[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

PETER D. KEISLER
Assistant Attorney General

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP

LEWIS S. YELIN
TARA L. GROVE
(202) 514-5089
Attorneys, Appellate Staff

* Authorities chiefly relied upon are marked with an asterisk.

Statutes

[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

REPLY BRIEF FOR THE APPELLANTS

INTRODUCTION AND SUMMARY

In this action to compel performance of the accounting required by the 1994 Act, the district court has asserted control over Interior's computer systems and has severed its electronic links to the public, government contractors, state governments and other federal agencies. Plaintiffs supply neither a legal foundation nor a factual predicate for these orders.

I. In 2001, this Court concluded that the government had unreasonably delayed in the performance of the accounting required by the 1994 Act and affirmed the district court's continuing jurisdiction for a five-year period. That jurisdiction, as this Court made clear, was limited to

determining whether the government was engaging in further unreasonable delay. Thus, IT security questions could fall within the district court's jurisdiction, if at all, only to the extent they bear upon unreasonable delay in the performance of the statutory accounting.

Plaintiffs are at pains to disclaim any connection between the present injunctions and the performance of an accounting, and they are surely correct: the district court had no authority to extend its jurisdiction to encompass IT security.

Even more clearly, the court cannot assert authority over issues of IT security when the basis for its limited continuing jurisdiction has ceased to exist. As we show in our briefs in the structural injunction appeal, No. 03-5314, since Secretary Norton assumed office in 2001, Interior has committed itself to meeting this Court's mandate. There can be no question of unreasonable delay in the period since this Court's initial decision, and the justification for the court's original retention of jurisdiction has disappeared. Contrary to the implicit premise of plaintiffs' argument, the district court has no independent jurisdiction to address all matters related to trust management.

Plaintiffs' insistence that the injunctions at issue bear no relation to the statutory accounting is, at least in part, a response to Pub. L. 108-108, which removes any legal basis for

connection between the injunctions and an accounting, Congress presumably was aware when it enacted the legislation that the Court had made clear that the only actionable duty at issue was the performance of an accounting. That some of the relief absence of any connection between the injunction and the accounting, the district court has itself taken a contrary injunction that requires an executive agency to sever its communications links. Under no circumstances could the court underlie the injunctions, reversal would be required because they are unsupported by <u>any</u> factual showing, much less the showing of executive department.

The district court conducted no meaningful evidentiary hearing on the issue of IT security. No evidence exists that any plaintiff has experienced harm as a result of alleged defects, and the only person known to have hacked into Interior's systems is the court's own Special Master.

In issuing its July 2003 injunction, the court specifically found that plaintiffs had not demonstrated a security threat from unauthorized internet access. Cobell v. Norton, 274 F. Supp. 2d 111, 132 (D.D.C. 2003). That finding alone should have been dispositive of plaintiffs' claims.

The court at no point considered the current state of IT security. Indeed, it dismissed the voluminous evidence submitted by Interior at the court's request on the ground that the agency's declarations were procedurally invalid. Plaintiffs offer no substantial defense of the court's ruling that Interior's declarations were improper, and they cite no evidence of present defects in IT security. Instead, they rely on outdated or inapposite reports, coupled with generalized and wholly unsupported allegations. And, plaintiffs completely ignore the enormous harm that the injunctions would inflict on Interior's operations and the public. For these reasons, the court's orders must be vacated and its oversight of IT security terminated.

Judicial Review And This Court's 2001 Decision.

1. The Injunctions Must Be Vacated

complete the Statutory Accounting.

The district court's 1999 declaratory judgment provided for

initial decision limited the district court's jurisdiction to detecting clear evidence of further unreasonable delay in the

security issues could be relevant, if at all, only to the extent they provided clear evidence of continued unreasonable delay in the performance of the accounting.

