IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 1:96CV01285
	)	(Judge Lamberth)
GALE NORTON, Secretary of the Interior, et al.,	)	
	)	
Defendants.	)	
	)	

NOTICE OF APPEAL

Notice is hereby given that all defendants in the above-named case hereby appeal to the United States Court of Appeals for the District of Columbia Circuit from the Preliminary Injunction and the Memorandum and Opinion entered in the above-named case on March 15, 2004, under Docket Numbers 2531 and 2530. A copy of the Preliminary Injunction and a copy of the Memorandum Opinion are attached.

Dated: March 22, 2004

Respectfully submitted,

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

/s/ Sandra P. Spooner
SANDRA P. SPOONER
Deputy Director
D.C. Bar No. 261495
JOHN T. STEMPLEWICZ
Senior Trial Counsel
Commercial Litigation Branch
Civil Division
P.O. Box 875, Ben Franklin Station
Washington, D.C. 20044-0875
(202) 514-7194

CERTIFICATE OF SERVICE

I hereby certify that, on March 22, 2004 the foregoing *Notice of Appeal* was served by Electronic Case Filing, and on the following who is not registered for Electronic Case Filing, by facsimile:

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

/s/ Kevin P. Kingston
Kevin P. Kingston

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action Number 96-1285 (RCL)**
	)	
GALE A. NORTON, Secretary of the Interior, et al.,	)	
	)	
	)	
Defendants.	)	
	)	

PRELIMINARY INJUNCTION

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

A. Definitions

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

1. **Information Technology System.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, including computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

2. **Individual Indian Trust Assets.** Particular lands, natural resources, monies, or other assets held in trust at a particular time by the Federal Government for a

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

3. **Management.** Actions that control, govern, administer, supervise, or regulate the use or disposition of Individual Indian Trust Assets.

4. **Federal Record.** This term is defined in 44 U.S.C. § 3301, and includes all documentary materials, regardless of physical form or characteristics, made or received under Federal law or in transaction of public business and preserved or are appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities or because of the informational value of the date in them.

5. **Individual Indian Trust Data.** Information stored in any Information Technology System that evidences, embodies, refers to, or relates to — directly or indirectly and generally or specifically — a Federal Record that reflects the existence of Individual Indian Trust Assets, and that either (1) was used in the Management of Individual Indian Trust Assets, (2) is a title or ownership record, (3) reflects the collection and/or disbursement of income from Individual Indian Trust Assets, (4) reflects a communication with a beneficiary (Individual or Tribe), or (5) was (a) created for the Bureau of Indian Affairs (BIA), Office of the Special Trustee (OST), or for a Tribe to use in the Management of Individual Indian Trust Assets; (b) provided to BIA, OST, or to a Tribe for use in the management of Individual Indian Trust Assets; and (c) used by the bureau or agency that created the record to manage Individual Indian Trust Assets.

6. **House.** The storage by electronic means of Individual Indian Trust Data.

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

B. Substantive Provisions

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

1. All Information Technology Systems within the custody or control of the U.S. Department of the Interior, and its employees, agents, and contractors, that House or Access Individual Indian Trust Data and are currently disconnected from the Internet must remain disconnected from the Internet and cannot be reconnected until such time as this Court approves their reconnection to the Internet.

2. All Information Technology Systems essential for the protection against fires or other threats to life or property may remain connected to the Internet. Interior shall, within 5 days of this date, provide declarations, sworn or in compliance with 28 U.S.C. §1746 and LCvR 5.1(h) specifically identifying any and every such Information Technology Systems that has remained connected to the Internet and setting forth in detail the reasons Interior believes such Information Technology System to be essential for the protection against fires or other threats to life or property. The Court will review such declarations, but absent a contrary order from the Court, such systems shall remain connected to the Internet.

3. The Office of Inspector General, the Minerals Management Service, the Bureau of Land Management, the Bureau of Reclamation, the Office of the Special Trustee, Fish and Wildlife, the Bureau of Indian Affairs, the Office of Surface Mining, and the National Business Center shall disconnect all Information Technology Systems within their respective custody or control from the Internet forthwith, whether or not such Information Technology Systems House or Access Individual

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

4. As the Court is satisfied the Information Technology Systems in the custody and control of the National Park Service, the Office of Policy Management and Budget, and the United States Geological Survey do not House or Access Individual Indian Trust Data, these agencies do not have to disconnect any currently connected systems from the Internet.

5. Interior may, at any time, submit a proposal to the Court for connecting the systems disconnected by this Order or any prior order of this Court to the Internet. Any such proposal must include all of the following: (1) a uniform standard to be used to evaluate the security of all Information Technology Systems within the custody or control of the U.S. Department of the Interior, its bureaus, its agents, and its contractors; (2) a detailed process whereby the uniform standard will be applied to each Information Technology System; (3) a proposed entity external to Interior and having no existing relationship with Interior that will perform the following functions: (a) evaluate the security of each Information Technology System that has completed the process set forth in (2); (b) submit a report to the Court setting forth its independent evaluation of the security of each Information Technology System; (c) monitor, on an ongoing basis, the security of the Information Technology Systems that the external entity determines House or Access Individual Indian Trust Data; and (d) submit monthly reports to the Court

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

6. Plaintiffs may submit the names and proposed plans of up to three entities that they submit can fulfill the requirements outlined in paragraph 5 (3).

7. Plaintiffs may, within ten (10) days of receipt, submit comments on any proposal submitted by the Department of the Interior in accordance with paragraph 5.

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

relevant Individual Indian Trust Data is secure, the Court will approve reconnection to the Internet for that Information Technology System. If the Court is not satisfied then that Information Technology System will not be reconnected to the Internet.

9. The Consent Order Regarding Information Technology, dated December 17, 2001, and stayed on July 28, 2003, remains stayed.

SO ORDERED.

Dated: March 15, 2004

/signed/
Royce C. Lamberth
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action Number 96-1285 (RCL)**
	)	
GALE A. NORTON, Secretary of the Interior, et al.,	)	
	)	
	)	
Defendants.	)	
	)	

MEMORANDUM OPINION

On July 28, 2003, the Court issued a preliminary injunction requiring the Department of the Interior to "immediately disconnect from the Internet all Information Technology Systems within [its] custody or control . . . until such time as the Court approves their reconnection to the Internet." Cobell v. Norton, 274 F.Supp.2d 111, 135 (D.D.C. 2003). In doing so, the Court carved out two exceptions: those systems impacting life or property and those for which Interior certifies "in accordance with Rule 11 of the Federal Rules of Civil Procedure" that "do[] not House or Access . . . Individual Indian Trust Data, and provide a specific justification thereof" or are "secure from Internet access by authorized users, and provide a specific justification in support thereof, stating in specific terms the security measures that are presently in place to protect unauthorized Internet access to the Individual Indian Trust Data that the Information Technology System Houses or provides Access to." Id. at 135-36.

On August 11, 2003 Defendants filed certifications attesting to the security of those systems in which individual Indian Trust Data resides or to the absence of such data on others.[1] The Court now considers those certifications and Interior Defendant's Submission Pursuant to the July 28, 2003 Preliminary Injunction Regarding Reconnection of Computer Systems, filed

[1] Twelve bureaus and sub-agencies filed certifications.

August 27, 2003, in light of Plaintiffs' responses and the entire record. Before doing so, however, it is necessary to recapitulate briefly the history of the parties' respective factual and legal positions concerning the state of information technology system security at the Department of the Interior and the impact of that IT system security on individual Indian trust data.

