michael Howell (acting)

Title Assistant Director, Information Resource Management

Organization Bureau of Land Management

Date 12/6/01

Attached is the description of the organizations efforts.

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White): Daryl White
When did they call: **6:00 PM MST 12/05/2001.**

Name of system(s) affected: **All Indian Trust Applications**

Where (H/W) system(s) located: **Nationwide**

Type of H/W: **Telecommunications and Computers (Wintell, IBM, and Sun)**

What Indian Trust data is housed there? **All - Detailed Response forthcoming**

What Indian Trust system(s) is run there? **All – Detailed Response forthcoming**

Name and telephone number of person who shutoff the Internet access: **Scott E. MacPherson BLM's National IRM Center Director (303-236-2925).**

Time they accomplished the shutoff: **Approximately 7:00 PM (MST) 12/05/2001**

How did they accomplish the shutoff: **Disabled all External Web or Telecommunications Access.**

External: Cut off Internet access

Actions: External Internet access to BLM's intranet (both inbound and outbound) was disabled at approximately 7 pm MST 12/5/2001.

External access to BLM's intranet through vDOINET was cutoff from DOI agencies at approximately 7 AM MST 12/5/2001.

Remote access to BLM internal systems through VPN access was shut down at 7 AM MST 12/06/2001.

Remote dial-up access is being monitored and was shut down at 9:00 AM 12/06/2001 MST.

Internet access to external BLM networks which are serviced from Internet Services Providers was shut down at approximately 10:00 AM MST 12/06/2001.

BLM has taken a broad based shut down to access. We are awaiting further instructions and assessing and inventorying all computers which would appear to fall under the nature of the court order. BLM will isolate all Indian Trust Management systems from all access until notified to do otherwise. We will have full mission critical functionality restored by 5:00 PM Mountain Time 12/6/01. BLM's internal email services are currently operable. We will update this as the day unfolds.

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

MMS

Memorandum of Record

To the best of my knowledge, based on the information provided to me, I, Walter Cruickshank, certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Walter D. Cruickshank

Title: For Acting Director, Minerals Management Service

Organization: Minerals Management Service

Date: Thursday, December 06, 2001

Minerals Management Service
December 6, 2001

DESCRIPTION OF MMS' EFFORTS TO DISCONNECT TRUST SYSTEMS FROM THE INTERNET

Who called to request: Daryl White, personal visit at 5:40 p.m. 12/5/01

Name of system(s) affected: Minerals Revenue Management (MRM) Financial Systems; CAMP Data Warehouse

Location: Lakewood, CO and Annapolis, MD

Type of Hardware: Unix and NT servers

What Indian Trust data is housed there? Lease level financial and production minerals revenue information.

What Indian Trust system is run there? MRM Financial and Compliance Systems

Name and telephone number of person who shutoff the Internet access:

Joe Lopez, Scott Fast – 6:00 p.m. 12/5/01 in Lakewood, CO. Remainder of connections by noon today, 12/6/01.

How did they accomplish the shutoff: Physical and machine level disconnects.

OSM

OFFICE OF SURFACE MINING
HALTING INTERNET ACCESS TO INDIAN FUND
DECEMBER 6, 2001

WHAT HAS BEEN DONE:

- OSM has eliminated Internet access to the Audit Fee Billing and Collection System (AFBACS), Fee Billing and Collection System (FEEBACS) and the Advanced Budget/Accounting Control and Information System (ABACIS) at their firewall for everyone outside of the Division of Financial Management in Lakewood, Colorado. In addition, FEEBACS and the Applicant Violator System (AVS) reside on the same computer and therefore, Internet access for AVS has also been eliminated.

- All of these systems are located at the Denver Finance Center in Lakewood, Co.

PERSON RESPONSIBLE FOR CLOSING DOWN SYSTEMS:

- Doug Simmons, Lakewood, Co. Telephone: 303-236-0330 X250

WHEN WAS THIS DONE:

- Internet access to the aforementioned was disconnected on December 5, 2001 Between the hours of 10:00pm and 10:30pm.

DESCRIPTION OF SYSTEMS:

- **AFBACS** – This system allows OSM to track information (accounts receivable) on funds owed to the Abandoned Mine Land Reclamation Fund based on the results of audits of coal companies. The system was developed to capture AML fees receivable (and associated fines, penalties, and interest) identified during the audit of an operator.
- **FEEBACS** – This system (accounts receivable) maintains information for approximately 25,000 mines, of which approximately 3,700 are actively producing coal. It keeps track of mines and their operational status. The system issues an OSM-1 form on a quarterly basis to every active mining operation for mine operators to use when filling their quarterly production data and payment.
- **ABACIS** – This is OSM's Core Administrative Accounting System. OSM uses this system as its system of record for all administrative accounting transactions processed by the Bureau. These transactions include obligations, invoices, payments, grants, receipts, investments, and bills processed by OSM.