As discussed in our briefs in the structural injunction appeal, No. 03-5314, the record since this Court's initial decision and Secretary Norton's assumption of office in January 2001 makes clear that there has been no such unreasonable delay. As this Court held, it was evident even at the time of the contempt trial that Interior had made significant strides in completing an accounting. Cobell v. Norton, 334 F.3d 1128, 1148

(D.C. Cir. 2003). Subsequent progress has yielded tangible

judgments and per capita accounts, and production of a plan for completing land-based accounts that would accomplish the accounting described in this Court's initial decision in a time-

As we show in No. 03-5314, because there is no evidence to support a finding of unreasonable delay with respect to the performance of an accounting, and no basis to extend the

has no independent jurisdiction to direct a range of trust matters, including IT security, that operates without respect to the limited jurisdiction

IT Security.

Plaintiffs seek to sustain the injunctions on the theory

in doing so, it could declare and enforce trust obligations without regard to the provisions of any statute or the

that it reflects.

A court cannot properly arrogate to itself the power to oversee programmatic change and the day-to-day operations of executive agencies. These agencies are responsible, under the President's direction, for implementation of the laws, and are accountable to Congress for the expenditure of appropriated funds.

The limitations on judicial review established by the APA ensure that judicial and executive branch functions are not blurred. In appropriate circumstances, a court may compel an agency to take action that, once taken, would be final agency action. It cannot, however, control the processes by which the agency meets its obligation to complete that action. Further review must await final agency action. See 5 U.S.C. 704.

Thus, as this Court explained in 2001, whereas an agency's "single step or measure is reviewable, an on-going program or policy is not, in itself, a 'final agency action' under the APA." 240 F.3d at 1095. That is why, as this Court declared, a plaintiff cannot "'seek 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.'" Ibid. (quoting Lujan v. National Wildlife Fed'n, 497 U.S. 871, 891 (1990)).

Plaintiffs appear to recognize that these precepts would generally preclude the judicial role assumed in this case. They

assert, however, that these "run-of-the-mill principles of administrative law" are not applicable because "[t]his is a trust case, not a routine administrative law case," Pl.Br. 29, and that Lujan is "irrelevant." Pl.Br. 30. They can do so only by ignoring this Court's explicit pronouncement to the contrary.

Plaintiffs' argument reflects their inability to distinguish between the nature of the suit considered by this Court in 2001 and the very different action that it has now become. This Court was vigilant to examine the limits of its jurisdiction, but concluded that a suit to compel a particular agency action could proceed without enmeshing a court in a project of wholesale reform. The Court's rejection of the position now espoused by plaintiffs was unambiguous.

Indeed, the "wholesale reform" repudiated in Lujan is directly analogous to plaintiffs' present effort. In Lujan, Interior had implemented statutory directives pertaining to the withdrawal of federal lands from private use (such as mining). 497 U.S. at 875-79. Plaintiff purported to challenge the entirety of the "land withdrawal review program," that is, "the continuing (and thus constantly changing) operations of the [Bureau of Land Management] in reviewing withdrawal revocation applications and the classification of public lands and developing land use plans as required by [statute]." Id. at 890. The Court declared it "impossible" to bring such a challenge

under the APA. Ibid. As the Court explained, the "land withdrawal review program" was "no more an identifiable 'agency action' - much less a 'final agency action' - than a 'weapons procurement program' of the Department of Defense or a 'drug interdiction program' of the Drug Enforcement Administration." Ibid. To the contrary, the "program" that plaintiff ostensibly challenged extended to "at least[] 1250 or so individual classification terminations and withdrawal revocations." Ibid. (quotation marks and citation omitted). In the passage reiterated by this Court, the Supreme Court stressed that plaintiffs could not seek wholesale improvement even assuming that "violation of the law" was "rampant within this program." Id. at 891. To the contrary, "[u]nder the terms of the APA, [the plaintiff] must direct its attack against some particular 'agency action' that causes it harm." Ibid.