I. LEGAL BACKGROUND

Interior's obligation to maintain and preserve individual Indian trust data is well established and a corollary of the Secretary's statutory responsibility to: "(1) Provid[e] adequate systems for accounting for and reporting trust fund balances. (2) Provid[e] adequate controls over receipts and disbursements. (3) Provid[e] periodic, timely reconciliations to assure the accuracy of accounts. (4) Determin[e] accurate cash balances. (5) Prepar[e] and supply account holders with periodic statements of their account performance and with balances of their account which shall be available on a daily basis." 25 U.S.C. §§ 162a(d) (1994).[2] Interpreting these statutory responsibilities, this Court emphasized that "[t]he Indian Trust Fund Management Reform Act, 25 U.S.C. §§ 162a et seq. & 4011 et seq., requires defendants to retrieve and retain all information concerning the IIM trust that is necessary to render an accurate accounting of all money in the IIM trust held in trust for the benefit of plaintiffs." Cobell v. Babbit, 91 F.Supp.2d 1, 58 (D.D.C. 1999) (Cobell V).[3]

---

[2] The Secretary's obligations to retain and preserve individual Indian trust information finds support in commentary and case law. See 2 Scott, Law of Trusts, § 172 (3d ed. 1967); 2 G. Bogert, Law of Trusts and Trustees § 970 (rev. 2d ed. 1983); Restatement (Second) of Trusts § 173 (1959); Restatement (Third) of Trusts § 171 cmt. c (2003) (recognizing a trustee's general duty to provide information); Eddy v. Colonial Life Ins. Co., 919 F.2d 747, 750 (D.C. Cir. 1990) ("The duty to disclose material information is the core of a fiduciary's responsibility, animating the common law of trusts . . . [a]t the request of a beneficiary (and in some circumstances upon his own initiative), a fiduciary must convey complete and correct material information to a beneficiary"); Sec. Exch. Comm'n. v. Sargent, 229 F.3d 68, 76 (1st Cir. 2000) (recognizing "fiduciary duty to safeguard information relating to" trust).

[3] The Court further stated:

> Document management is the single biggest issue that must be comprehensively addressed if plaintiffs are to be assured any practical prospective assurance that their trustee will be able to give them an accurate accounting. As the Acting

On that score, the D.C. Circuit affirmed "[t]he government's broad duty to provide a complete historical accounting to IIM beneficiaries" and the "obligations on those who administer the IIM trust lands and funds to, among other things, maintain and complete existing records, recover missing records where possible, and develop plans and procedures sufficient to ensure that all aspects of the accounting process are carried out." Cobell v. Norton, 240 F.3d 1081, 1105 (D.C. Cir. 2001).

It is against this backdrop that the Court analyzes the Secretary's duty to maintain and preserve individual Indian trust data residing on Interior's IT systems, the certifications offered by Interior's agents, and Interior's proposal for the future.

II. PROCEDURAL BACKGROUND

On April 4, 2000, the Court remarked that it was "alarmed and disturbed by the revelation that BIA had no security plan for the preservation of [trust] data . . . that BIA has now placed itself in the incredible position that it cannot now create such a plan with its own employees, but that it can do so only if this Court allows BIA to go forward with these government contractors creating the plan, and then insuring that this critical data is preserved and protected." (Hr'g Tr. 11-12, Apr. 4, 2000). As of November 14, 2001, "nothing has changed." Report and Recommendation of the Special Master Regarding the Security of Trust Data at the Department of the Interior at 141 (Nov. 14, 2001). After reviewing and analyzing countless reports and studies performed by both government and private organizations, the Special Master observed that critical data of concern to individual Indian beneficiaries were housed on systems that have:

> no firewalls, no staff currently trained/capable of building and maintaining firewall devices, no hardware/software solution for monitoring network activity including but not limited to hacking, virus and worm notification. . . . [and] a

---

> Special Trustee testified, "[t]he records are the base for the entire trust operation."
>
> The missing-data problem is undoubtedly the single biggest obstacle that Interior will face in rendering an accurate accounting . . . Clearly, the destruction of necessary trust documents will make defendants' statutory task of rendering an accurate accounting impossible.

Cobell V at 14, 43 (internal citations omitted).

> serious lack of wide area networking and security personnel in general. The BIA is also far behind the other bureaus in Interior regarding staffing of messaging systems and infrastructure support.

Report and Recommendation of the Special Master Regarding the Security of Trust Data at the Department of the Interior at 141 (Nov. 14, 2001) (quoting FY 2003 Budget Request to the Department Bureau of Indian Affairs Trust Reform – Information Resources Technology (COP), Statement of Problem/Current Condition).

In reaction to the Special Master's report, on December 5, 2001, the Court ordered "that defendants shall immediately disconnect from the Internet all information technology systems that house or provide access to individual Indian trust data" and "that defendants shall 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." T.R.O. at 2 (Dec. 5, 2001).[4]

On December 17, 2001, at the behest of Interior,[5] the Court entered a Consent Order Regarding Information Technology Security ("Consent Order"), modifying the December 5, 2001 temporary restraining order. The Consent Order provided, among other things, that "Interior shall not reconnect any information technology system to the Internet without the concurrence of the Special Master as provided herein," Consent Order at 5, and that

> the Special Master shall verify compliance with this Consent Order and may conduct interviews with Interior personnel or contractors or conduct site visits wherever information technology systems or individual Indian trust data is housed or accessed. Each party will have the opportunity to have at least one counsel present at such interviews or site visits, and any additional personnel permitted by the Special Master. The Special Master will provide notice to counsel for both parties in advance of such interviews or site visits, but such notice may be limited to the minimum necessary for counsel to make arrangements to attend. Unless

---

[4] Three days later, the Court modified the temporary restraining order to allow Interior to "reconnect to the Internet, within 24 hours of notice to the Special Master and plaintiffs' counsel with appropriate documentation, any information technology system that does not house individual Indian trust data and that does not provide access to individual Indian trust data." Order Providing Partial Relief From T.R.O. at 1 (Dec. 8, 2001).

[5] It bears noting that it was Interior who proposed that the Court adopt the Consent Order in lieu of entering the preliminary or permanent injunction proposed by Plaintiffs.

> expressly permitted by the Special Mater in writing, counsel shall not inform their clients or any third parties about such interviews or site visits in advance[.]

Consent Order at 7-8.

In accordance with the Consent Order, the Special Master retained the services of IBM and subsequently, in March 2002, the Security Assurance Group ("SAG") to conduct independent site risk assessments and external penetration testing in connection with the Consent Order. Both contractors assessed and validated the computer security posture of Interior's systems by conducting site visits to those Department of Interior bureaus and agencies requesting re-connection to the Internet and by performing external penetration testing of Interior's networks pursuant to rules of engagement agreed to by the Special Master and the Department.

Between March 2002 and July 28, 2003, SAG's investigations identified numerous vulnerabilities exposing individual Indian trust data to uninvited review and manipulation.[6] For example, SAG conducted penetration testing against the Bureau of Land Management ("BLM") from February 10, 2003 through March 26, 2003. According to its report, "throughout all Phases of the testing (I through IV), no effort was made by BLM administrators to restrict, block, or deny access from the source of the attacks. SAG believes that none of SAG's activities were detected at any time." Internet Assessment of DOI/BLM Networks at 1 (Mar. 27, 2003). In contrast, the BLM certification to this Court on August 11, 2003 indicates that "[a]t present time, the IDS logs are monitored by network security personnel on a daily basis." BLM Certification at 34.[7]

---

[6]SAG generated reports documenting the results of each site visit or penetration testing. These reports are part of the record of this case and were filed under seal on February 10, 2004 after being redacted by SAG and Interior. In citing these reports the Court specifically refrains from disclosing any technical details that might compromise security at Interior and instead provides only enough information to show that SAG uncovered many problems that were not fixed.

