[SCHEDULED FOR ORAL ARGUMENT ON SEPTEMBER 14, 2004]

Nos. 03-5262, 04-5084

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ELOUISE PEPION COBELL, et al.,

Plaintiffs-Appellees,

v.

GALE A. NORTON, SECRETARY OF THE INTERIOR, et al.,

Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BRIEF FOR THE APPELLANTS

PETER D. KEISLER
Assistant Attorney General

ROSCOE C. HOWARD, JR.
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
CHARLES W. SCARBOROUGH
ALISA B. KLEIN
LEWIS S. YELIN
TARA L. GROVE
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room 9108
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530-0001

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), undersigned counsel certifies as follows:

A. Parties and Amici:

Defendants-Appellants are Gale A. Norton, as Secretary of the Interior; David W. Anderson, as Assistant Secretary of Interior- Indian Affairs; and John W. Snow, as Secretary of Treasury. The named plaintiffs-appellees in this class action are Elouise Pepion Cobell; Mildred Cleghorn; Thomas Maulson; and James Louis Larose. Earl Old Person remains a member of the class but is no longer a class representative. The class consists of present and former beneficiaries of Individual Indian Money accounts, excluding those who had filed their own actions prior to the filing of the complaint in this case.

B. Rulings Under Review:

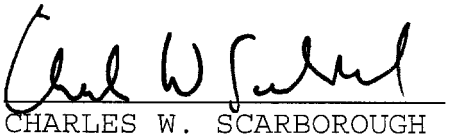
Appellants seek review of a preliminary injunction and memorandum opinion entered on July 28, 2003 by Judge Royce C. Lamberth, United States District Court for the District of Columbia, in Civ. No. 96-1285 (RCL), and published at 274 F. Supp. 2d 111. Appellants also seek review of a preliminary injunction and memorandum opinion entered on March 15, 2004 that "supersedes and replaces" the preliminary injunction entered by the court on July 28, 2003.

C. Related Cases:

This case has previously been before this Court in Cobell v. Norton, 334 F.3d 1128 (D.C. Cir. 2003), and Cobell v. Norton, 240 F.3d 1081 (D.C. Cir. 2001).

The government has filed an appeal in No. 03-5314 from a structural injunction entered by the district court on September 25, 2003 in the same underlying district court case. On the government's motion, the Court has placed that appeal on the same briefing schedule as the government's appeals in this case. The government's opening brief in each of those cases is due on April 6, 2004.

The government has also filed a petition for a writ of mandamus seeking the disqualification in this case of Special Master Alan Balaran, No. 03-5288, and the Court has set oral argument on that petition for April 8, 2004. Other mandamus petitions arising out of the same case have been filed by various parties in Nos. 03-5047, -48, -49, -50, & -57, and the Court heard oral argument on those petitions on March 15, 2004.



CHARLES W. SCARBOROUGH
Attorney for Appellants

GLOSSARY

APA	Administrative Procedure Act
BIA	Bureau of Indian Affairs
DOI	Department of the Interior
GAO	General Accounting Office
IITD	Individual Indian Trust Data
IT	Information Technology
OHA	Office of Hearings and Appeals
OMB	Office of Management and Budget
OPMB	Office of Policy Management and Budget
OST	Office of Special Trustee
MMS	Minerals Management Service
NBC	National Business Center
NPS	National Park Service
USGS	United States Geological Survey

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases: **Page**

---

* Authorities chiefly relied upon are marked with asterisks.

Statutes:

---

* Authorities chiefly relied upon are marked with asterisks.

Rules:

Legislative Materials:

* Authorities chiefly relied upon are marked with asterisks.

[SCHEDULED FOR ORAL ARGUMENT ON SEPTEMBER 14, 2004]

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Nos. 03-5262, 04-5084

ELOUISE PEPION COBELL, et al.,

Plaintiffs-Appellees,

v.

GALE A. NORTON, SECRETARY OF THE INTERIOR, et al.,

Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BRIEF FOR THE APPELLANTS

STATEMENT OF JURISDICTION

Plaintiffs invoked the district court's jurisdiction under 28 U.S.C. §§ 1331 and 1361, inter alia. On July 28, 2003, the district court issued a preliminary injunction. The government filed a timely notice of appeal from that injunction on September 25, 2003. On March 15, 2004, the district court issued a new preliminary injunction that "supersedes and replaces" the July 28, 2003 injunction. The government filed a timely notice of appeal from that injunction on March 22, 2004, and the two appeals were consolidated. This Court has jurisdiction over both appeals under 28 U.S.C. § 1292(a)(1).

STATEMENT OF THE ISSUES

1. Whether, in this suit under the APA to compel an accounting of Individual Indian Money (IIM) trust accounts, the district court had authority to assume control over the security of the Department of the Interior's computer systems.

2. Whether the district court erred in issuing preliminary injunctions requiring the Department of the Interior to disconnect its computer systems from the internet, notwithstanding the absence of any demonstrated danger to trust data and the significant impact the injunctions would have on the government and the public.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutory provisions are set forth in the addendum to this brief.

STATEMENT OF THE CASE

The American Indian Trust Fund Management Reform Act, enacted in 1994, requires the Department of the Interior to account for the daily and annual balance of funds held in trust for an individual Indian. In 1999, the district court held that Interior had unreasonably delayed in performing that accounting, and this Court largely affirmed. Cobell v. Norton, 240 F.3d 1081 (D.C. Cir. 2001). In approving the district court's exercise of continuing jurisdiction, however, the Court specifically admonished that the only legal breach at issue was the failure to

provide a timely accounting and that the court's jurisdiction on remand would be limited to determining whether steps taken in the preparation of that accounting might be "so defective" as to constitute unreasonable delay. Id. at 1106, 1110.

On remand, the district court asserted authority over a wide range of matters not directly related to an accounting. Based on reports from its Special Master, Alan Balaran, the court in 2001 entered a temporary restraining order requiring Interior to disconnect from the internet all information technology ("IT") systems housing Individual Indian Trust Data ("IITD"). Interior subsequently entered into a consent order establishing procedures by which it could reconnect computer systems housing or providing access to IITD to the internet subject to the Special Master's approval, and a number of systems were reconnected pursuant to those procedures. That process ultimately foundered, however, on a dispute over the Special Master's conduct of "penetration testing" of reconnected systems.

On July 28, 2003, without hearing any new evidence concerning the current security of Interior's computer systems, the district court issued a preliminary injunction requiring Interior to disconnect from the internet all systems that house or access IITD (including those previously reconnected by the Special Master), subject to certain exceptions allowing Interior to certify that those systems were either "essential for

protection against fires or other threats to life or property," did not house or access individual Indian trust data, or were secure from unauthorized internet access. See Cobell v. Norton, 274 F. Supp. 2d 111, 135-36 (D.D.C. 2003).

In August 2003, Interior provided voluminous certifications to the district court, as required under the terms of the injunction, and was thus able to avoid disconnecting any of its computer systems that had previously been reconnected to the internet. In light of the continuing threat of disconnection under the injunction, and because no evidence existed to suggest that individual Indian trust data was or had been in jeopardy, Interior appealed the July 28 injunction.

For over seven months, the district court took no action on Interior's certifications. On March 15, 2004, without providing notice or holding a hearing, the court issued a new preliminary injunction requiring Interior immediately to disconnect all of its IT systems from the internet, subject to certain limited exceptions. The court declared that it would not even consider the government's certifications, because they contained the following language: "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief." The court concluded that this language deviated from the requirements of 28 U.S.C. § 1746 and LCvR

5.1(h) because they included the words "to the best of my knowledge, information, and belief." 3/15/04 Op. 9-11.