* AVS – This system is used by OSM and the State Surface Mining Regulators to determine whether a permit applicant and its owner/controllers are responsible for any unabated federal or state violations of the surface mining law, and/or have outstanding unpaid civil penalties, Abandoned Mine Land Fees or audits.

WHAT IS THE EFFECT OF THIS ACTION:

- No one outside of DFM can access these systems.
- Auditors can't access AFBACS or FEEBACS to prepare for audits
- Budget and other staff within OSM can not access ABACIS
- OSM staff will not be able to match credit card purchases with billing information from Bank of America.
- Grantees can't access ABACIS to perform draw downs
- Since AVS and FEEBACS are on same computer, the AVS Office and States will not be able to access AVS for permit deny or issue recommendation information.

WHAT IS NEEDED:

- We need an exact definition of Indian Trust Data, because we are not sure the data in these systems should actually be considered Indian Trust Data without further clarification.

- Need to eliminate impact on Auditors and OSM staff that need to access these systems, by allowing them access to these systems based on their IP address.

WHAT HAS BEEN DONE TO WORK AROUND SYSTEMS BEING OFF-LINE:

- E-mail will be sent to all grantees informing them to FAX their draw down information to DFM. DFM will manually input the data and send the information to treasury and the grantee will receive the requested draw down on their Grant.

- The AVS office has been asked to telephone DFM with the permit application information. DFM will attempt to process the information and fax the recommendations back to the AVS Office.

MAJOR PROBLEM:

- The States will have a major problem with not being able to access the AVS and we can expect to receive telephone calls and perhaps complaints.

I, Donna K Scholz certify that none of the publicly accessible telecommunications networks of the USGS support Indian Trust activities. In cooperation with the December 5, 2001 court order, the USGS shut down the desktop PC and the file server where our documentation of our search for any potential Indian Trust information was filed. Neither system was publicly accessible. There were **no** Indian Trust information or data on these two systems.

Signature Donna K Scholz

Title Chief, Office of Information Services

Organization U.S. Geological Survey

Date December 6, 2001

Attached is the description of the organizations efforts.

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White):
Carol Aten, USGS Chief of Administrative Policy and Services.
She had been called by Chip Groat, USGS Director
He was called by Bennett Raley

When did they call:
I rec'd the call at 10:15pm, Dec 5, 2001

Name of system(s) affected:
Desktop of Ellen Findley and Novell file server IGSROCARLON

Where (H/W) system(s) located:
Ellen's desktop is in her office at USGS HQ in Reston, VA, the Novell server is in the server room in room 1P at the USGS HQ in Reston, VA

Type of H/W:
Desktop – Dell Dimension XPS
Novell Server – Compaq Proliant 5000

What Indian Trust data is housed there?
None. Only records of search by Ellen Findley were kept. No Indian Trust data or information are on Ellen's desktop or on the server.

What Indian Trust system(s) is run there? **None**

Name and telephone number of person who shutoff the Internet access:
We were told to shut down any computers that contained any information potentially relevant to the Indian Trust case, not Internet access.
Troy Miller
703-648-5383
Time they accomplished the shutoff: **11:39pm**
How did they accomplish the shutoff: **Orderly power down of the server. The desktop had been shut down late in the afternoon when Ellen left for the day.**

~~Request~~ verification ~~of~~ of the shutoff in the form of a Memorandum of Record (example attached)

USGS Computer Shutdown Court Order Status
December 6, 2001 – 8 a.m.

The USGS has no individual Indian money accounts responsibilities or information in its databases, on servers, on web sites or in any other computer compatible format. Nor does the USGS have access to Indian Trust electronic information on any DOI computer systems managed by the Department or its sister bureaus.

Ms Ellen Findley, the designated USGS team leader for the DOI Indian Trust case, has had responsibility for the thorough search of USGS paper and electronic archives. The progress of this search and all communications related to the search has been documented and has either been printed out in hard copy permanent archive, or stored on Ms Findley's desktop computer and a small partition of the network computer drive. These electronic records detail the search of USGS records, and do not contain any Indian Trust data or information.

In compliance with a court order issued on December 5, 2001, Ms Findley's desktop computer and the network file server where her files are stored were shut down at approximately 11:30 p.m on December 5, 2001. The entire Novell network file server volume that contains Ms Findley's files was backed up to tape at 10:30pm on November 28, 2001.

The shut down of this server has stopped critical operational functions at the USGS, it is recommended that the USGS make copies of the two Novell backup tapes from our archive for the convenience of the court. This will allow the USGS to continue its functional responsibilities related to monitoring the natural resources of the country. Downtime of this server leaves almost 600 USGS employees unable to perform their mission functions.