[7]In response to a request from the Court, on February 12, 2004 defendants filed Defendants' Comments on the Information Technology Security Reports Filed by the Special Master in Accordance with this Court's January 21, 2004 Order (As Modified on January 22, 2004) ("Defendants' Comments on IT Reports"). In that filing defendants recite certain corrective measures taken after SAG issued the aforementioned report. But the Court observes that such measures came as a result of oversight and testing by the Special Master's contractors not on

During the three separate site visits performed of the Minerals Management Service office in Camarillo, California vulnerabilities were continually being identified. The Special Master's team conducted the last such visit in March 2003 during which time vulnerabilities identified in earlier reports were identified as not being remedied. The team again identified and documented the vulnerabilities in a report delivered to the Special Master. See Assessment of Minerals Management Service - Camarillo revisit (Mar. 26, 2003). Interior admits these vulnerabilities were not remedied. Defendants' Comments on IT Reports at 4 n.7. Apparently, since SAG did not recommend this office disconnect from the Internet Interior believes that it should take no steps to remedy a known weakness. It is precisely this sort of minimalist band-aid approach that has led to Interior's repeated "F" grades and put IITD at risk[8]

Similarly, in March 2003, SAG identified many of the same vulnerabilities identified during a previous visit to the Bureau of Reclamation office located in Sacramento, California in March 2002. See Assessment of Bureau of Reclamation - Sacramento revisit (Mar. 24, 2003). Again, during one of its site visits, the Special Master's team inspected the Office of Surface Mining contractor's office in Cannonsburg, Pennsylvania on May 13, 2003. It identified that the Intrusion Detection System had not been monitored or reviewed by anyone for approximately forty-five days and that an additional system was connected to the Internet for twenty-six days with no Intrusion Detection System implemented at all. See Office of Service Mining – Pittsburgh Revisit (June, 2003). This finding is particularly relevant in light of subsequent findings by the Interior's Office of Inspector General that outsourced websites and contractor managed applications were not included in Interior's internal inventory of systems. Thus these types of vulnerabilities remain unaccounted for and therefore uncorrected by Interior.[9]

Interior's own initiative and furthermore that the Court has no means to verify the efficacy of any such corrective actions. See Defendants' Comments on IT Reports at 14-15.

[8]See Section IV.C, infra.

[9]Even though this report was issued in May 2003, as of February 2004 Interior cited no corrective actions of the problems identified. See Defendants' Comments on IT Reports at 21; See also

The aforementioned examples underscore the continuing concern this Court harbors for the security of individual Indian trust data.

The collaborative process between Interior and the Special Master operated effectively. Interior and the Special Master cooperated to allow the reconnection of almost 95% of Interior's systems within one year of the December 5, 2001 shutdown. This cooperation continued until the April, 2003 incident regarding penetration testing at the Office of Surface Mining. The July 28, 2003 opinion chronicles the breakdown in cooperation between Special Master and Interior and the proximate events that led to the entry of the preliminary injunction. The tension between the Special Master and the agency appears to have been precipitated by the Special Master's inquiry into the "unplugging" of a cable from the Office of Surface Mining server at the exact time the agency was aware the Special Master's contractor was performing penetration testing on that system. See 274 F.Supp.2d at 114-24.

In its July 28, 2003 Opinion the Court concluded that "the parties continue to be at an impasse as to the manner in which the Consent Order should be implemented. . . . the Court has no confidence that this impasse will be resolved. In response . . . the plaintiffs have moved for the entry of a preliminary injunction that would return the parties to the status quo that existed prior to the entry of the Consent Order." 274 F.Supp.2d at 126.

The Court evaluated the request for a preliminary injunction and concluded that while injunctive relief was warranted, the precise nature of the relief would be different from that requested by plaintiffs. Rather than disconnect from the Internet all Interior Department computer systems that either house or permit access to individual Indian trust data as the plaintiffs requested, the Court determined that it would in effect permit Interior to disconnect only those systems that Interior thought were insecure and to provide certifications to the Court explaining why the systems connected to the Internet were secure. The Court would then assume the responsibility previously held by the special master of reviewing the information on each system

---

section IV.C, infra.

and determining if a connected system should stay connected as well as determining new requests to connect to the Internet. Id. at 133, 136.

The July injunction makes clear that it is creating at minimum a two stage process. In stage one, Interior is ordered to make its own determinations as to the security of its IT systems and to shutdown any insecure systems that house or access individual Indian trust data. For those systems Interior determines are secure, the Department is to provide a certification to the Court explaining the security measures in place. In stage two, the preliminary injunction anticipated that the Court would evaluate the certifications and then determine based on the record whether the systems should remain connected. Furthermore the Court would evaluate any plan submitted by Interior to control the process of reconnecting other systems that remain disconnected. The July injunction made clear that the Court intended to rely on information provided by Interior in making its determination. But the certifications that Interior filed mocked this Court's injunction and its request for information. All of the certifications were procedurally and substantively defective. They were not properly subscribed as true as required by local rule and statute and the very Interior officials who drafted the reports simultaneously gave conflicting information to other government agencies such as the Office of Management and Budget and the General Accounting Office stating that Interior's IT systems were in fact vulnerable. These deficiencies will be discussed more fully below. See section III, IV, supra. In late September 2003, before this Court had made its determinations as to whether any systems should remain connected or be disconnected, Interior filed an appeal of the July injunction.[10]

---

[10]The Court observes at the outset that the normal rule is that a party's filing of a notice of appeal divests the district court of jurisdiction over the matters being appealed. Griggs v. Provident Consumer Discount Co., 459 U.S. 56, 58 (1982). But a district court is not deprived of jurisdiction to modify a preliminary injunction while that injunction is on appeal. Fed. R. Civ. P. 62(c) (2003) ("When an appeal is taken from an interlocutory or final judgment granting, dissolving, or denying an injunction, the court in its discretion may suspend, modify, restore, or grant an injunction during the pendency of the appeal upon such terms as to bond or otherwise as it considers proper for the security of the rights of the adverse party."); see also Sec. Indus. Ass'n v. Bd. of Governors of the Fed. Reserve Sys., 628 F.Supp. 1438, 1440 n.1 (D.D.C. 1986) (noting that pending appeal district courts continue to "retain jurisdiction to . . . modify, restore, or grant injunctions" (citing Venen v. Sweet, 758 F.2d 117, 120 n.2)); Bd. of Educ. of St. Louis v. State

III. INTERIOR'S CERTIFICATIONS TO THE COURT

On August 11, 2003, Interior submitted certifications attesting to the fact that its agencies' computers either housed no individual Indian trust data or were secure from outside intrusion. As demonstrated below, the certifications provided the Court are both facially and substantively inadequate as well internally inconsistent. It is based on these certifications that the Court must conclude that individual Indian trust data residing on Interior's computers remain vulnerable to external penetration and that such systems cannot remain operational.

A. Certifications Violate Local Rules and Federal Statute and Cannot Be Considered In Support of Interior's Position.

The Court ordered that those systems Interior wishes to remain connected must be supported by a certification that those systems "do[] not House or Access [] Individual Indian Trust Data and provide a specific justification thereof" or are "secure from Internet access by authorized users, and provide a specific justification in support thereof, stating in specific terms the security measures that are presently in place to protect unauthorized Internet access to the Individual Indian Trust Data that the Information Technology System Houses or provides Access to." 274 F.Supp.2d at 135-36. The preliminary injunction specified that the Court "will decide on the record before it whether a Reconnected System shall remain connected to the Internet, and will decide all future applications for reconnection." Id. at 136.