The court's March 15 injunction provided no mechanism for Interior to certify that certain systems did not house or provide access to IITD, or were secure from unauthorized internet access, thereby enabling Interior to keep those systems connected to the internet. Although the injunction allowed computer systems "essential for the protection against fires or other threats to life or property" to remain connected to the internet, and allowed systems in three specified bureaus to remain connected, it compelled immediate disconnection of all other systems.

On March 24, 2004, this Court granted a temporary stay pending consideration of Interior's stay motion. On April 1, the Court consolidated the government's appeals from the July 28, 2003 and March 15, 2004 injunctions.

STATEMENT OF FACTS

I. The Underlying Litigation for an Accounting.

The 1994 Act provides that "[t]he Secretary shall account for the daily and annual balance of all funds held in trust by the United States for the benefit of an Indian tribe or an individual Indian which are deposited or invested pursuant to the Act of June 24, 1938 (25 U.S.C. 162a)." Pub. L. No. 103-412, § 102(a).

Plaintiffs filed this class action in 1996 to require Interior to take actions with respect to individual Indian money ("IIM") accounts. The district court dismissed plaintiffs' common law trust claims with prejudice, but allowed their suit to go forward because plaintiffs' "statutorily-based claims against the government can be brought under the APA." Cobell v. Babbitt, 91 F. Supp. 2d 1, 29 (D.D.C. 1999). This Court largely affirmed the declaratory judgment, concluding that agency action had been improperly delayed under APA standards. Cobell v. Norton, 240 F.3d 1081, 1108-09 (D.C. Cir. 2001). The Court explained, however, that the only actionable breach of duty was the failure to produce an accounting, and required the district court to amend its order to the extent that it purported to exercise jurisdiction over other related duties such as the management of computer systems. Id. at 1106. The Court stressed that the choice of how an accounting should be conducted was properly left to the agency, id. at 1104, and admonished the district court "to be mindful of the limits of its jurisdiction," id. at 1110, explaining that its jurisdiction was confined to determining whether future steps taken by Interior were so defective that they would "necessarily delay rather than accelerate the ultimate provision of an adequate accounting," ibid.

The district court did not amend its order as required by this Court. In September 2003, the district court issued a

"structural injunction" that purported to assert control over virtually all of Interior's accounting and trust operations, to be overseen by a monitor and agents with unlimited powers of access. Cobell v. Norton, 283 F. Supp. 2d 66 (D.D.C. 2003). Congress responded by enacting new legislation. The Conference Committee explained that the court-ordered accounting would cost between six and twelve billion dollars, H.R. Conf. Rep. 108-330, at 117 (2003), and "would not provide a single dollar to the plaintiffs." Ibid. The new statute, Pub. L. No. 108-108, provides that "[N]othing in the American Indian Trust Management Reform Act of 1994, Public Law 103-412, or in any other statute, and no principle of common law, shall be construed or applied to require the Department of the Interior to commence or continue historical accounting activities with respect to the Individual Indian Money Trust," absent new legislation or the lapse of Pub. L. No. 108-108 on December 31, 2004. 117 Stat. 1241, 1263.

On the government's motion, this Court stayed the structural injunction pending appeal. See No. 03-5314. It then set the present appeal and the appeal from the structural injunction on the same expedited briefing schedule.

II. Special Master Balaran and the District Court's Initial Computer Security Orders.

The present injunctions have their roots in a report issued by Special Master Alan Balaran in November 2001. The court had appointed Mr. Balaran as a Special Master on February 24, 1999,

and authorized him to review and assess defendants' compliance with particular document production orders and to "oversee the discovery process in this case." The court later expanded his jurisdiction to encompass certain aspects of records preservation. Dkt. 369, 370.[1]

On November 14, 2001, Mr. Balaran issued a lengthy report addressing Interior's computer security ("SM Report"). Most of Mr. Balaran's report consisted of a general discussion of a series of previous reports issued by other entities, such as the General Accounting Office (GAO). See SM Report at 17.

In a crucial section, however, Mr. Balaran detailed the results of his own activities. Mr. Balaran explained that he believed that informal comments by an Interior employee had not been fully accurate in their depiction of the current security of the agency's networks. SM Report at 137. Accordingly, in Mr. Balaran's words, he "commissioned" a computer contractor (Predictive Systems) to "penetrate" Interior's systems and "create a false account in his name." Ibid.

---

[1] In October 2003, the government filed a petition for a writ of mandamus seeking the disqualification of Mr. Balaran under 28 U.S.C. § 455. See No. 03-5288 (scheduled for oral argument on April 8, 2004). Several non-party individuals have also filed mandamus petitions seeking Mr. Balaran's recusal with respect to contempt proceedings concerning them. See No. 03-5047 and related cases (argued March 15, 2004). On March 15, 2004, this Court issued an order in the latter matter, staying the portion of the district court's September 17, 2002 order referring to Mr. Balaran various contempt matters regarding non-party individuals. See Order, No. 03-5047 (Mar. 15, 2004).

As Mr. Balaran described, the contractor was successful in its attempt to "hack" into an Interior system. Pursuant to Mr. Balaran's directions, the contractor "altered the name of an existing account belonging to a beneficiary * * * to that of Alan Balaran." SM Report at 138. Mr. Balaran cited no evidence that anyone else had ever "hacked" into any Interior computer system that housed or provided access to individual Indian trust data. Nevertheless, Mr. Balaran recommended to the district court "that the Court intervene and assume direct oversight of" Interior's computer systems, at least to the extent such systems contain Indian trust data. SM Report at 154.

The district court reacted promptly to the Special Master's recommendation. On December 5, 2001, the court issued a TRO cutting off Interior computer systems from the internet. The TRO ordered 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." 12/5/01 TRO at 2.

In the face of this ruling, Interior agreed to a Consent Order on December 17, 2001, in an effort to bring back on-line as many of its disconnected computer systems as rapidly as possible. The Consent Order established a process pursuant to which Interior's computer systems could be reconnected to the internet. Generally speaking, the Consent Order provided that a computer

system's internet connection could be restored upon agreement by the Special Master that the system was adequately secure, or that it neither housed nor accessed individual Indian trust data. See 12/17/01 Consent Order at 5-7.

Following entry of the Consent Order, Interior cooperated with the Special Master in an effort to reconnect its computer systems in a prompt and efficient manner. Over the course of 2002 and into 2003, many if not most of Interior's systems came back on line pursuant to the Consent Order's procedures, after the Special Master was persuaded by Interior's showings that particular systems either housed or accessed no individual Indian trust data, or were otherwise adequately secure from unauthorized access through the internet. Reconnected systems housing or accessing individual Indian trust data included the Minerals Management Service, the Inspector General, the Bureau of Land Management, and the National Business Center.