Novell Server Alternatives

1. Bring the Novell server back online and duplicate to CD all files in the directory accessed by Ellen Findley. Make this CD available for the convenience of the court. Return remaining employees to full functional service. Estimated time: 2 hours
2. Duplicate the November 28, 2001 full backup (in Novell Legato format) for the convenience of the court. Immediately return the Novell server to normal operation. Estimated time: Server up and operational within an hour, archive tape duplicated within 4 hours.
3. Back up the Novell server volume containing Ellen Findley's files and return all 600 employees to full service. Make the backup tape available to the court. Estimated time: 4 hours
4. Back up Novell server volume and "lock out" portion of server where Ellen Findley's files were written. Return everyone else in DO and APS to full service. Make backup tape available to the court. Estimated time: 5 hours

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-~~2340~~ 2360
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

USGS
science for a changing world

Fax Cover

Date: Dec 6

U.S. Department of the Interior
U.S. Geological Survey

Pages including this cover:

The USGS provides the Nation with reliable, impartial information about the Earth to minimize the loss of lives and property from natural disasters, to manage biological, water, mineral, and energy resources, to enhance and protect the quality of life, and to contribute to wise economic and physical development

To: Julia ~~Fo~~ Lewis

Fax: 202-501-2360 Phone:

From: Jonny Scholz

Email: dscholz

Mailing address:

Fax: 703-648-7112 Phone: -7119

Message:

I, Robert J. Quint certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Robert J Quint

Title Chief of Staff

Organization Bureau of Reclamation

Date 12/6/01

Attached is the description of the organizations efforts.

202-513-0308

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White): BENNETT RALEY, ASMB
When did they call: 8:22 PM EST
Name of system(s) affected: DISCONNECTED ALL SYSTEMS THAT ARE PUBLICALLY ACCESSABLE BY INTERNET AND THOSE CONNECTED TO THE DOI NETWORK
Where (H/W) system(s) located: → RECLAMATION-WIDE
Type of H/W: → ALL
What Indian Trust data is housed there? POSSIBLE REFERENCES IN WEB SITES
What Indian Trust system(s) is run there? ~~NONE~~ UNKNOWN
Name and telephone number of person who shutoff the Internet access: LINDA MARTINEZ 303 445 [illegible] RANDY FEUERSTEIN 303 445 3317
Time they accomplished the shutoff: 10:45 PM EASTERN
How did they accomplish the shutoff: DISCONNECTED AT THE ROUTER

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

Bureau of Reclamation
Office of the Commissioner
1849 C Street, N.W.
Washington, DC 20240
Phone: (202) 513-0540 Fax: 513-0308

Facsimile Transmittal

To: Julia Fax: 501-2340

From: Mike Gabaldon Phone: 513-0618

Re: Pages:

CC: Date 6Dec01

☒ Urgent ☐ For Review ☐ Please Comment ☐ Please Reply ☐ Please Recycle

2360

Based upon the certification of the system operator which is attached hereto,

I, Charles E. Breece certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Charles E Breece

Title Principal Deputy Director

Organization Office of Hearings & Appeals

Date 12/6/01

Attached is the description of the organizations efforts.

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White): Daryl White

When did they call: 5:45 p.m.

Name of system(s) affected: OHA Probate Tracking System

Where (H/W) system(s) located:
LCL Designs (contractor); St. Louis, Missouri

Type of H/W: Windows NT Server; Connected by T-3 lines to DOI/OHA

What Indian Trust data is housed there? BIA and OHA probate data which is used in connection with the determination of heirs in probate adjudications.

What Indian Trust system(s) is run there? OHA Probate Tracking System

Name and telephone number of person who shutoff the Internet access:

Lewis Lorenz - (918) 583-7865

Time they accomplished the shutoff: 9:00 p.m. central standard time

How did they accomplish the shutoff: Disabled File Maker Pro server service

Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)

I, LEWIS C. LORENZ certify that my systems that support Indian Trust activities have been removed from publicly accessible telecommunications networks.

Signature Lewis C. Lorenz

Title Owner

Organization LCLDESIGNS

Date 12-6-01

Attached is the description of the organizations efforts.

JIM CASON NEEDS THIS BY 10:30 am EST TODAY (DEC 6)
NO EXEMPTIONS - NO EXCEPTIONS

Description of your Organization's Efforts to
Disconnect Trust Systems from the Internet

Who called you to request (e.g. Steve Griles, Daryl White): Reni Hegmering
When did they call: 12-5-01 6:00 pm CST
Name of system(s) affected: PROBATE TRACKING SYSTEM
Where (H/W) system(s) located: ST. LOUIS, MO.
Type of H/W: WINDOWS NT SERVER
What Indian Trust data is housed there? IIM AMOUNTS AT DATES OF DEATH + SUBMISSI
What Indian Trust system(s) is run there? NONE. (PROBATE TRACKING SYSTEM)
Name and telephone number of person who shutoff the Internet access: LEWIS C. LORENZ 918-583-7865
Time they accomplished the shutoff: 9:00 PM 12-5-01
How did they accomplish the shutoff: DISABLED FILEMAKER SERVER SERVICE ON THE WINDOW NT OPERATING SYSTEM
Request verification of the shutoff in the form of a Memorandum of Record (example attached)

Send this completed form AND the Memorandum for Record by email and fax, with a confirmation phone call to Julia Laws.