Plaintiffs object to the unsworn certifications submitted by Interior's agencies as not conforming to Local Civil Rule 5.1(h).[11] Rule 5.1(h), which parallels Federal statute 28 U.S.C. §

---

of Missouri, 936 F.2d 993, 996 (8th Cir. 1991) (holding that the district court could grant substantial injunctive relief during the pendency of an appeal in an education desegregation case because the court of appeals believed that the nature of the district court's ongoing supervision over the integration of vocational educational programs required it to retain the broadest discretion possible).

[11] Local Rule 5.1(h) of the United States District Court for the District of Columbia provides:

> Whenever any matter is required or permitted by law or by rule to be supported by the sworn written statement of a person . . . the matter may, with the same force and effect, be supported by the unsworn declaration, certificate, verification, or statement, in writing of such person which is subscribed as true under penalty of

1746 (2003)[12] in both form and substance, provides that where any rule, regulation, order, etc. requires any matter to be supported by a sworn declaration an unsworn declaration, certificate, verification or statement in writing, subscribed as true under penalty of perjury, in statutory form, may support the matter asserted. See Thomas v. United States Dept. of Energy, 719 F.2d 342, 344 n. 3 (10th Cir.1983) (interpreting 28 U.S.C. §1746). Indeed, courts have repeatedly emphasized that unsworn statements submitted to the court not in conformity with 28 U.S.C. § 1746 (or, by extension, Local Civil Rule 5.1(h)) will not be considered. See, e.g., Mumme v. United States Dept. of Labor, 150 F.Supp.2d 162, 169 (D.Me. 2001) ("To gain access to information about one self through the mail, a claimant first must send the relevant Department component a request with 'an example of his signature, which shall be notarized, or signed as an unsworn declaration under penalty of perjury,' pursuant to 28 U.S.C. 1746.").

On July 28, 2003, the Court ordered that Interior certify as to the security of its systems upon which individual Indian trust data resides. That order required Interior to conform to both local rules and federal statute and provide, in lieu of a sworn affidavit, a certification that attested to the truth of the agency's averments under penalty of perjury. Instead, Interior filed

---

> perjury, and dated, in substantially the following form: . . . (2) If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)".

Loc. Civ. R. 5.1(h) (2003).

[12] 28 U.S.C. §1746 (2003) provides:

> Wherever, under any law of the United States or under any rule, regulation, order, or requirement made pursuant to law, any matter is required or permitted to be supported, evidenced, established, or proved by the sworn declaration, verification, certificate, statement, oath, or affidavit, in writing of the person making the same . . . such matter may, with like force and effect, be supported, evidenced, established, or proved by the unsworn declaration, certificate, verification, or statement, in writing of such person which is subscribed by him, as true under penalty of perjury, and dated, in substantially the following form: . . . (2) If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date)."

certifications attesting to the presence of individual Indian trust data or the security of systems housing trust based on nothing more than "knowledge, information, and belief."[13] It is unrefuted that securing individual Indian trust data is central to the trust. Notwithstanding, agency representatives refused to certify to the security of their systems under penalty of perjury. This reticence naturally begs the question why, if the facts as stated in the submitted "certifications" are accurate, Interior refuses to assure the Court in the manner prescribed by local rules and federal statutes.[14] The Interior's reluctance in this regard makes it apparent it will not stand by its assertions. They can not and, therefore will not, be considered.

B. Certifications Provide Conflicting Information on the Current State of Interior's IT Security.

Interior submitted in excess of 900 pages responding to the preliminary injunction. The information represented in these pages is often confusing and contradictory. For example, attached to the certification provided by the Bureau of Land Management was a report entitled Trust Enterprise Architecture, Trust Systems Internet Connectivity Report, Information Resource Catalog (August 11, 2003) ("IRC Report"). Appendix A to the IRC Report, "a table of the current baseline Trust systems and the Internet connectivity status of each," IRC Report at 3 (emphasis added), reveals that the Automated Fluid Minerals Support System ("AFMSS"), as of

---

[13] Loc. Civ. R. 5.2(i) states: "A paper that does not conform to the requirements of this Rule and Rule 10(a) of the Federal Rules of Civil Procedure shall not be accepted for filing."

[14] Interior cannot claim ignorance or accident. Following the entry of the aforementioned December 5, 2001 T.R.O. Interior filed an emergency motion for partial relief. The Court granted immediate relief to the National Interagency Fire Center ("NIFC") and the United States Geological Survey ("USGS") and allowed them to reconnect to the Internet and submit verifications immediately thereafter. David Potter of the NIFC filed a declaration in support of that motion stating that the NIFC did not handle trust funds and included the appropriate statement: "I declare under penalty of perjury that the foregoing is true and correct." Likewise, Kathryn Clement filed a declaration in support of the USGS that concluded "I declare under penalty of perjury that the foregoing is true and correct." Interior has even had the impudence to attach the 2001 declaration of Kathryn Clement to their current certification with its insufficient verification. From where sprung the misconception that this Court had authorized a novel form of certificate is unknown as indeed this Court has not authorized any deviation from statute or local rule.

August 11, 2003, had "No Internet Connectivity."[15] Yet in the BLM Certification, Executive Summary, the agency represents that AFMSS has "been operating under an Interim Approval to Operate that was initially issued in March 2002 and extended in October 2002" and was only disconnected from the Internet between June 27, 2003 and July 28, 2003. By its own admission, after July 28, 2003, "BLM was authorized to reconnect the systems disconnected under the June 27, 2003 Temporary Restraining Order based on its IT security." BLM Certification at 15. On this record, the Court is without basis to determine whether, at the time the certification was filed, AFMSS was connected or not. Approval based on this type of inconsistent record can not be granted.[16]

IV. INTERIOR'S PROPOSAL FOR APPROVING FUTURE RECONNECTIONS AND MONITORING EXISTING RECONNECTED SYSTEMS

The preliminary injunction ordered Interior to "file with the Court a proposal setting forth a method of approving individual reconnections of disconnected Interior computer systems, and of determining whether the Reconnected Systems should stay reconnected." 274 F.Supp.2d at 136. On August 27, 2003 Interior submitted Interior Defendant's Submission Pursuant to the July 28, 2003 Preliminary Injunction Regarding Reconnection of Computer Systems ("Interior

---

[15] AFMSS "is a major computer software application that supports statutory and regulatory requirements for oil and gas development on public and Indian lands." Appendix A to IRC Report at 1. AFMS users "include the BLM, MMS, BIA in the Department of the Interior and the U.S. Forest Service, Department of Energy, State governments and the private sector." BLM Certification, Executive Summary at 18.

16 Beyond this, the agency's insistence that, "[b]ecause the BLM's IT systems are secure against unauthorized access from the Internet, it should remain connected to the Internet," is ironic. BLM Certification at 2. In the first instance, BLM bolsters its position with the representation that, "on July 9, 2003, BLM's acting CIO signed a memorandum to the BLM Director that stated that BLM's external perimeter network security had been certified in accordance with Office of Management and Budget Circular A-130, Appendix III." Id. at 26. What BLM fails to reconcile is that its certification was done by the BLM's own CIO. and that "[o]n March 27, 2003 the Special Master's contractor conducted penetration testing on four BLM web servers. . . [and] [t]hey were able to successfully penetrate these servers." Id. at 24-25. Interior asks the Court to believe that only 15 weeks after its systems were readily penetrated, it was secure from outside penetration in compliance with OMB Circular A-130 Appendix III. It further asks the Court to do so based solely on the unsworn statements of its supervisors. This, the Court will not do.