Other systems, however, including the Bureau of Indian Affairs, the Office of Special Trustee, the Office of Hearing and Appeals, and the Office of the Solicitor, remained offline and remain disconnected to this day.[2] Under the Consent Order's

---

[2] Because of the disconnection of the Solicitor's Office, Interior's attorneys, even in the context of dealing with this very litigation, are unable to engage in electronic communication (e-mail) with the Department of Justice, and cannot conduct on-line research. As noted below, the disconnection of other components including BIA also undermines Interior's ongoing ability to carry out basic operations and serve the public.

procedures, Mr. Balaran was not required to complete his review of an Interior reconnection proposal within any particular time frame. See 12/17/01 Consent Order at 7. Nor did the Consent Order specify the criteria governing Mr. Balaran's determination whether particular systems were secure enough from unauthorized internet access to warrant reconnection. See ibid. Thus, under the Consent Order, the Special Master could wait indefinitely before concluding an assessment of an Interior submission. And the Order placed no restraints on the Master's authority to reject Interior's documentation that various systems were secure. See ibid. Thus, for example, Interior sought but did not receive permission to reconnect the Office of Special Trustee and the Office of Hearings and Appeals. See Letter from John Warshawsky to Alan Balaran (June 10, 2002); Letter from Glenn Gillett to Alan Balaran (May 16, 2003) (detailing background and Special Master's failure to approve Interior reconnection plan).

Indeed, in the Special Master's view, the Consent Order did not merely confer upon him discretionary control over the reconnection of Interior's systems. Mr. Balaran also believed that he was authorized to continue further "penetration testing" of Interior's networks to detect potential vulnerabilities. Again, Interior for a time cooperated with Mr. Balaran while attempting to reach agreement on final "rules of engagement" under which Mr. Balaran would give advance notice of his

"hacking" attempts to a limited number of designated "trusted points of contact" within Interior and Justice. See Cobell v. Norton, 274 F. Supp. 2d 111, 114 (D.D.C. 2003).

Beginning in April 2003, however, this process broke down when Mr. Balaran's desire to "hack" into an Office of Surface Mining (OSM) server was temporarily thwarted because a cable to the server had become dislodged. Mr. Balaran wrote multiple letters to the Department of Justice suggesting that a named DOJ attorney had been untruthful in explaining the incident, demanding additional, detailed information, and insisting that the attorney in question provide a personal certification that prior representations were accurate. See id. at 114-19 (excerpting exchange of correspondence between Mr. Balaran and DOJ from April through June 2003).

By that point in this litigation, the court had already referred to Mr. Balaran - in connection with another of his roles as Special Master - numerous contempt matters involving more than three dozen current and former Interior and Justice Department employees. Cobell v. Norton, 226 F. Supp. 2d 1, 155 (D.D.C. 2002). Against that backdrop, the government made clear to Mr. Balaran, in letters dated June 19 and 20, 2003, that his unfounded accusation of misconduct against yet another employee was inappropriate and jeopardized any further cooperation regarding "penetration testing." See 274 F. Supp. 2d at 118-19.

As he had done in 2001, Mr. Balaran immediately brought his concerns to the court's attention, and the court again reacted swiftly. On June 27, 2003, the court for the second time issued a TRO severing Interior's internet connection. The court's order required continued disconnection of systems that were still off-line and, in addition, required disconnection of all systems housing or providing access to IITD, including those that had already been placed back on line because the Special Master had agreed they were secure. 6/27/03 TRO at 2. The TRO provided that "[a]ny system essential for protection against fires and other threats to life or property is exempted from this order." Ibid.

Like its December 2001 counterpart, the TRO was not premised on evidence that the integrity of Indian trust data had been compromised or was in any imminent danger of being compromised. The only basis for the TRO was the impasse created by Mr. Balaran's continued "penetration testing" and related demands.

III. The July 28, 2003 Injunction and Interior's Computer Security Submissions.

On July 28, 2003, the court converted the TRO into the preliminary injunction that is the subject of the appeal in No. 03-5262. See Cobell v. Norton, 274 F. Supp. 2d 111 (D.D.C. 2003). Based in part on the government's pending motion to disqualify the Special Master, the injunction terminated any further role for the Master in determining the extent to which

Interior may communicate electronically with the public. Under the terms of the July 28, 2003 injunction, the court assumed full authority over internet access.

In assuming control over Interior's computer systems, the court treated all Interior systems as presumptively subject to disconnection without regard to whether a particular system had already been reconnected because the Special Master had agreed that it was secure or did not house or access IITD. The court emphasized that "plaintiffs have not demonstrated to the satisfaction of the Court that the reconnected systems are not presently secure from unauthorized Internet access." Id. at 132. The court declared, however, that Interior had "failed to demonstrate to this Court that its reconnected systems are, in fact, secure from such unauthorized access." As a result, the court concluded that "it would be an act of folly for this Court simply to permit [Interior] to remain connected." Ibid.

The court performed a highly abbreviated analysis of the merits and the balance of harms. The court explained that, by virtue of its 1999 ruling, "plaintiffs have already prevailed on the merits of the first phase of this litigation," and that they had therefore demonstrated a likelihood of success on the merits. Id. at 126. And, the court found that, absent an affirmative showing that Interior's computer systems were secure, plaintiffs might suffer irreparable harm. Id. at 127-29.

Although the injunction purported to require immediate disconnection, it did not in fact do so. Instead, it included a procedure that delayed its full impact. Interior was allowed to submit certifications showing that the systems still connected to the internet were either "essential for protection against fires or other threats to life or property," or that these systems either did not house or access IITD or were secure from internet access by unauthorized users. Id. at 135-36. Additionally, Interior was required to file 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." Id. at 136.

On August 11, 2003, a variety of Interior officials provided detailed and comprehensive certifications, under penalty of perjury, that specific systems either were secure from internet access by unauthorized users or did not house or provide access to IITD. For example, an MMS official explained at length the security measures in place to prevent unauthorized access through the internet, including perimeter scans and multiple firewall and router protections. See Certification of Robert E. Brown, Acting Director, Minerals Management Service, at 28-46 (Aug. 11, 2003).

As required by the injunction, Interior also filed a proposal later in August setting forth a method of approving individual reconnections of disconnected Interior computer

systems, and of determining whether reconnected systems should stay reconnected. Plaintiffs filed responses to Interior's submissions within the time frames set forth in the injunction.

The court did not rule on Interior's certifications for seven months.

IV. The District Court's March 15, 2004 Shutdown Order.

On March 15, 2004, without holding any additional evidentiary hearings, the district court issued a preliminary injunction rejecting Interior's certifications and its proposal for approving reconnection of systems already off-line. The court declared that its March 15, 2004 injunction "supersedes and replaces" the July 2003 injunction that was already on appeal to this Court. 3/15/04 PI at 1.

Although Interior's certifications had been pending before the court since the previous August, the order required Interior immediately to disconnect all of its IT systems from the internet, whether or not they house or access IITD. The court allowed IT systems "essential for the protection against fires or other threats to life or property" to remain connected to the Internet, subject to the requirement that Interior provide sworn declarations within 5 days "specifically identifying any and every such Information Technology System 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." In addition, the court also allowed systems in the custody and control of the National Park Service, the Office of Policy Management and Budget, and the United States Geological Survey to remain connected because the court was satisfied that these bureaus do not house or access IITD.

The district court did not base its injunction on any new evidence that the security of IITD had been compromised or was in imminent jeopardy. Nor did the court purport to review on their merits the August certifications provided by Interior. Instead, the court declared that Interior's certifications submitted pursuant to the July injunction were procedurally inadequate. The court believed, in particular, that the certifications did not comply with 28 U.S.C. § 1746 and LCvR 5.1(h) because they stated that "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief." The court was of the view that the declarations were defective because they used the words "to the best of my knowledge, information, and belief." 3/15/04 Op. 9-11.

The court identified the harm justifying the disconnection of thousands of computers as follows: because the "Special Master ceased his monitoring activities in July 2003," the court had "no assurance that even those systems previously reconnected

by the Special Master are secure." Id. at 25. The court further observed 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.