The attempt to exercise control over all aspects of the Indian trusts represents a particularly striking departure from settled law insofar as the court purported to identify and enforce obligations without connection to any statute. Apart from claims arising directly under the Constitution, it is for Congress to determine what actions may be brought against the federal government that will require payment from the fisc. Office of Personnel Mgmt. v. Richmond, 496 U.S. 414, 424 (1990) ("no money can be paid out of the Treasury unless it has been

appropriated by an act of Congress") (quotation marks and citation omitted). "The command of the [Appropriations] Clause is not limited to the relief available in a judicial proceeding seeking payment of public funds." Id. at 425.

Consistent with that bedrock principle, the Supreme Court has made clear that actions seeking enforcement of Indian trust obligations cannot be premised solely on the basis of a trust relationship. Congress acts against a background of trust principles which may inform the interpretation of a statute. But an actionable breach must be premised on a provision of substantive law. That is the teaching of United States v. Mitchell, 445 U.S. 535 (1980) (Mitchell I), and its progeny. The Court has stressed that to state a claim for breach of an Indian trust, a beneficiary must "identify a substantive source of law that establishes specific fiduciary or other duties[.]" United States v. Navajo Nation, 537 U.S. 488, 506 (2003). The General Allotment Act of 1887, the Court made clear, created no such enforceable trust management obligations. See id. at 503-04 (describing the holding of Mitchell I); see also United States v. White Mountain Apache Tribe, 537 U.S. 465, 473 (2003) (same).

Plaintiffs vigorously disclaim any connection between the injunctions they seek to defend and the 1994 Act, but cite no other statute as an alternative source of the duty at issue.

Even if the Supreme Court had not foreclosed plaintiffs' argument, their attempt to create enforceable trust obligations

trusts and the IIM trusts, and, in particular, the fact that the expenditures they seek to compel come entirely from appropriated

how common law principles could require a trustee to spend millions of dollars of its own money to improve its security

result of the asserted deficiencies.

Plaintiffs' attempted reliance on this Court's initial

litigation. Moreover, the Court confirmed that, under the APA, a plaintiff seeking to compel agency action unreasonably delayed

observed, when the agency is under such an unequivocal statutory

duty, "failure so to act constitutes, in effect, an affirmative act that triggers 'final agency action' review." Ibid.

Plaintiffs nevertheless urge that observations in the Court's 2001 opinion that the 1994 Act reflected preexisting trust duties (Pl.Br. 31-32) implicitly permit plaintiffs to press claims without any statutory anchor. This Court explained that interpretation of statutory terms is informed by common law trust principles. See 240 F.3d 1099. Thus, the Court looked to such principles in construing the requirement, set out in the 1994 Act, that the Secretary "account for" the balances in the IIM accounts. Likewise, the Court concluded that the reasonableness of the government's response in implementing that accounting requirement should take into consideration the government's preexisting trust responsibilities and should not be measured solely on the basis of a foreshortened time frame commencing in 1994. But the Court did not suggest that general fiduciary responsibilities could be enforced in the absence of any connection to a specific statutory command. Indeed, the Court distinguished between an action to compel a statutory accounting and attempts to assert control over subsidiary aspects of the agency's activity, noting that a "failure to implement a computer system" is not itself an actionable breach. Id. at 1105.

3. The Court Could Not, In Any Event, Require Interior To Disconnect Its Communications Links.

In the injunctions on review, the district court not only addressed matters outside the scope of its authority but compounded its intrusion into the affairs of a coordinate branch by ordering Interior to disconnect its communications links.

Plaintiffs offer no authority whatsoever for this unprecedented relief against an executive agency or, for that matter, against a private trustee. Under no circumstance could a court direct the agency to disable vital communications.

B. Pub. L. No. 108-108 Removes Any Possible Legal Basis For the Court's Injunctions.

As shown, the injunctions are without legal basis even apart from the enactment of Pub. L. 108-108, which provides that no provision of 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 expiration of the statute on December 31, 2004. 117 Stat. 1241, 1263.[1] The new statute removes any conceivable ground for ordering relief associated with the duty to provide an accounting.