Proposal").

A. Problems With Interior's Proposal

1. Interior Must Use a Uniform Standard to Evaluate the Security of Individual Indian Trust Data

The preliminary injunction specifically required that "[t]he proposal should demonstrate a method of providing to the Court adequate evidence that the Reconnected Systems and the Information Technology Systems disconnected pursuant to this Order are secure against Internet access by unauthorized users." Id. at 4. This Court expects Interior to evaluate the security of its IT systems according to a uniform standard and with uniform methodologies.

The problems begin with Associate Deputy Secretary James E. Cason's statement that:

> Interior does not recognize there to be a fixed test or set of standards, guidelines, or technologies that distinguish between an IT system that is "secure" and one that is "not secure." Similarly, Interior has not found a uniformly accepted minimum standard within the Federal Government for IT information security or for Internet connectivity security . . . Interior's IT security policies provide internal direction that the bureaus and officers are expected to follow, but do not purport to establish requirements that determine whether an IT system is "secure" or "not secure," for purposes of justifying connectivity to the Internet.

Decl. of James E. Cason at 5-6 (Aug. 11, 2003). Thus, it will be "Interior's bureau and office heads and Chief Information Officers" who will determine "whether an IT system is 'secure' for purposes of deciding whether or not to connect to the Internet." Id. at 4-5. Interior will "provide reconnection submissions to the Court describing the analysis undertaken by the bureau or office and the basis for the conclusion that the subject IT system is secure from Internet access by unauthorized users." Id. at 4.

The Financial Management Status Report and Strategic Plan FY 2004—FY 2008 ("FMSRSP")[17] submitted by the Department of the Interior to the Office of Management and Budget on September 8, 2003 completely contradicts Associate Deputy Secretary Cason. It

17 This report is attached as an exhibit to Plaintiffs' Notice of Supplemental Authority In Support of Comments Filed By Plaintiffs On August 27, 2003 and September 10, 2003 Regarding This Court's Preliminary Injunction, (Sept. 17, 2003), available at http://www.doi.gov/pfm/5year2004/index.html.

states:

> On June 16, 2003, Interior's CIO Security Office completed and delivered the final version of Interior's [Certification & Accreditation] guide, which outlines Interior's C&A process based on NIST Special Publication (SP) 800-37. An Interior OCIO bulletin on C&A roles and responsibilities was also developed and released on April 11, 2003. A major goal of Interior's IT security program is to achieve C&A of its IT systems in full compliance with OMB Circular A-130, Appendix III. Interior's Indian trust IT systems, i.e., those systems identified as supporting trust business processes, are scheduled to achieve C&A compliance by December 31, 2005.

FMSRSP at 66. Based on this representation, Interior does possess a department-level, uniform standard for evaluating IT security within its bureaus and intends to certify and accredit its individual Indian trust data systems by 2005 – facts not mentioned in any certification to this Court.

The central importance of individual Indian trust data mandates a single uniform standard for determining whether such data remains secure from outside influence rather than the bureau by bureau balancing approach offered by Interior under the guise of 44 U.S.C. §3544 (2003). Since Interior has already developed a such a standard and is preparing to implement it department wide, without more, it appears more efficient and more effective for this Court to take advantage of such a standard in evaluating the security of individual Indian trust data. As to this issue, therefore, Interior's proposal is unacceptable.

2. Verifying Representations of Security Must Be Done By An Independent Entity

The Preliminary Injunction further requires that Interior's proposal "provide a means to verify the representation that the Reconnected Systems and the Information Technology Systems disconnected pursuant to this Order are secure against Internet access by unauthorized users." 274 F.Supp.2d at 136. The Court included this requirement in the preliminary injunction because throughout this case Interior has time and again failed to take proactive measures to protect individual Indian trust data. Whether it is destruction of paper records,[18] electronic records,[19] or

[18] See, e.g., Corrected Report of the Special Master Regarding the Deletion of Individual Indian Trust Information by Former Assistant Secretary-Indian Affairs Neal McCaleb (Jan. 24, 2003);

penetration of computer networks,[20] it was the special master and his contractors' careful scrutiny that uncovered and led to the rectification of innumerable individual Indian trust data retention and preservation problems, not the self evaluative efforts of Interior or its bureaus.

It is unfortunate, therefore, that Interior proposes that "[e]ach bureau or office for which reconnection is intended will take steps to verify its representation that the IT system is secure from Internet access by unauthorized users." Interior Proposal at 7. In support, Interior plans to submit documentation to the Court that "will incorporate the data necessary to support a risk-based decision on Internet reconnection. The assessment may include, as appropriate: (1) network mapping and enumeration; (2) SANS/FBI Top 20 Vulnerability List Comparison; (3) vulnerability assessment; and (4) penetration testing." Id. at 7. Interior further offers that the above assessment will be performed by "Interior or its contractor." Id. at 7 n.9. "Interior's current contractor is Science Applications International Corporation ("SAIC")." Id. at 8 n.11. As this Court already noted: "SAIC is a contractor that is paid by the Interior Department" and as such "it cannot be considered to be a testing agency that operates independently of the Interior Department." 274 F.Supp.2d at 133. Furthermore, the Court observes that SAIC's long history as an Interior contractor in this area and the simple fact that Interior's IT security remains poor makes this Court reticent to rely on their judgment. Allowing Interior or SAIC to provide the verification of representations made by its bureaus on the adequacy of their IT security does not offer this Court any party without a conflict of interest or a track record of incompetency and is an insufficient method of verifying IT security. The Court's desire is simple and specific. The Court wants Interior to propose and the Court to approve 1) an entity with no prior relationship to

---

Opinion of the Special Master (July 27, 2001).

[19] See, e.g., Site Visit Report of the Special Master To the Office of Appraisal Services in Gallup, New Mexico and the Bureau of Indian Affairs Navajo Realty Office in Window Rock, Arizona (Aug. 20, 2003) (detailing Chief Appraiser Anson Baker's admission that he erased individual Indian trust data in the form of appraisal records for rights of way);

[20] See section II, supra.

Interior, 2) that possesses the requisite expertise in IT security, 3) whose only work for Interior will be performing the tasks set forth for it in the preliminary injunction issued this date, and 4) who will report all its findings to the Court. The Court does not mandate that such an entity work for the Court, in fact they can be paid and supervised directly by Interior. In this regard the Court is now making and continues to make every effort to allow the department to manage its own affairs without Court intervention. But the Court must absolutely have an entity not tainted by the history of falsehoods and deceptions that has plagued this litigation, nor otherwise dependent upon Interior for its revenues and livelihood, to provide honest appraisals of the security of individual Indian trust data.

3. Continued Monitoring Must Be Done By An Independent Entity

"[T]he proposal must allow for the continued monitoring of systems that have been reconnected, in order to determine whether the systems continue to be secure from unauthorized Internet access." 274 F.Supp.2d at 134. As noted in section IV.A.2, supra, this Court expected Interior's proposal to include continued monitoring by an entity independent of the Department of Interior as described above. Instead, Interior's proposal for continued monitoring is as follows:

> bureaus with reconnected systems that house or access individual Indian trust data will file a status report with the Court on an annual basis . . . [and] will include the steps taken in the previous twelve-month period to monitor and improve the security of the IT system . . . Supplemental information from the Department may include a description of IT security oversight activities and any testing conducted by the Department on the bureau"

Interior Proposal at 9-10. Interior's concept of continued monitoring appears to be limited to more self-monitoring by the bureaus with limited potential oversight by the Department. These are, of course, the very same bureaus that have repeatedly considered themselves secure only to be penetrated by the Special Master's contractor. Neither this Court nor the hundreds of thousands of Indian allottees for whom these accounts represent a livelihood should have to rely

on such a shoddy track record.[21]

Almost as an afterthought, Interior included the following as the last sentence of their proposal: "The Inspector General has informed the Office of the Chief Information Officer that it intends to pursue independent testing or auditing of various IT systems, and of its willingness to make available the results of such testing to further inform the Court." Id. at 10. While this Court appreciates the Inspector General's willingness to participate in this process of securing individual Indian trust data in Interior's IT systems, if Interior was serious about such a role they would have submitted a far more detailed plan than this trifling. Any plan for continued monitoring would contain a budget of costs and resources required, an agenda listing tests and methodologies, a schedule of proposed site visits, etc., etc. Interior submitted none of this. The Court does observe that it would be open to having the proposed independent entity be supervised by and be paid through the Inspector General's office as an added degree of separation from the bureaus being examined.