Ibid. On this basis, the court concluded that "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." Id. at 25-26.

The court dismissed the impact of disconnections on the government and the public. The court stated that Interior would "no doubt continue to suffer some hardship and inconvenience as a result of having systems disconnected from the Internet," but concluded that "such hardship is outweighed by the potential alteration or destruction of IIM trust data by unauthorized access through the Internet." Id. at 26. And, because "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," the court concluded that 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." Ibid.

SUMMARY OF ARGUMENT

In an age in which internet communication has become as integral as the telephone, the district court has required a cabinet agency to eliminate its electronic connections to the world. No provision of law vests the district court with that authority, and no factual predicate exists for the extraordinary relief ordered by the court.

I. This is an action under the APA to compel the provision of an accounting under the 1994 Act, and, as this Court emphasized in its 2001 decision, the duty to account is the only actionable duty at issue. Cobell v. Norton, 240 F.3d 1081, 1106 (D.C. Cir. 2001). In that decision, this Court approved limited continuing jurisdiction, but made clear that this jurisdiction was confined to considering whether steps taken in preparation of an accounting were so defective as to constitute further unreasonable delay. Nothing in the Court's ruling authorized the district court to hack into computer systems or to issue injunctive orders to effectuate its conception of appropriate security.

The appropriate limitations on the district court's jurisdiction should have been clear even absent this Court's

admonitions. The only statute at issue in this suit is the 1994 Act. That statute requires Interior to provide a daily and annual accounting for IIM accounts. It does not reference computer security and provides no measure for determining what level of security might be adequate.

The passage of Pub. L. No. 108-108 in November 2003 removed any arguable legal basis for the court's action. That statute responded to a "structural injunction" that broadly asserted control of the operations of government in the same way that the court has asserted control over computer security here. It provides that nothing in any law "shall be construed or applied to require the Department of the Interior to commence or continue historical accounting activities." 117 Stat. 1241, 1263 The only basis for the court's assertion of authority over Interior's computer operations is their purported relation to an accounting. Pub. L. No. 108-108 deprives the court of any basis for ordering accounting activities, or any relief claimed to be attendant on a duty to account.

Even assuming arguendo that the district court had authority to review issues of computer security, it would have no authority to destroy the communications links of a federal agency by cutting off its internet connection. The APA, and the separation of powers principles that it reflects, permit no such

intervention into the day-to-day operations of a coordinate branch of government.

II. The injunctions are thus without legal foundation. They are equally devoid of any factual predicate. The present injunctions trace their origin to the "hacking" undertaken by Special Master Balaran in 2001. Prompted by the Special Master's report, the court ordered an immediate systemwide severance of electronic communications. But no evidence indicated that system data had, in fact, been compromised by anyone other than the Special Master himself. And the court provided no plausible explanation for severing all of the agency's electronic links to deal with the potential problem the Master identified.

To avoid the consequences of agency-wide disconnection, the government agreed to a Consent Order by which certain systems were reconnected at an early point. However, the Consent Order mandated no fixed time constraints and specified no criteria for authorizing reconnection of particular systems shown to be secure from unauthorized internet access. Thus, components such as the Bureau of Indian Affairs have remained disconnected from the internet for years and have been hamstrung in their electronic communications with the public and in carrying out their missions. When the court again ordered a system-wide disconnection in 2003, it did so without considering the existing state of IT security and without any evidence that data integrity

would in any way be compromised without an injunction. The court's injunction responded, instead, to the government's refusal to agree to the full range of "penetration testing" demanded by the Special Master. In concluding the Special Master regime and issuing its preliminary injunction, the court thus acted without any showing that an injunction was required.

The March 2004 injunction throws to the wind the criteria governing injunctive relief. In issuing its most recent injunction, the court failed even to conduct a hearing. It considered no evidence regarding the security status of Interior computer systems. Had it conducted a hearing on that question, it would have been required to confront the extraordinary investments made by the agency in the past three years. However, the court refused even to consider the detailed certifications submitted pursuant to its July 2003 order. Whatever the state of security may have been in 2001, the court had no basis for issuing a preliminary injunction in 2004 with respect to any Interior system.

No explanation exists for the court's willingness to sever agency communication links to deal with conjectural harm. The Department of the Interior is a massive organization that performs a vast array of critical functions on behalf of the American people. As Secretary Norton and others have made painstakingly clear in their declarations, the court's orders

would cripple Interior in its basic operations and in its ability to serve the nation.

In sum, the injunctions are without legal foundation, impose significant consequences on Interior and the public, and achieve nothing. The orders here, which are insupportable on their own terms, reflect the same mistaken understanding of the nature of this case and the limits of judicial intervention that characterize the structural injunction. In our appeal from the structural injunction, we urge that there is no longer any basis for the court's continuing jurisdiction and that the case should be remanded with instructions to dismiss. The court's assumption of control over the agency's electronic communications is symptomatic of the extent to which the case as a whole has lost its moorings.

STANDARD OF REVIEW

The court's legal rulings are subject to de novo review. Although the decision to enter an injunction is reviewed for abuse of discretion, a court necessarily abuses its discretion when it fails to apply proper legal standards. Koon v. United States, 518 U.S. 81, 100 (1996). Any pertinent factual findings would be reviewed for clear error.

ARGUMENT

I. THE DISTRICT COURT HAS NO AUTHORITY IN THIS CASE TO ASSUME CONTROL OVER THE SECURITY OF THE DEPARTMENT OF THE INTERIOR'S COMPUTER SYSTEMS.

A. The Court's IT Security Orders Have No Basis In The 1994 Act, Violate Settled Limits On Judicial Review, And Depart From This Court's 2001 Decision.

1. As this Court emphasized in its first decision in this case, a court cannot, consistent with the separation of powers, order "wholesale improvement of [a] program by court decree, rather than in the offices of the Department [of the Interior] or the halls of Congress, where programmatic improvements are normally made." Cobell v. Norton, 240 F.3d 1081, 1095 (D.C. Cir. 2001) (quoting Lujan v. National Wildlife Fed'n, 497 U.S. 871, 891 (1990)). Thus, the Court required the district court to amend its ruling to reflect the fact that the "actual legal breach" at issue "is the failure to provide an accounting, not [the] failure to take the discrete individual steps that would facilitate an accounting." Id. at 1106.

Among other things, this Court specifically emphasized that "[t]he failure to implement a computer system is not itself the breach." Id. at 1105. And the Court admonished the district court "to be mindful of the limits of its jurisdiction," id. at 1110, noting that the only basis for retaining jurisdiction over this case was to determine whether future actions taken by Interior were "so defective that they would necessarily delay

rather than accelerate the ultimate provision of an adequate accounting," ibid.

These admonitions reflect settled law. The courts have power to review agency action (or inaction) and to declare it unlawful or inadequate pursuant to the standards articulated in the APA. But "that authority is not power to exercise an essentially administrative function." Federal Power Comm'n v. Idaho Power Co., 344 U.S. 17, 21 (1952). The "guiding principle * * * is that the function of a reviewing court ends when an error of law is laid bare." Id. at 20. Thus, after declaring agency action unlawfully withheld (or unreasonably delayed), courts may not seek to control the processes by which an agency fulfills its congressionally-mandated functions on remand. See United States v. Saskatchewan Minerals, 385 U.S. 94, 95 (1966) (vacating order that precluded ICC from receiving evidence on remand). These limitations reflect the respective allocation of powers to the executive and judicial branches.