Email: julia_laws@ios.doi.gov
Fax: 202/501-2340
Voice: 202/208-5444 (Julia)
202/208-6194 (Daryl's Secretary, Aileen Smith)
202/437-8427 (Julia's cell)

U.S. Department of the Interior
Office of Hearings and Appeals
4015 Wilson Boulevard
Arlington, Virginia 22203-1956

To: Julia Lawa

Fax Number: (202) 501-2340

From: Charles Breece

Telephone: (703) 235-3810

Date: 12/6/01

Pages: _____ including this cover memo.

FAX

Comments:

The information contained in this memo is confidential and /or privileged. This fax is intended to be reviewed only by the individual named above. If the reader of this transmittal page is not the intended recipient, you are hereby notified that any review, dissemination or coping of the information contained ·ein is prohibited. If you have received this fax in error, please notify the sender immediately. nk you.

Jean Maybee
12/06/01 11:16 AM
☐ Return receipt

To: Clark Debbie, Bill Roselius
cc: Bettie Rushing/ALBUQUERQUE/BIA/DOI@BIA
Subject: Confirmation Modem Lines are Disconnected

----- Forwarded by Jean Maybee/DC/BIA/DOI on 12/06/2001 11:14 AM -----

Bettie Rushing
12/06/2001 11:09 AM
☐ Return receipt

To: Jean Maybee/DC/BIA/DOI@BIA
cc: Janice Ruffin/DC/BIA/DOI@BIA, Colleen Florence/PHOENIX/BIA/DOI@BIA
Subject: Confirmation Modem Lines are Disconnected

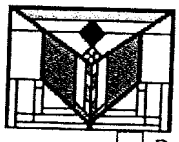
Jean, I am not sure who should receive this confirmation. The Albuquerque Security Office has one modem line that has not been used since last Spring when we returned the modem to OPM.

----- Forwarded by Bettie Rushing/ALBUQUERQUE/BIA/DOI on 12/06/01 09:04 AM -----

Janice Ruffin
12/06/01 07:58 AM
☐ Return receipt

To: Bettie Rushing/ALBUQUERQUE/BIA/DOI@BIA, Colleen Florence/PHOENIX/BIA/DOI@BIA, Antoinette Fragua/PHOENIX/BIA/DOI@BIA, Jackie Johnson/ALBUQUERQUE/BIA/DOI@BIA, Rebecca Valenzuela/ALBUQUERQUE/BIA/DOI@BIA, Sharon Garcia/ALBUQUERQUE/BIA/DOI@BIA, Michele Justice/ALBUQUERQUE/BIA/DOI@BIA, Alesia Thomas/DC/BIA/DOI@BIA
cc:
bcc:
Subject: *******Important Security Mandate**********

----- Forwarded by Janice Ruffin/DC/BIA/DOI on 12/06/2001 09:54 AM -----



Lynn Hopkins@DOI
12/06/2001 09:25 AM
☐ Return receipt

To: DC_CENTRAL OFFICE EAST_EMPLOYEES, DOI_ASIA_LAN
cc:
Subject: *******Important Security Mandate**********

At the direction of the Associate Deputy Secretary, Mr. Jim Cason, and the Assistant Secretary-Indian Affairs we have been tasked to locate all PCs with modems connected to them that are also connected to BIANet and disconnect the modem until further notice. **If you have a modem please UNPLUG IT IMMEDIATELY.** If you are not sure which is your LAN connection and which is your modem line, the modem line has a telephone jack on both ends. The LAN connection that plugs into your PC is much larger. If you get them mixed up you'll know immediately because you won't have any web, email or Novell connections.

All Regional Directors and Central Office Directors are being required to certify that organizations within their administrative organizations are complying with this and other mandates. If you have been tasked to locate modems or comply with any of the other requirements and have any questions about LAN or modem connections please contact the TAO office at 219-4249 or 219-4250 and they will assist you in any way they can.

Please be advised that any employee who may attempt to circumvent this order by connecting to

the internet via an outside line for any reason will be subject to disciplinary action up to and including termination of employment.

We request that you please be as patient and wait for further instructions and information. We will send you further information as soon as we can. Thank you for your cooperation in this matter and all others of this nature. Your response and cooperation in the past has been a great help and it makes our job much smoother.