B. Interior Is Incapable of Meeting the Obligations in Its' Proposal

In the prior subsections, the Court observed several problems with Interior's proposed plan. But even if the Court decided to accept Interior's proposal without modification or change of any kind, numerous other facts indicate Interior is not even capable of properly executing the plan it submitted.

1. The Department of the Interior Report to The Office of Management and Budget Shows the Department Suffers From Many Significant IT Security Problems

The Financial Management Status Report and Strategic Plan FY 2004—FY 2008 ("FMSRSP") depicts Interior as an agency striving to implement information technology security programs and equipment, not an agency fully secure from external threats as the certifications imply. The FMSRSP catalogs a myriad of issues affecting the security of Interior's information

[21] See section IV.B.2, infra, for the General Accounting Office's analysis of the bureaus' IT management and section IV.C, infra, for the Office of Inspector General's analysis.

technology, including individual Indian trust data. Apropos of the instant analysis, the FMSRSP calls into question Interior's ability to secure individual Indian trust data from unauthorized access and to monitor itself. According to the FMSRSP:

> As a result of the material weaknesses identified in security and other controls over information technology systems and resources during the FY 2001 financial statement audit, Interior concluded that its financial management systems did not substantially comply with the financial management systems requirements of the FFMIA [Federal Financial Management Improvement Act]. In addition, the results of the financial statement audit did not allow Interior to conclude that it was in substantial compliance with all applicable federal accounting standards. The Department in is the process of developing a remediation plan to correct the material weaknesses in security and other controls over information technology systems and resources as well as comply with all federal accounting standards. The corrective actions are targeted for completion by 2004.

FMSRSP at 30. Without more, this statement singularly contradicts Interior's assertions that individual Indian Trust data is currently secure and that Interior has no further need for external monitoring.

Interior's Proposal allocates significant responsibility at the Department level to verify the representations of the bureaus and to assist in the continued monitoring of the security of the bureaus' IT systems by submitting supplemental information. It is particularly concerning that the FMSRSP documents such significant technological and administrative problems with Interior's existing IT systems and systems management. For example:

> In some instances, the Department has not ensured proper segregation of duties for personnel working with information technology systems and applications through its policies, procedures, and organization structures. As a result, It is possible for a single individual to control key aspects of system-related information operations and thereby possibly conduct unauthorized actions or gain unauthorized access to assets or records without detection. The Department's IT Security Plan will require review and restructuring of employee roles and responsibilities to achieve a higher degree of segregation of duties in information technology system-related operations.

Id. at 30.

> In some instances, the Department has not established access controls that limit or detect inappropriate access to information technology systems and related resources, thereby increasing the risk of unauthorized modification , loss, or disclosure of sensitive or confidential data. The Department will take action to secure network vulnerabilities and improve access control deficiencies in each of

> the following areas: network configuration management; password management; monitoring of security violation logs; access to program and sensitive files that control computer hardware and sensitive applications; and, other physical security controls."

Id. at 31 (emphasis added.).

> The Department does not have adequate controls over applications software development and change controls for all of its information technology systems and applications. The Department's IT Security Plan will seek to ensure that appropriate policies, procedures and operational controls are developed and implemented to prevent unauthorized system, program or application modifications.

Id.

The National Business Center ("NBC") certification states that the NBC "identified six applications containing IITD," NBC Certification at 2 (Aug. 11, 2003). It is disturbing then that FMSRSP reports that:

> Material weaknesses and other control deficiencies recently identified could affect the NBC's ability to prevent and detect unauthorized access and changes to its financial information, and increase the need for costly and less efficient manual controls to monitor and reconcile financial information. Although the NBC has taken prompt action to improve security and controls for its information technology systems, the NBC will take steps to improve entity-wide security planning, system configuration and operating systems, system software controls, software development and change controls, and service continuity.

FMSRSP at 31.

Moreover, the FMSRSP report acknowledges reports generated by General Accounting Office, Interior's Office of Inspector General, and independent accounting firms identify "serious financial management problems in the management of Indian Trust Funds." Id. at 72. The FMSRSP continues: "Reports based on these reviews indicated, among other things, that trust fund data was unreliable, inaccurate, and inconsistent, and trust systems have been inadequate to comprehensively process trust data and support investment activities. Inadequate internal controls and lack of consistent written policies and procedures were also cited in the reports." Id. at 72. This Court cannot conceive of any means by which Interior could be allowed to monitor itself and be solely responsible, without external monitoring, for the security of individual Indian trust data.

2. The Report by the General Accounting Office on Interior's Information Technology Demonstrates the Bureaus' Incapability to Perform the Tasks Allotted Them in Interior's Proposal

The General Accounting Office submitted a report to the Subcommittee on Interior and Related Agencies, Committee on Appropriations, House of Representatives on September 12, 2003 titled "Information Technology: Departmental Leadership Crucial to Success of Investment Reforms at Interior," GAO-03-1028, ("GAO Report").[22] The GAO performed the study to evaluate "(1) departmental capabilities for managing the agency's information technology (IT) investments, including its ability to effectively oversee bureau processes, and (2) the department's actions and plans to improve these capabilities." GAO Report at 1. The GAO summarized its findings stating: "The Department of the Interior has limited capacity to effectively manage its planned and ongoing IT investments." Id. (emphasis added).

The GAO Report demonstrates that neither Interior nor the individual bureaus have control over their information technology programs and cannot undertake the responsibility for monitoring the security of individual Indian trust data within their systems without independent, external monitoring.

> In August 2002, Interior's OIG reported that the department did not have a process to ensure that IT capital investments or projects focused on departmental mission objectives or federal government goals and initiatives—principally because of its decentralized approach to IT investment management. The OIG further stated that only 20 investment projects—representing over 24 percent of the total—were subject to departmental review and approval in fiscal years 2002 and 2003 through submission of capital asset plans. Therefore, about $1 billion in Interior IT investment projects were not subject to department-level review and approval during those 2 years.

[22]This report is attached as an exhibit to Plaintiffs' Third Notice of Supplemental Authority In Support of Comments Filed By Plaintiffs On August 27, 2003 and September 10, 2003 Regarding This Court's Preliminary Injunction, (Dec. 1, 2003), available at http://www.gao.gov/new.items/d031028.pdf.

> Consistent with these reports, OMB reported in the President's fiscal year 2003 budget that Interior was putting large sums of public funds at high risk for failure and that it had not complied with applicable legislative requirements that were established in the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996. OMB also reported that the department had not been able to adequately identify major projects within its IT portfolio or to demonstrate through adequate business cases the need for all of the major projects that it did identify. In addition, out of the 23 federal agencies included in the fiscal year 2003 budget supplemental document entitled *Performance Information for Major IT Investments,* the Department of the Interior was one of only two agencies that were unable to provide the type of information on the actual performance of their IT investments.