Nor may a court insert itself into an agency's internal operations by imposing additional requirements beyond those mandated by statute. As the Supreme Court stressed in Vermont Yankee Nuclear Power Corp. v. NRDC, Inc., 435 U.S. 519 (1978), the judiciary may not dictate to agencies the methods and procedures of needed inquiries on remand because "[s]uch a procedure clearly runs the risk of 'propel[ling] the court into

the domain which Congress has set aside exclusively for the administrative agency.'" Id. at 545 (quoting SEC v. Chenery Corp., 332 U.S. 194, 196 (1947)). See also Natural Resources Defense Council v. Nuclear Regulatory Comm'n, 216 F.3d 1180, 1189-90 (D.C. Cir. 2000) (refusing to impose procedures on agency that are not required by statute).

These principles apply regardless of whether an agency has delayed in taking action in some respect. See The Mashpee Wampanoag Tribal Council v. Norton, 336 F.3d 1094, 1100-01 (D.C. Cir. 2003); In re Barr Labs., Inc., 930 F.2d 72, 74 (D.C. Cir. 1991). Indeed, even in exceptional cases in which an agency has flagrantly disregarded a congressionally-mandated deadline for rulemaking, the appropriate judicial role is to retain jurisdiction over a case and require periodic progress reports until the agency has completed the required action. See In re United Mine Workers of Am. Int'l Union, 190 F.3d 545, 556 (D.C. Cir. 1999) (retaining jurisdiction and requiring semi-annual progress reports from the Mine Safety and Health Administration until it issued final regulations); Global Van Lines, Inc. v. FCC, 804 F.2d 1293, 1305 n.95 (D.C. Cir. 1986) (recognizing agency "discretion to determine in the first instance" how to bring itself into compliance); Telecommunications Research & Action Ctr. v. FCC, 750 F.2d 70, 81 (D.C. Cir. 1984) (retaining jurisdiction pending FCC's resolution of underlying issues).

Perhaps most clearly of all, as this Court has previously stressed in this case, a court cannot in keeping with the judicial role direct "wholesale" programmatic reforms. 240 F.3d at 1108-09 (quoting Lujan, 497 U.S. at 891). As illustrated by the history of the district court's attempts to assert control over Interior's computer security, judicial takeovers of this kind necessarily trench on the authority of politically accountable executive officials to implement the law and to determine whether and to what extent particular activities or programs should be funded.

2. The district court never amended its order as required by this Court. 240 F.3d at 1106. In its December 2001 TRO, its June 28, 2003 preliminary injunction, and again in its March 15, 2004 injunction, the district court paid no heed to this Court's prior decision or the settled legal principles that it reflects. Instead, the district court aggressively expanded its portfolio on remand, asserting authority over Interior's computer security and other day-to-day agency operations based on a November 2001 report from Special Master Balaran.

As this Court recognized in its 2001 decision, the 1994 Act - the source of the only enforceable legal obligations at issue in this case - contains no reference to computer security. See 240 F.3d at 1105, 1106. It provides no measure for determining what level of security is adequate, and does not authorize a

court to respond to security problems by disconnecting communications networks. Nor was there a basis for concluding, even in 2001, that the Special Master's ability to "hack" into a computer system had any significant relation to the performance of an accounting. And under no circumstances could any aspect of the statute be construed to authorize injunctions that disconnect agency communications.

Indeed, the district court's analysis of plaintiffs' "probability of success" on the merits of their request for injunctive relief reflects the absence of any relation between the present injunctions and the subject matter of this litigation. The court's discussion of plaintiffs' likelihood of success simply noted that "plaintiffs have already prevailed in the merits in the first phase of the litigation," and concluded that their previous success supported a finding of likely success in this context. 274 F. Supp. 2d at 126.

Plaintiffs prevailed on what the district court itself had characterized as "statutorily-based claims against the government [that] can be brought under the APA." 91 F. Supp. 2d at 29. In prevailing on those claims, plaintiffs established that the government had unreasonably delayed in providing account statements as of 1999. Plaintiffs did not thereby demonstrate that they were likely to prevail on later actions taken by the

agency, much less actions related only tangentially, if at all, to the provision of an accounting.[3]

B. The 2003 Legislation Removes Any Possible Basis For The Court's Injunctions.

The passage of Pub. L. No. 108-108 in November 2003 has now removed any arguable legal basis for the court's injunctions. As noted, that statute provides that nothing in any law "shall be construed or applied to require the Department of the Interior to commence or continue historical accounting activities." 117 Stat. 1241, 1263.

Congress has undoubted authority to amend the substantive law that provides the basis for forward-looking relief. See, e.g., Miller v. French, 530 U.S. 327, 344 (2000); Plaut v. Spendthrift Farm, Inc., 514 U.S. 211, 232 (1995); Robertson v. Seattle Audubon Soc'y, 503 U.S. 429, 432-35, 441 (1992). It has done so here. The only asserted basis for the preliminary injunctions is their purported relation to an accounting. See 3/15/04 Op. 2 (the IT security issues addressed in the

---

[3] Even assuming arguendo that problems with the security of Interior's computer systems had formed part of the basis for the district court's 1999 ruling, this Court specifically instructed the district court to "amend its opinion on remand" to reflect the fact that the only actionable breach was the failure to provide an accounting. 240 F.3d at 1106. Moreover, absent new evidence, the court's 1999 ruling could not provide any justification for the issuance of an injunction, years later, in July 2003 or March 2004. See generally O'Shea v. Littleton, 414 U.S. 488 (1974) (explaining that injunctions may be issued only on the basis of imminent and ongoing threats).

preliminary injunction are "a corollary" to Interior's statutory responsibility under the 1994 Act to provide an accounting). Pub. L. No. 108-108 plainly deprives the court of any ground for ordering accounting activities, or any other relief claimed to be attendant on a duty to provide an accounting.

C. A Court Would In Any Event Have No Basis For Ordering A Federal Agency To Sever Its Connection To The Internet.

Because the district court has no authority to assume control over Interior's computer security, the injunctions must be vacated. But even assuming that such matters could be deemed to fall within the potential scope of this litigation, the court would have no authority to order the agency, in whole or in part, to cut itself off from the internet.

Even as to matters properly within their jurisdiction, federal courts may order, at most, circumscribed relief tailored to the problem at hand. If the court had properly found and identified a particular deficiency, the proper course, at most, would have been to order a specific remedy for that shortcoming. See Hills v. Gautreaux, 425 U.S. 284, 293-94 (1976); Gulf Oil Corp. v. Brock, 778 F.2d 834, 842 (D.C. Cir. 1985); see also In re United Mine Workers of Am., 190 F.3d at 556 (requiring progress reports until promulgation of regulation unreasonably delayed). A court could not respond to asserted security problems in an agency telephone system by disconnecting the

phones. Nor can it enforce its version of appropriate security by severing the agency's electronic communications links.

In short, the court's rulings severing the internet connection of an executive agency have no basis in the 1994 Act and defy every previously settled limitation on judicial review of executive branch action. The court's limited continuing jurisdiction did not extend to a review of computer security unconnected to any statutory provision or standard, much less did it leave room for sweeping internet disconnection orders. The injunctions must be vacated.

II. THE INJUNCTIONS ARE FATALLY FLAWED ON THEIR OWN TERMS BECAUSE THEY ARE IN NO RESPECT NECESSARY TO PROTECT DATA SECURITY AND THEY IMPOSE SEVERE AND WIDESPREAD INJURY ON THE GOVERNMENT AND THE PUBLIC.