Lynn A Hopkins
TAO Work Group Leader
202.208.1829

LAN TEAM
12/06/2001 12:33 PM

To:
cc:
Subject: Modem access

Pursuant to a Federal Court Order, you are required to **immediately disconnect** from the wall socket any telephone cable connected to any modem connected to your computer. This is to ensure that there is no possibility that a malicious hacker could use your computer to gain unauthorized access to Indian Trust systems or data. We apologize for the inconvenience, but require immediate compliance. Thank you for your understanding.

If you have any questions, please contact Roberta Heintz at 208-5148.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

DEC -7 2001

To: Jim Cason
Associate Deputy Secretary

From: Daryl W. White
Chief Information Officer

Subject: Meeting with Bureau and Office CIOs and IT Personnel

At noon today I held a meeting with Bureau CIOs, Deputy CIOs and Information Technology Chiefs to discuss their compliance with the Court's order of December 5, 2001, to disconnect from the Internet all systems and computers that house or have access to individual Indian trust data.

I stated to the attendees (listed below), "If I don't hear differently, I assume you disconnected from the Internet. Further, you are directed to remain disconnected until further notified." There were no disagreements with any statement.

The attendees were:

BIA	Debbie Clark, Acting CIO
FWS	Shane Compton, DCIO
BOR	Kathy Gordon, CIO (by phone)
BLM	Hord Tipton, CIO
NPS	Dom Nessi, CIO
OSM	Roy Morrison
MMS	Bob Brown, CIO
USGS	Donna Scholtz, DCIO
OHA	Bob More, Director
NBC	Roberta Heintz
	Bob Schiebel
OAS	Dan Stievson
SOL	Stephan Graves
OIG	Eddie Saffarnia

United States Department of the Interior
Office of the Special Trustee for American Indians
Trust Acquisition Support Services
505 Marquette N.W., Suite 1402
Albuquerque, New Mexico 87102
Phone (505) 248-6321 Fax (505) 248-6328

December 7, 2001

Science Application International Corporation
1710 SAIC Drive
ATTN: Hart Rossman - T 2-5-5
McLean VA 22102

Dear Mr. Rossman:

RE: LETTER CONTRACT NO. OST02CT0013 BETWEEN THE OFFICE OF SPECIAL TRUSTEE AND SCIENCE APPLICATIONS INTERNATIONAL CORP (SAIC)

This Letter Contract constitutes the preliminary contractual instrument authoring the contractor, SAIC, to begin services to design, implement and manage an information assurance infrastructure and information security management program for several critical function/system supporting the Department of the Interior. These services will commence November 6, 2001 in accordance with the attached Scope. Justification will follow to support a Determination of Unusual and Compelling Urgency.

The following contract clauses pertinent to this letter contract are hereby incorporated by reference by Citation Number, Title and Date in accordance with the clause at FAR 52.2522-2, CLAUSES INCORPORATED BY REFERENCE (FEB 1998).

52.216-23 Execution and Commencement of Work (APR 1984)
52.216-26 Payments of Allowable Costs Before Definitization (OCT 1997)
52.216-24 Limitation of Government Liability (APR 1984)
52.224-1 Privacy Act Notification
52.224-2 Privacy Act
52.239-1 Privacy or Security Safeguards
43 CFR 1452-224-1 Privacy Act Notification
Security Requirments (See attached)

(a) In performing this contract the contractor is not authorized to make expenditures or incur obligations exceeding $500,000.00.

(b) The maximum dollar amount for which the Government shall be liable if this contract is terminated is $500,000.00

52,216-25 Contract Definitization (OCT 1997)

(a) A Cost Reimbursement/Time & Materials contract is contemplated. The contractor agrees to begin promptly negotiating with the Contracting Officer the terms of a definitive contract that will include (1) all clauses required by the Federal Acquisition Regulation (FAR) on the date of execution of the Letter Contract. (2) all clauses required by law on the date of execution of the definitive contract and (3) any other mutually agreeable clauses, terms and conditions.

(b) The schedule for Definitization is:

On or before January 31, 2002.

(c)If agreement on a definitive contract to supersede this Letter Contract is not reached by the target date in paragraph (b) above or within an extention of it granted by the Contracting Officer, the Contracting Officer may, with the approval of the head of the contracting activity, determine a reasonable price or fee in accordance with Subpart 15.4 and Part 31 of the FAR 31 of the FAR, subject to contractor appeal as provided in the Disputes Clause. In any event the contractor shall proceed with completion of the contract, subject only to the Limitation of Government Liability clause.

(1) After the Contracting Officer's determination of price or fee, the contract shall be governed by---

(i) All clauses required by the FAR on the date of execution of this Letter Contract for fixed price, as determined by the Contracting Officer under this paragraph.