GAO Report at 7-8 (internal citations omitted) (emphasis added).

> Until Interior successfully implements stable investment management practices throughout the department, it will lack essential management controls over its IT investments, and it will be unable to ensure that the mix of investments it is pursuing is the best to meet the department's strategic goals, objectives, and mission.

GAO Report at 12-13 (internal citations omitted).

Interior asserts that "the decision whether or not to connect an IT system to the Internet should be made by heads of agencies or businesses in the exercise of their sound discretion, after considering appropriate relevant factors." Decl. of James E. Cason at 6 (Aug. 11, 2003). Yet the GAO Report reflects profound problems with IT project implementation at the bureau level.

> In 2002, Interior contracted with Science Applications International Corporation (SAIC) to study the department and bureau CIO organizations and determine whether it was in compliance with the requirements of the Clinger-Cohen Act . . . According to SAIC, in most of the bureaus, the CIOs lacked the authority to effect change among their subordinate IT staff and decision areas because they cannot allocate or withdraw funds and do not control hiring, training, or performance appraisals . . . On the basis of the SAIC study, and because of its desire to comply with the Clinger-Cohen Act, Interior issued Secretarial Order 3244, which acknowledged that authority and control over management of IT resources had not been fully established or coordinated in the department, resulting in significant variability among bureaus and offices in implementing IT functions and setting funding priorities. To rectify this situation, the order provides broad authorities to all of Interior's CIOs. Among other things, the order requires all bureaus to standardize their IT functional areas to achieve continuity of responsibility and accountability throughout the department. Specifically, the order calls for establishing a function described as technology management, which encompasses IT investment management.
>
> Interior's CIO issued specific direction to the bureaus in November 2002 and in January 2003, indicating how to implement Secretarial Order 3244 and establishing a process for monthly status reporting, which was to begin on January 31, 2003. However, at the time of our review, only two bureaus had provided the

> required monthly status reports, and none of the bureaus had fully implemented the order. This lack of responsiveness is consistent with concerns described in the SAIC report that Interior's CIO currently lacks adequate support from bureau CIOs to ensure that departmental efforts at improving IT investment management will be effectively implemented.

GAO Report at 31-33 (internal citations omitted) (emphasis added).[23]

If the bureaus are unable to implement clear Secretarial Orders regarding information technology, even nine months after such orders are issued, this Court has no confidence that these same bureaus can make a determination as to whether a system containing individual Indian trust data should be reconnected to the Internet and then follow that up with annual status reports that purport to be the "continued monitoring" this Court ordered. But, as the certifications frequently observe, when the bureaus were confronted with the thorough and persistent efforts of the Special Master and his contractors, they made frequent improvements to their IT security.[24] The bureaus were responsive to external independent monitoring in ways the Department appears unable to achieve.

C. Interior Received Its Fourth Consecutive "F" Grade From Congress For Its IT Security

On December 9, 2003, the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, United States House of Representatives, released its "2003 Federal Computer Security Report Card" ("Report

---

[23] One further example of bureau apathy: "On January 15, 2003, the department CIO issued a memorandum that called for the bureaus to immediately begin implementing more formal IT processes, using the *CPIC Guide*. . . Despite this initial instruction on its expectations, the department has yet to fully implement a certification process through which it can hold bureaus accountable for their IT investment management processes." GAO Report at 33.

[24] See, e.g. Certification of Bureau of Land Management at 20 (Aug. 11, 2003) (describing that as a consequence of the Report and Recommendation of the Special Master Regarding the Security of Trust Data at the Department of the Interior, (Nov. 14, 2001), the Department "compiled these weaknesses and associated recommendations into a 'Findings and Recommendations' Database to streamline analysis, remediation, and closure of the identified weaknesses. By June 2002, a preliminary set of the findings was distributed to Bureau CIO's to confirm the 'open/closed' status of each finding.").

Card").[25] The 2003 grade for Interior is an "F" with an underlying numerical score of 43 out of 100. In the four year history of the Report Card Interior received a score of 17 in 2000, 48 in 2001, 37 in 2002 and 43 in 2003, all obviously "F" grades. This year, for the first time, scores were based on the Federal Information Security Management Act of 2002 ("FISMA"). Congress uses two reports to grade federal agencies.[26] One report is a self assessment created by each agency, in Interior's case by its Chief Information Officer. This report is titled Report on the Implementation of the Federal Information Security Management Act FY 2003 ("CIO Report"). The second is an evaluation of that report by the Office of Inspector General at that agency. This report is titled Annual Evaluation of the Information Security Program at the Department of the Interior ("OIG Report"). Predictably, the CIO Report paints a much rosier picture of IT Security at Interior. In fact, Interior's CIO was bold enough to give Interior an overall score of 69.7 on its internally generated scorecard. App. B to CIO Report. The OIG report is not so sanguine about the state of Interior's IT Security, calling it a "material weakness." OIG Report at 3. The list of problem areas is simply frightening and takes up eight pages in the OIG Report as compared to only two pages dedicated to listing accomplishments. Given the extensive citations to other reports used throughout this opinion, the Court will spare the reader from a recitation of the full panoply of problems found by the OIG and instead provide a few highlights.

> "Bureau and office senior-level management were not always held accountable for ensuring that federal and DOI policies, procedures, practices, and control techniques were implemented." Id. at 5.
>
> * * * * *
>
> . "DOI's inventory of systems did not contain all systems operated for or on behalf of DOI. . . . includ[ing] . . . outsourced Web sites

[25]See Ex. A, Notice of Filing of "Fourth Report Card on Computer Security at Federal Departments and Agencies" Dated Dec. 9, 2003, Published by Subcommittee on Technology, Information Policy, Intergovernmental Relations And The Census, United States House of Representatives, (Dec. 11, 2003), available at http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=652.

[26]In response to an order from this Court, Interior filed redacted versions of both of these reports in the public record of this case, as well as unredacted versions under seal.

or contractor operated and managed applications used to collect and process DOI information." Id. at 7.

* * * * *

"DOI's network perimeters were expanded without assurance that adequate controls were implemented." Id. at 8.

* * * * *

"Many of DOI's information systems, including major applications, have operated and continue to operate without certifications and accreditations. Thus, management is not assured that risks have been minimized to an acceptable level for systems under their control." Id. at 9.

* * * * *

"There is little assurance that the 83 completed system security plans provide controls needed to effectively safeguard information systems." Id. at 9 Note that only 83 of 166 systems even have plans at all. Id.

* * * * *

"There is little assurance that security plans were updated based on periodic reviews of security controls or practiced throughout the lifecycle of each system." Id. at 10.

* * * * *

"Plans of Actions and Milestones (POA&M) developed by bureaus and offices were not complete or used effectively. Specifically, the plans did not:

- Include all information systems owned and operated by DOI that had weaknesses.
- Include all weaknesses whether identified through the organizations's internal reviews or by organizations such as the Office of Inspector General." Id. at 11.

The purpose of these excerpts is to show, yet again, that individual Indian trust data remains in jeopardy and that this Court can not and will not accept as true Interior's statements to the contrary.