The series of computer security orders at issue here reflects the fundamental errors that have characterized the conduct of this litigation following this Court's 2001 decision. First, the evidence of a security risk followed from a judicial officer's "hacking" into a government computer system, not from the customary presentation of evidence in the framework of the adversarial system. Second, the court's reaction to such "evidence" was to take action wildly in excess of its jurisdiction. Third, because the entire inquiry is divorced from any specific statutory command or judicially manageable standard, no meaningful metric exists to assess any security risks at issue

or the level of resources that should appropriately be devoted to the IT security issue.

A. The Court's Disconnection Orders Have Never Had Any Plausible Justification.

As outlined above, the court's initial shutdown order - the December 5, 2001 TRO - was prompted by Special Master Balaran's November 14, 2001 report. In that report, Special Master Balaran explained that he had "commissioned" a computer contractor to "penetrate" Interior's systems and "create a false account in his name." SM Report at 137. As Mr. Balaran described, the contractor was "successful" and "altered the name of an existing account belonging to a beneficiary * * * to that of Alan Balaran." SM Report at 138. Mr. Balaran concluded his report by urging the court to "intervene and assume direct oversight of" Interior's computer systems, at least to the extent that such systems contained Indian trust data. Id. at 154.

It is extraordinary that a federal judicial officer would direct a private consultant to "hack" into a government computer system. Seeking to obtain unauthorized access to government computer data poses grave risks and, indeed, may constitute a federal crime under 18 U.S.C. § 1030. We are aware of no authority under which Mr. Balaran could "commission" his hired experts to alter data and establish fictitious accounts in Interior's computer files.

It is even more extraordinary that the district court would react to the Special Master's activity by ordering a Cabinet agency to disconnect itself from the internet. There is no evidence in this case that anyone other than the Special Master has ever "hacked" into any Interior computer system housing or providing access to individual Indian trust data. Against this backdrop, no plausible basis existed for the court's December 5, 2001 TRO requiring an across-the-board internet disconnection for the Department of the Interior's computers.

In the face of the December 2001 TRO, Interior agreed to a regime of Mr. Balaran's oversight to allow reconnection as quickly as possible. But the Consent Order itself specified no standards, and set no firm timelines, pursuant to which the Special Master was required to complete his review of agency reconnection proposals urging that particular systems were secure from unauthorized access through the internet. See 12/17/01 Consent Order at 7. As noted, the Special Master approved the reconnection of some systems, but declined to reauthorize others.

When the court once more issued an injunction in July 2003, it was not based on evidence that any data had been compromised, or even on any evidence that Interior had failed to devote significant resources to dealing with security problems. 274 F. Supp. 2d at 132. Any such conclusion would have been without basis.

As Secretary Norton has emphasized, "Interior has invested substantial time, effort and funding in improving [its] information technology security." Declaration of Gale A. Norton, at 2 (March 22, 2004). Indeed, "Interior has fully certified and accredited 30 of its systems and issued interim approval to operate for 108 systems at an approximate cost of $13.2 million." Declaration of Chief Information Officer W. Hord Tipton, at 8 (March 22, 2004). As further detailed in Interior's most recent quarterly report:

> Interior has installed additional firewalls and intrusion detection systems, reconfigured systems, updated security patches, scanned networks for vulnerabilities, updated password procedures and provided computer security training in an effort to reduce further the potential risk to IITD associated with the potential threat of unauthorized access from the Internet.

Sixteenth Quarterly Report (Feb. 2, 2004), at 5.

Likewise, Associate Deputy Secretary James Cason testified at the Phase 1.5 trial that Interior has "started a process of scanning ourselves, doing perimeter scanning of our security." Phase 1.5 Trial Tr. (June 21, 2003, AM), at 37. Although such testing initially revealed some vulnerabilities, Mr. Cason emphasized that Interior has now "driven the vulnerabilities down close to zero for our perimeter security at the Department overall." Ibid. And, in response to concerns that vulnerabilities in one system could provide a portal for hacking into other systems, Mr. Cason added that the agency has "taken a

lot of measures to basically bulletproof the [network infrastructure] from providing any access to a hacker that might enter into an agency that doesn't have Indian information into a Department that may have." Id. at 38. Indeed, in light of Mr. Cason's testimony, the district court noted during the Phase 1.5 trial that the Special Master had sent him a number of reports by his experts on computer security, which "all indicate that everything is on track. Every time they make a recommendation, you all hop on it, and it really sounded like things are being done very constructively there." Id. at 39.

These substantial improvements to IT security have included both disconnected and reconnected systems. For example, twenty-eight of the still-disconnected systems in the Bureau of Indian Affairs "have undergone initial Certification and Accreditation (C&A) reviews and have received an Interim Approval to Operate," and numerous BIA employees have received computer security training. Sixteenth Quarterly Report, at 6. Likewise, computer systems in the Solicitor's Office recently "underwent a third-party security assessment consisting of penetration testing," and "[s]ecurity defenses successfully blocked all attempts to breach the perimeter security of the network." Id. at 7.

In addition, of course, the twelve voluminous certifications filed with the court pursuant to its July 2003 order also comprehensively described the full range of measures that had

been implemented with respect to Interior's computer security, including, among other things, perimeter scanning regimens, multiple internal and external firewalls, router protections, advanced "DMZ" technology, enhanced physical access controls, and stringent password protocols. See, e.g., Declaration of Associate Interior Deputy Secretary James (Aug. 11, 2003); MMS Certification (Aug. 11, 2003). In connection with these efforts, Interior has also contracted with independent IT security experts to help ensure optimal results. See, e.g., id. at 49-50.

Against this backdrop, the 2003 injunction was not and could not have been based on agency delay or evidence that any system, whether reconnected or off-line, posed any threat to the integrity of individual Indian trust data.

Instead, the injunction was the product of the Special Master's belief that his continued hacking exercises were being frustrated. In April 2003, a cable failure temporarily stymied Mr. Balaran's attempt to "penetrate" an Office of Surface Mining (OSM) server. In ensuing correspondence with the Department of Justice, Mr. Balaran implicitly accused a Justice Department attorney of misrepresenting the facts underlying the cable failure, and demanded that the attorney submit to him a "personal certification" regarding the matter. 274 F. Supp. 2d at 114-19. As the district court recounted, that incident led to a breakdown in cooperation between the Special Master and Interior, and

prompted the court to issue its July 28, 2003 injunction. Ibid. Thus, it was Special Master Balaran's continued insistence on pursuing "penetration testing" - rather than any demonstrable threat of harm - that led directly to the court's July 28, 2003 preliminary injunction. Indeed, as the court itself acknowledged in issuing the injunction, "plaintiffs have not demonstrated to the satisfaction of the Court that the reconnected systems are not presently secure from unauthorized Internet access." 274 F. Supp. 2d at 132.

B. The Court Refused To Acknowledge The Evidence Of Current Security Measures.

The March 15, 2004 injunction makes even more vivid the dangers inherent in allowing a court to assert unfettered control over the operations of an agency without reference to any congressional command or administrable standards. Subject to a limited exception for computers essential for protection against fires and other threats to life or property, the court's March 2004 injunction (promptly stayed by this Court) directs an immediate and across-the-board disconnection of Interior's computer systems, whether or not they house or provide access to individual Indian trust data.[4]

---

[4] Interior's information technology portfolio includes approximately 110,000 computers. Only about 6,600 of them - approximately six percent of the total - house or provide access to individual Indian trust data. Tipton Decl. at 1.