(ii) All clauses required by law as of the date of the Contracting Officer's determination; and

(iii) Any other clauses, terms, and conditions mutually agreed upon.

(2) To the extent consistent with subparagraph (c)(1) above, all clauses terms and conditions included in this Letter Contract shall continue in effect, except those that by their nature apply only to a Letter Contract.

Definitization of contract shall not exceed 180 days after the date of the LETTER CONTRACT or before 40 percent completion of the work to be performed, whichever occurs first. However, the Contracting Officer may, in extreme cases and according to agency procedures authorize an additional period. If, after exhausting all reasonable efforts, the Contracting Officer and the contractor cannot negotiate a definitive contract due to failure to reach agreement as to price or fee, the clause at 52.216-25 requires the contractor to proceed with the work and provides that

the Contracting Officer may, with the approval of the head of the contracting activity, determine a reasonable price or fee in accordance with Subpart 15.4 and Part 31, subject to appeal as provided in the Disputes Clause.

APPROVALS:

Carl Hotubbee, Bureau Procurement Chief — 12-07-01 — Date

Contracting Officer, Office of Special Trustee — 12-7-01 — Date

SCOPE OF WORK

The Department of the Interior has a requirement for support services to design, implement, and manage an information assurance infrastructure and information security management program in support of several critical functions/systems. The infrastructure shall serve as a trusted environment for users to access various sensitive information technology applications. This task is to identify the services required to develop a trusted information infrastructure and provide for the continued integrity of the systems through a comprehensive information security management program.

Require a system security capability for the Bureau of Indian Affairs (BIA) to utilize these services for the Trust Asset and Accounting Management System (TAAMS) as well as for other applications in the future.

Due to the highly sensitive nature of this system security is essential to include personnel security, information security and physical security in accordance with all DOI and Federal Regulations. It is also imperative that the trusted information infrastructure incorporate detailed logging mechanisms and an off site contingency backup.

CLAUSES FOR CONTRACTS INVOLVING ACCESS TO INDIAN TRUST DATA

What follows are both **mandatory clauses** (required by the Federal Acquisition Regulations and Department of Interior Acquisition Regulations) as well as **exemplary contract language** taken from existing contracts.

With respect to the **mandatory clauses**, each contracting office shall immediately review its existing contracts involving Indian trust data to ensure that these clauses are present in those contracts. If they are not, the contracts must be modified immediately to include these clauses in full text.

The **exemplary contract language** reflects the manner in which various contracting offices have implemented the requirements of OMB Circular A-130 and FAR Parts 24 and 39. There is a large degree of functional duplication between examples. Each contracting office should review its current contracts to determine the degree to which such language is already included in its affected contracts. To the extent that such implementing or clarifying language is lacking in present contracts, each contracting office should, as necessary and appropriate to each unique contracting situation, add identical or functionally similar language in appropriate places within affected contracts to best effectuate the purpose and intent of this language.

A. Mandatory Clauses

1. 52.224-1 PRIVACY ACT NOTIFICATION.

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

2. 52.224-2 PRIVACY ACT.

(a) The Contractor agrees to--

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies--

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of clause)

3. (43 CFR) 1452.224-1 **PRIVACY ACT NOTIFICATION**

(a) As prescribed in 1424.104, the clause at FAR 52.224-1, Privacy Act Notification, shall be modified before insertion into solicitations and contracts by -

(1) changing the title of the clause to read "PRIVACY ACT NOTIFICATION (JUL 1996) (DEVIATION)"; and

(2) adding the following sentence to the end of the clause:

"Applicable Department of the Interior regulations concerning the Privacy Act are set forth in 43 CFR 2, Subpart D. The CFR is available for public inspection at the Departmental Library, Main Interior Bldg., 1849 C St. NW, Washington D.C., at each of the regional offices of bureaus of the Department and at many public libraries."

(b) As prescribed in FAR 52.103(a) and 52.107(f), the clause at FAR 52.252-6, Authorized Deviation in Clauses, shall be inserted into solicitations and contracts containing the clause in (a) above.

(End of Clause)

4. 52.239-1 PRIVACY OR SECURITY SAFEGUARDS.

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(End of clause)

CONTRACTOR PERSONNEL SECURITY REQUIREMENTS FOR DOI/OST INFORMATION TECHNOLOGY CONTRACTS

In accordance with Federal law, Department of the Interior policies, each contractor and subcontractor employee will be subject to a background investigation under this contract, as determined by the Contracting Officer's Technical Representative (COTR) Security Program Office. In addition, every contractor and subcontractor employee, while working with DOI information technology systems, is required to receive a "favorable" screening prior to a grant of access to those DOI systems and records (see below for definition of "favorable screening").