V. REQUIREMENTS FOR PRELIMINARY INJUNCTION

The opinion issued in support of the July 28, 2003 preliminary injunction set out the requirements for a preliminary injunction in great detail. See 274 F.Supp.2d 126-31. Little has

changed in the intervening months to alter that analysis, save that on September 25, 2003 this Court entered a permanent injunction. When considering a request for injunctive relief, a court must consider four factors: (1) whether the movant has demonstrated a substantial likelihood of success on the merits; (2) whether the movant would suffer irreparable injury if the requested relief is not granted; (3) whether the injury to the movant if the injunction is not granted outweighs the injury to other interested parties who will be affected by the injunction; and (4) whether the issuance of the preliminary injunction would further the public interest. See Al-Fayed v. CIA, 254 F.3d 300, 303 (D.C. Cir. 2001); George Washington Univ. v. District of Columbia, 148 F. Supp.2d 15, 17 (D.D.C. 2001).

Plaintiffs have demonstrated a substantial likelihood of prevailing on the merits. Plaintiffs have already prevailed on the merits in both the first phase and phase 1.5 of the litigation. Cobell v. Babbitt, 91 F.Supp.2d 1 (D.D.C. 1999), aff'd sub nom. Cobell v. Norton, 240 F.3d 1081 (D.C. Cir. 2001); Cobell v. Norton, 283 F.Supp.2d 66 (D.D.C. 2003). Therefore, in light of their previous successes on the merits, the Court finds that Plaintiffs have demonstrated a substantial likelihood that they will prevail on the merits.

Plaintiffs will suffer irreparable injury if the injunction does not issue. As discussed at length in the July 28, 2003 opinion and in previous sections of this opinion, Interior's track record on IT security is poor. The Special Master ceased his monitoring activities in July 2003 and this Court has no assurance that even those systems previously reconnected by the Special Master are secure. Furthermore, the Court finds that many of Interior's IT systems are connected to each other, and an Internet connection to an IT system that does not house individual Indian trust data itself but is operated by a bureau that has another IT system that does house or access individual Indian trust data might allow unauthorized access to the IT system housing individual Indian trust data through the connections between systems. The Court finds that the continued connection to the Internet of any IT system that houses or accesses individual Indian trust data constitutes further and continuing irreparable injury to Plaintiffs. Furthermore, the continued

connection to the Internet of any IT system that may not itself house individual Indian trust data but is operated by a bureau within Interior that has custody or control over another IT system that does house or access individual Indian trust data constitutes further and continuing irreparable injury to Plaintiffs. Their continued connection to the Internet provides an opportunity for undetectable, unauthorized persons to access, alter, or destroy individual Indian trust data via an Internet connection. The alteration or destruction of any of the trust data would further prevent the beneficiaries of the individual Indian money trust from receiving the payments to which they are entitled, in the correct amount. Further, if neither Interior nor the beneficiaries are aware that trust information has been altered or destroyed then money damages could not compensate for such loss.[27]

The balance of the hardships weighs in favor of the Plaintiffs. While Interior will no doubt continue to suffer some hardship and inconvenience as a result of having systems disconnected from the Internet, such hardship is outweighed by the potential alteration or destruction of IIM trust data by unauthorized access through the Internet.

Finally, the Court finds that preliminary injunctive relief would advance the interests of the public. The interest of the three hundred thousand plus current beneficiaries of the individual Indian trust outweigh the potential inconvenience of those parties that would otherwise have access to Interior's Internet services. This conclusion is bolstered by the fact that those systems necessary to protect U.S. citizens against the threat of fire, or any other threat to life or property will remain connected to the Internet.

VI. CONCLUSION

There will no doubt be much hand-wringing by Interior over yet another preliminary

[27]Of course, the alteration or destruction of IIM trust information would necessarily render any accounting of the individual Indian trust inaccurate and imprecise. But the Court need not rely on Interior's obligation to provide an historical accounting in accordance with the structural injunction entered on September 25, 2003 as Interior's present obligation to administer the trust presents sufficient grounds for finding that Plaintiffs will be irreparably injured.

injunction issued by this Court disconnecting Interior's IT systems from the Internet. True to form, Interior will surely rail against this Court for taking over the executive and unconstitutionally usurping power, etc. etc. Such issues in the abstract are vitally important and even in this case a source of serious reflection and analysis for this Court. In fact, plaintiffs will likely describe this most recent injunction as a capitulation. But the ranting of plaintiffs and the feigned indignance of Interior aside, there is simply no other alternative. Interior brought this injunction upon themselves. In 2001, in response to overwhelming evidence the Court entered not plaintiffs' order but Interior's plan to rectify its IT security problems. The Court appointed a special master not on its own motion but on Interior's motion. And from December 2001 until July 2003 Interior and the Special Master worked together productively to reconnect many of Interior's IT systems. However Interior might try to characterize the Special Master now, the fact remains that the many systems he allowed reconnection bear witness to a productive working relationship. But now Interior has decided that it no longer requires the services of a Special Master. Instead they propose that the Court rely solely on them to self-monitor and self-report their progress at securing individual Indian trust data. To make matters worse, they put forth their proposal even as every other government agency to examine their IT security finds it to be woeful, a material weakness, an "F."

Of course, the Court expects to receive an immediate motion for stay and any such motion shall receive its due consideration. But in anticipation of the likely argument of Interior that its systems are now secure and thus it should not be forced to endure another disconnection or this Court's procedures for reconnection this question remains: how then does Interior explain the pervasive criticism of the other government entities who have evaluated Interior's IT security, whether it be the Office of Management and Budget, the General Accounting Office, the Inspector General at Interior, or even Congress? It is even more likely that Interior will wail that this Court is taking over the department and must be stopped in its unconstitutional quest for power. Such fear-mongering proved effective in the past. Yet even a cursory examination of the

history of this case and the preliminary injunction shows that the Court has extended and continues to extend Interior the utmost latitude in managing its own affairs. The Court is not telling Interior how to run its operations nor foisting management directives on the agency. It is Interior that is tasked with proposing a security standard, it is Interior that is tasked with proposing a plan for reconnection, and it is Interior that is tasked with proposing a new contractor to evaluate IT security. Furthermore, this proposed contractor need not work for the Court or a special master. Just as it did in its July 28, 2003 preliminary injunction the Court again gives Interior the opportunity to propose an alternative to the use of a Special Master. Unfortunately Interior's response to the July 28, 2003 preliminary injunction was not to propose an alternative but just to propose itself as judge and jury and given Interior's poor record for truthful disclosure in this case that was no alternative at all.

What then remains? The documents tendered by Interior under the guise of "certifications" are of no value as being unsworn in violation of federal statute and local rules. If a Chief Information Officer is unwilling to swear under penalty of perjury that the systems under his control are secure then the Court is unwilling to treat them as such. Beyond this, Interior's plan is facially inadequate as not providing for any independent third party to oversee its efforts and progress. The only assurance Interior offers this Court that a bureau housing or providing access to individual Indian Trust Data will not choose to reconnect such data to the Internet, or will not change or alter its existing security structure in a way that jeopardizes the present security of such data is an unsworn statement of that bureau or of Interior. Interior truly brought this on themselves.

Accordingly, the Office of Inspector General, the Minerals Management Service, the Bureau of Land Management, the Bureau of Reclamation, the Office of the Special Trustee, Fish and Wildlife, the Bureau of Indian Affairs, the Office of Surface Mining, and the National Business Center must disconnect all of their respective computer systems from the Internet. This includes every single IT system within that bureau whether or not that IT system houses or

provides access to individual Indian trust data. In contrast, the National Park Service, the Office of Policy Management and Budget, and the United States Geological Survey do not have to disconnect any currently connected system from the Internet. Lastly, no system essential for the protection against fires or other threats to life or property should be disconnected from the Internet. A separate preliminary injunction specifically setting forth these provisions and the provisions governing reconnection of the relevant IT systems shall issue this date..

Dated: March 15, 2004

/signed/

Royce C. Lamberth
United States District Judge