Like the July 2003 injunction, the March 2004 injunction is not based on evidence of any jeopardy to the integrity of trust data. The court's previous recognition that "plaintiffs have not demonstrated to the satisfaction of the Court that the reconnected systems are not presently secure from unauthorized Internet access," 274 F. Supp. 2d at 132, should alone have been sufficient to demonstrate that injunctive relief was unwarranted. To obtain a preliminary injunction, the moving party bears the burden of proving both a substantial likelihood of success on the merits and irreparable injury. See Serono Labs., Inc. v. Shalala, 158 F.3d 1313, 1317-18 (D.C. Cir. 1998). Plaintiffs' failure to demonstrate that Interior's systems are not presently secure from unauthorized internet access thus precluded the entry of any injunctive relief.

The court's apparent indifference to the justification for its injunction is underscored by its refusal even to consider the extensive evidence of computer security submitted by Interior. The district court devoted just one paragraph of its opinion to the substance of the 900 pages of materials submitted by the agency. In so doing, the court noted an inconsistency regarding the status of the Automated Fluid Minerals Support System (AFMSS). 3/15/04 Op. 11-12. The certification indicated that the AFMSS had been reconnected. However, a table attached to the applicable report indicated that the system was not connected.

The information in the table was, in that respect, outdated. To comply with the July 2003 injunction, the government was required to assemble its detailed certifications within two weeks. That a court would disconnect an agency's communications systems on the basis of a single item of outdated information is extraordinary. See ibid.

The court rested its March 15 ruling primarily on what it perceived to be "procedural[]" flaws in the government's submissions. 3/15/04 Op. 8; see id. at 9-11. Even if a procedural defect existed in Interior's filings, the court could not properly have chosen to dismiss them and to issue an injunction without regard to the evidence of the agency's current security status.

But the procedural defect itself is chimerical. Each of Interior's twelve certifications had stated that "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief." The court concluded that this language deviated from the requirements of 28 U.S.C. § 1746 and LCvR 5.1(h) because it included the words "to the best of my knowledge, information, and belief." 3/15/04 Op. 9-11.

By their terms, 28 U.S.C. § 1746 and LCvR 5.1(h) apply only where "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 . . . by the sworn declaration, verification, [or] certificate . . . of [a] person . . . ." No statute, rule, or order required the "certifications" here to be executed under oath, and the district court cited none. Moreover, both the statute and the local rule provide that a certification meets applicable requirements if it is "substantially" in the form of the language set forth in those provisions, i.e., "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct." A declaration or certification "to the best of" the declarant's knowledge, information, and belief is plainly sufficient under the statute and the rule, and also under the requirements of Fed. R. Civ. P. 56. See United States v. Roberts, 308 F.3d 1147, 1154-55 (11th Cir. 2002), cert. denied, 123 S. Ct. 2232 (2003) (false statement attested to as "correct and true to the best of my knowledge and belief" was substantially in the form provided by § 1746); Colon v. Coughlin, 58 F.3d 865, 872 (2d Cir. 1995) (reversing summary judgment against plaintiff because verified complaint "attesting under the penalty of perjury that the statements in the complaint were true to the best of his knowledge" was sufficient under Rule 56).

The court's ruling is additionally inexplicable because the July 2003 injunction required only that the certifications made to the court were to comply with Fed. R. Civ. P. 11. See 274 F.

Supp. 2d at 135-36. Rule 11 governs the signing of pleadings, not evidentiary submissions by witnesses, and nothing in the Rule would, in any event, support the imposition of the requirement now announced by the court. To the contrary, insofar as the Rule is relevant at all, it provides that "[e]xcept when otherwise specifically provided by rule or statute, pleadings need not be verified or accompanied by affidavit." Fed. R. Civ. P. 11(a). No rule or statute imposes a specific requirement of this kind with respect to the certifications submitted to the district court pursuant to the July 2003 order. And, in any event, Rule 11 explicitly contemplates a certification standard based on "knowledge, information, and belief." Fed. R. Civ. P. 11(b).

The district court also discussed, without directly relying upon, three recent government reports addressing broad questions of IT management and security. 3/15/04 Op. 17-24. The court's citation to these reports further highlights the extent to which its security evaluations are not tethered to any standard made enforceable by Congress.

For example, the court cited a report of a congressional subcommittee giving Interior a grade of "F" for its overall computer security. 3/15/04 Op. 22 (citing House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "2003 Federal Computer Security Report Card"). But computer security in

general includes a wide range of issues, including physical facilities security, personnel qualifications and training, and protections against data loss.[5] From this overall perspective, the report also issued grades of "F" for computer security to the Departments of Justice, State, Homeland Security, Health and Human Services, Agriculture, and Housing and Urban Development. Nothing in the subcommittee's scorecard even remotely addressed the particular question of the threat to the integrity of data posed by unauthorized internet access, much less whether any such threat might exist with respect to Individual Indian Trust Data.

The court also cited an Interior report to OMB entitled "Financial Management Status Report and Strategic Plan (FY2004-FY2008)," issued September 8, 2003. See 3/15/04 Op. 17. Again, no part of this report was focused on the particular question of unauthorized access to data via the internet, much less the question of such unauthorized access to IITD. Indeed, the court's brief discussion of the report dwells on issues pertaining to financial management and compliance with accounting standards. See id. at 18.

---

[5] The court misapprehended this basic point in criticizing Interior for failing to provide a "uniform" IT security metric. See 3/15/04 Op. 13-14. While there are various government standards dealing with aspects of computer security in general, there is, as Interior's certifications explained, no uniform method of measuring whether a system is fully "secure" from the particular threat of unauthorized access to data via the internet. See Cason Decl. at 5-6 (Aug. 11, 2003).

A September 12, 2003 GAO report entitled "Information Technology: Department Leadership Crucial to Success of Investment Reforms at Interior" likewise offers no evidence of a threat to IITD. The report deals with Interior's overall management of its IT investments. It lends no support to the proposition that unauthorized access through the internet presents any imminent danger to the integrity of individual Indian trust data. See 3/15/04 Op. 20-22.

C. The Court Utterly Disregarded The Consequences Of An Internet Shutdown Order.

While the court's injunctions address an injury that is speculative at best, they inflict significant, immediate, and wholly unjustifiable harm on the government and the public.

The Department of the Interior is a cabinet level agency with an annual budget of $11 billion and 70,000 employees. Tipton Decl. at 1. "It is responsible for managing one out of every five acres of land in the United States; provides the resources for nearly one-third of the nation's energy; provides water to 31 million people through 900 dams and reservoirs; receives over 450 million visits each year to the parks and public lands it manages; and implements hundreds of statutorily-mandated programs." Ibid. "In addition, the Department provides a variety of critical services on which other federal agencies rely." Ibid. To meet its responsibilities, the Department

manages an information technology portfolio that includes more than 100,000 computers. Ibid.

In purporting to address the balance of harms that would result from an internet shutdown, the court observed that Interior would "no doubt continue to suffer some hardship and inconvenience as a result of having systems disconnected from the Internet." 3/15/04 Op. 26. This laconic assessment is difficult to comprehend. No one would suggest that the Department could carry out its missions without access to the telephone. It is unclear why the district court believed that Department-wide disconnection from electronic communication would result in mere "inconvenience." Ibid. As Secretary Norton made clear in her declaration filed with the government's stay application, "[t]he Department is integrated into the web of electronic communications as fundamentally as the telephone system. Internet communication is not merely a useful tool - it is essential to much of what we do." Norton Decl. at 1.