1. Contractor Personnel Security Forms. Upon the written request of the COTR, the Security Program Office shall provide security forms to the contractor to be completed as soon as possible. The Security Program Office must provide those forms to the contractor. The contractor or subcontractor will be required to submit security forms for person directly associated with the requirement and determined to need a security clearance.

The following forms are required for screening and to initiate a background investigation:

(1) OPM Optional Form (OF) 306, Declaration of Federal Employment
(2) OPM Standard Form (SF) 85P, Questionnaire for Public Trust Positions
(3) FD 258, Applicant (Fingerprint Card)
(4) Release to Obtain Credit Information

The contractor shall ensure that each contractor employee completes and furnishes the completed security forms directly to the cognizant bureau security office. (This address can be obtained from the Contracting Officer or COTR.) Completed forms shall be submitted within a reasonable time (time to be mutually agreed upon by contractor, COTR or Security Program Office).

2. Investigative Requirements. Risk and investigative requirements, under this contract, are determined by the potential risk of the contractor's position or contractor activity, which has been designated by the Security Program Office. The risk for this contract is determined to be High or Moderate risk level. The scope and coverage of each background investigation is determined by Office of Personnel Management (OPM). The investigative background investigation is performed by OPM and in accordance with the appropriate level of risk. The cost of the investigative background investigation for each contractor employee is the burden and responsibility of the Government, NOT the contractor.

3. OMB Circular No. A-130 "Screening". The Security Program Office will assess whether each contractor employee's past conduct, as disclosed in the security forms, poses a risk of harm.

i. Notice of Favorable or Unfavorable "Screening" by Security Office.

a. The Security Program Office will notify the Information Technology (IT) -Security Officer (either verbally or in writing) whether each of the contractor employee's security forms have been favorably or unfavorably screened.
b. The IT Security Officer will provide to the COTR (in writing) the name of contractor employee(s) for who access has been granted or revoked

c. It is the responsibility of the COTR, to notify the Contractor (in writing) as soon as possible with the results of the "screening
d. The Contractor's personnel shall not have access to DOI information technology systems, until the IT-Security Officer has assigned a user-id number granting access to information technology systems.

4. Suitability Determination. Upon completion of the "Screening" by Security Program Office, coordination will occur between OST and OPM to conduct a background investigation for each individual contractor's employee(s) to determine suitability. Upon completion and receipt of the OPM investigative report, the Security Program Office will determine whether each contractor employee is determined to be suitable as provided by 5 CFR Part 731, Department of Interior – 441 Departmental Manual Chapter 5. This process involves assessment of the impact (or potential impact) of conduct on the performance of activities, including any indicated risk of abuse of the public trust in carrying out specific duties and activities.

5. Access to DOI Facilities and Information Technology Systems. Upon written justification, DOI reserves the right to deny a contractor and its employees and subcontractors, access to its facilities and/or information technology systems. Based upon information provided by contractor employee(s), information provided by the contractor or investigative information provided by the OPM, the Security Program Office may determine, at any time, a contractor employee is unsuitable to perform work under this contract and recommend revocation of access to the IT-Security Officer. Failure to complete and submit the required security forms or to truthfully answer all questions contained in the security forms shall constitute grounds for the denial or revocation of access to DOI information technology systems. Denial of access to DOI information technology systems or a determination the contractor employee is unsuitable does not preclude the Contractor from employing the individual in any capacity not associated with this contract.

6. Contractor Responsibilities Regarding Access to DOI Facilities and Information Technology. The contractor and subcontractors are responsible for immediately reporting to the Security Program Office (referenced above) of any circumstance which may affect the suitability of an individual for access to DOI information technology resources or determination of suitability. Contractors and its subcontractors are responsible for reporting changes in employee rosters, including new hires, terminations, transfers to positions which are unrelated to this contract to the COTR within ten (10) calender days of the change.

7. COTR Responsibilities. The COTR must direct all security concerns and issues directly with the Security Program Office. If, subsequent to the date of award of this contract, risk designation and investigative requirements are changed by the Government, and the changes cause an increase or decrease in contractor costs or otherwise affect any other term or condition of this contract, the COTR must notify the Contracting Officer in writing and the contract shall be modified, as if, the changes were directed under the Changes clause of the contract.

8. Contractor Identification Badges. The IT-Security Officer or any other designee will determine if there is a need to issue contractor identification badges to contractor or subcontractor employees who are working in DOI/OST offices where photo identification is required to gain access.

B. Exemplary Contract Language

Language of this kind may properly be inserted at Section "H" of most contracts, "Special Conditions" or "Special Contract Requirements." The contracts from which this language (some is abbreviated) is taken can be provided in full text upon request.

1. SECURITY REQUIREMENTS - [Agency]

In accordance with the [agency] security policy and Office of Management and Budget Directives, all contractor employees that have been identified as Risk and Sensitivity Designations working on [agency] requirements, must be granted a [agency] security clearance prior to commencement of work, unless such is temporarily waived by the [agency] Security Officer.

(a) *Personnel Clearances* The Contractor shall furnish to the [agency] Office of Security the following Bureau-supplied document on each person who will be directly associated with the requirement:

(1) Form OMB No. 3206-1082 - Declaration of Federal Employment
(2) Form OMB No. 3206-0191 - Questionnaire for Public Trust Positions
(3) Form OPM - SF 87 - FBI Applicant Fingerprint Card
(4) Resume of Employee

Additional security forms necessary for final clearance will then be provided to the successful offeror with a Conditional Notice of Award for each employee listed.

(b) *Access Security Clearance* All individuals requiring access to the [agency] shall complete and submit the required security investigative forms (security packet), to the COTR within 10 calendar, for use by the [agency] Office of Security.

(c) *[agency] Security* The [agency] reserves the right to deny access to its facilities and/or security systems [. . .] to any individual about which an adverse suitability determination is made. Failure to submit the required security investigation packet or to truthfully answer all questions contained in security investigation packets shall constitute grounds for denial of access clearance.

(d) *Contractor Responsibilities* The Contractor shall not provide access to employees, or subcontract employees, until written access clearance is provided by the Personnel Security Branch, Office of Security, [agency]. Contractors and subcontractors are responsible for reporting all changes concerning any of their employees, which may affect the suitability of their employees for access to the [agency] or placement in any of these positions including additions, or deletions, to the COTR within five (5) calendar days of the occurrence of the change.

(e) *COTR Responsibilities* The COTR shall maintain a current listing of access

requirements and provide that information to the Personnel Security Branch, [agency]. The Personnel Security Branch will inform the COTR of all access denials. Denial of access does not preclude employment of the individual concerned by the Contractor in any capacity not associated with the contract.

(f) *Changes to Security Requirements* If, subsequent to the date of award of this contract, the security requirements are changed by the Government, and the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of the contract, the contract shall be adjusted as if the changes were directed under the Changes clause of the contract.

(g) *Contractor Badges* [agency] security badges will be issued to all contractor staff located at the [agency] facilities.

2. DATA INTEGRITY AND SECURITY

Data pertaining to other contracts/services reside on information technology systems used by the Department of the Interior/Bureau of Indian Affairs. The contractor shall not divulge this information or use this information for the contractor's gain or shall not divulge any information to any other without written permission from the Director, [agency] IT office.

3. COMPUTER SECURITY REQUIREMENTS

a. The Contractor must meet the requirements of OMB Circular A-130, Appendix III, the Computer Security Act of 1987, and the [applicable agency security procedures]. Technological safeguards and managerial procedures shall be applied to assure that [agency] programs and data do not differ from their source format and content, and have not been accidently or maliciously altered, disclosed, or destroyed; and that [agency] clients, users assets, organizational assets, and individual privacy are protected.

b. The Contractor's facility must be physically secure and access must be controlled and limited to personnel with appropriate need.

c. All Contractor personnel dealing with [agency] data must have clearances appropriate for processing sensitive, proprietary, and mission critical data.

d. The Contractor's facility must be available to authorized [agency] personnel to conduct reviews and inspections on a periodic basis.

4. LIMITED DISTRIBUTION OR USE OF CERTAIN DATA AND INFORMATION

a. Performance of this contract may require the Contractor to have access to and use

of data and information which may be considered proprietary by other customers, or which may otherwise be of such nature that its dissemination or use, other than in performance of this contract, would be adverse to the interests of the Government and others.

b. The Contractor agrees that Contractor personnel will not divulge or release data or information developed or obtained in connection with the performance of this contract except to authorized Government personnel or upon written approval of the Contracting Officer.

* * *

5. RELEASES OF INFORMATION

a. Disclosure of information gained as a result of work performed under this contract shall be accomplished according to [agency] procedures. As used in this clause, the term "information" includes raw data, data derivative therefrom, and analysis or interpretations thereof, regardless of form. The term includes data developed or acquired by the Contractor during performance of this contract. * * *

b. The Contractor hereby agrees not to disclose such information to the public or to unauthorized parties without the prior written approval of the Contracting Officer. This restriction does not apply to releases of information to Subcontractors as necessary for successful performance of this contract provided that the Subcontractor agrees to be bound by the restrictions in this clause.

6. DISPOSITION OF MATERIAL

Upon termination or completion of all work under this contract, the Contractor shall prepare for shipment, deliver F.O.B. Destination, or dispose of all materials received from the Government and all residual materials produced in connection with the performance of this contract as may be directed by the Contracting Officer, or as specified by the provisions of this contract. All materials produced or required to be delivered under this contract become and remain the property of the Government.