That the operations of a federal cabinet agency and its ability to serve the public would be crippled by a court-ordered internet shutdown should border on the self-evident. In any event, the significant and immediate harm that would flow from the court's orders is outlined in detail in the declaration of Interior's Chief Information Officer, Mr. W. Hord Tipton. The declaration provides a far from exclusive list of the ways in

which an internet disconnection would undermine Interior's ability to carry out fundamental operations and to provide service to the public:

- Contracting and Procurement. Interior averages more than 50 procurement announcements per business day on requirements that exceed $4 billion per year. A government-wide regulation requires that all such procurement actions be electronically posted on a single point of entry through GSA (the General Services Administration). The court's injunctions would seriously hinder this process, undermining the Department's ability to post notices for millions of dollars in contracts involving critical and time-sensitive matters. At least one of Interior's acquisition programs provides acquisition services on behalf of other agencies, and involves contracts for goods and services not only within the United States but in other countries as well. Tipton Decl. at 3.

- Financial Management. Internet connectivity is critical to the systems used in performing Interior's financial accounting, funds control, management accounting, and financial reporting. Tipton Decl. at 4. Interior's financial management activities affect a host of other government agencies as well; an Interior accounting and reporting system is used by roughly a score of non-Interior entities. Ibid.

- Education Programs. Internet disconnection would disable many programs that directly benefit Indians. For example, Interior operates an extensive school system for the benefit of tens of thousands of Indian children, in hundreds of institutions, spread across more than twenty states. Many of the facilities involved are located in remote parts of the country, where their scholastic programs cannot operate without computer access and communications via the internet. Tipton Decl. at 6.

- Royalties Distribution. Each month the Minerals Management Service (MMS) receives, processes, and disburses over $500 million in mineral revenues derived from federal and Indian leased lands. Among the beneficiaries of these royalty payments are at least 41 Indian tribes. The processes for handling and distributing these monies are heavily reliant on

automated systems and access to the internet, and a shutdown order would make it difficult if not impossible for significant sums to be allotted and paid in a timely and accurate manner. Tipton Decl. at 7.

- IT Security. The court's injunctions impair IT security itself. Interior's IT security program depends on the internet to download anti-virus software and other critical "patches." Tipton Decl. at 8. The injunctions thus threaten to prevent Interior not only from making improvements but even from maintaining and preserving its existing IT security profile.

- Hiring and Recruitment. Under the court's orders, Interior's web-based personnel system for hiring and recruitment would grind to a halt. Tipton Decl. at 6-7.

- Public Data Bases. Every year, millions of people use the internet to learn about and plan visits to the nation's national wildlife refuges. Tipton Decl. at 6. Under the injunctions, this information would no longer be accessible. Other databases widely relied upon by the public would also be shut down. To note just one example, BLM maintains case status for all public domain lands, which consist of approximately 270 million acres and an additional 500 million acres of subsurface minerals.

- Regulatory Activities. Interior uses the internet in distributing information to government agencies and the public about environmental analyses, land use planning, and other regulatory matters. The court's orders would halt this flow of information. For example, the Office of Surface Mining administers the Technical Innovation and Professional Services (TIPS) database containing critical information pertaining to mines, including technical designs, permitting information, and subsidence data. State regulatory authorities access TIPS approximately 135 times each day. Id. at 5-6.

Finally, the consequences of the court's injunctions are even broader than those specifically directed, and would undermine intra-Department communications as well as communications between Interior and the public. To maintain an

internet connection for portions of systems necessary to protect against fires and other threats to life or property, Interior would be forced to reconfigure its IT systems in ways that would drastically affect the effectiveness of those systems. Tipton Decl. at 2. The computers used for these "essential" services are linked to the internet through a series of connections that are shared by computers devoted to services that are not "essential" in this sense. Ibid. To maintain the internet link for "essential" systems and also sever all internet links for "nonessential" systems, the Department would have to physically disconnect from all communications access thousands of laptops and personal computers not directly used for functions essential to protect against fires and other threats to life and property. As a result, the employees who use those computers would be unable to communicate electronically within the Department as well as outside the Department. Ibid. (Indeed, because of the loss of community networking, even the basic capacity to print out documents might be impaired.)

Nor is the harm inflicted by the court's injunctions limited to the effect of disconnection upon systems that had previously been reconnected. As discussed, a number of Interior's systems, including those of the Bureau of Indian Affairs, the Office of Special Trustee, the Office of Hearing and Appeals, and the Office of the Solicitor, were disconnected in 2001 and remain disconnected to this day. Interior and the public suffer ongoing

harm from those disconnections, including, for example, BIA's inability to access online genealogy records for family histories needed for probate and the bureau's inability to communicate between offices, which has significantly delayed the probate process for individual Indians and their heirs. See Fifteenth Quarterly Report at 37, 82; Sixteenth Quarterly Report at 71. Similarly, as noted above, even in the context of responding to this very litigation, Interior's lawyers in its Solicitor's Office are unable to communicate by e-mail with their Justice Department counterparts, and cannot avail themselves of on-line research tools.

In sum, just as the injunctions are without basis in law, they are also without basis in fact. They reflect no consideration of the current state of IT security, and no evidence exists that the court's orders are necessary to prevent harm of any kind. The court's cursory dismissal of the very real impact of its rulings on fundamental government operations and the public welfare constitutes an extraordinary abuse of its equitable authority. The court's orders should be reversed and the injunctions vacated.

CONCLUSION

For the foregoing reasons, the district court's July 28, 2003 and March 15, 2004 preliminary injunctions, which preclude reconnection of systems already disconnected and require further disconnections, should be reversed and vacated, allowing online connection of all of Interior's computer systems.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

ROSCOE C. HOWARD, JR.
United States Attorney

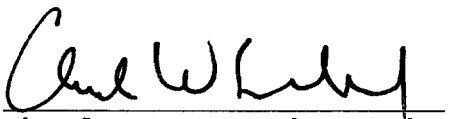
GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
CHARLES W. SCARBOROUGH
ALISA B. KLEIN
LEWIS S. YELIN
TARA L. GROVE
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room 9108
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530

APRIL 2004

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)(7)(c)
OF THE FEDERAL RULES OF APPELLATE PROCEDURE

I hereby certify pursuant to Fed. R. App. P. 32(a)(7)(C) that the foregoing brief contains 10,772 words, according to the count of Corel WordPerfect 9.



Charles W. Scarborough

CERTIFICATE OF SERVICE

I hereby certify that on this 6th day of April, 2004, I caused copies of the foregoing brief to be sent to the Court and to the following counsel by hand delivery:

The Honorable Royce C. Lamberth
United States District Court
United States Courthouse
Third and Constitution Ave., N.W.
Washington, D.C. 20001

Keith M. Harper
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
(202) 785-4166

G. William Austin
Kilpatrick Stockton
607 14th Street, N.W., Suite 900
Washington, D.C. 20005
(202) 508-5800

and to the following by federal express, overnight mail:

Elliott H. Levitas
Law Office of Elliott H. Levitas
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309-4530
(404) 815-6450

and to the following by regular, first class mail:

Dennis Marc Gingold
Law Office of Dennis Marc Gingold
607 14th Street, N.W., Box 6
Washington, D.C. 20005

Earl Old Person (pro se)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417

Charles W. Scarborough