---

[1] Plaintiffs colorfully refer to this enactment as the "Midnight Rider" because it was introduced by the Conference Committee. As noted in our brief in No. 03-5314, plaintiffs neglect to mention that the House and Senate submitted their versions of the Interior appropriations bill before the court issued its September 25, 2003 structural injunction.

1. Pub. L. No. 108-108 Applies To The Injunctions.

Plaintiffs urge that Pub. L. 108-108 is inapplicable to the IT security injunctions because the legislation was intended solely to remove the requirement to conduct "historical accounting activities," and thus does not affect "the portion of the case involving trust management and prospective institutional trust reform." Pl.Br. 33-34.

This characterization runs headlong into the district court's own view of the matter. In issuing the March 15, 2004 disconnection order, the court stated that "Interior's obligation to maintain and preserve individual trust data" - the sole basis for the court's oversight of IT security - is "a corollary" to Interior's duties to provide an accounting under the 1994 Act. JA 478. Although the court concluded that its injunction would in any event be an appropriate remedy for alleged breaches of "present trust obligations," JA 502 n.27, it did not abandon the view set out in the July 28, 2003 injunction that the alteration or destruction of trust data "would necessarily further render any accounting of the individual Indian trust inaccurate and imprecise, and therefore inadequate." 274 F. Supp. 2d at 129-30.

In any event, when Congress enacted Pub. L. 108-108, it was presumably aware that the district court, in issuing its 1999 declaratory judgment, had dismissed plaintiffs' common-law claims

"with prejudice," Cobell v. Babbitt, 91 F. Supp. 2d 1, 58 (D.D.C. 1999), and rejected plaintiffs' contention that they "may simply claim that they are the beneficiaries of a trust relationship with the United States and therefore invoke all of the rights that a common-law trust entails." Id. at 29. The court observed that "[w]hatever the scope of the government's legal duties under the IIM trust, the source is statutory law." Id. at 30. Congress was also presumably aware that this Court's 2001 opinion made clear that the only actionable breach at issue was the failure to provide an accounting, 240 F.3d at 1106, and that it had directed the court to amend its opinion to reflect that distinction, ibid. The new legislation applies to all relief issued in connection with the claim for the accounting, which is the sole claim remaining in this suit, and does not cease to have effect because the relief could not properly have been ordered in the first place.

To the extent plaintiffs argue that the injunctions on review cannot plausibly be regarded as an aspect of the duty to perform an accounting, the government is in full agreement. Nevertheless, their attempt to remove this aspect of the case from the scope of the legislation is unavailing.

The irony of plaintiffs' argument is evident. To avoid the impact of Pub. L. 108-108, plaintiffs are obliged to disown any connection between the statutory accounting and IT security. In

so doing, they only underscore the absence of any legal basis for inapplicable "because the IT injunctions do not require the expenditure of federal funds" to conduct an accounting. Pl.Br. the agency's communication links, and, indeed, Interior has spent enormous sums to do so. See, e.g., JA 1811-12 (Norton Decl.); JA [illegible] and continuing judicial monitoring of reconnected systems contemplated in the court's orders, JA 509-12, would undoubtedly

[illegible]

As in the appeal from the structural injunction, No. 03-5314, plaintiffs contend (Pl.Br. 35-43) that Pub. L. 108-108 is

[illegible]

[2] Plaintiffs also contend (Pl.Br. 35) that Pub. L. 108-108 "plays no role in this appeal," because the July 2003 injunction was in effect at the time the statute was passed, and that injunction was not mentioned by name in the statute's text or

[illegible] court was considering Interior's security certifications, and the court's more recent, across-the-board disconnection order was not issued until March 15, 2004, when it entered the second preliminary injunction with no prior notice to the parties

an unconstitutional "legislative stay" and an impermissible taking of property without due process of law. Both arguments are meritless.

In enacting Pub. L. 108-108, Congress amended the substantive law that provided the basis for this suit. See, e.g., First Gibraltar Bank, FSB v. Morales, 42 F.3d 895, 900 (5th Cir. 1995) ("numerous statutory schemes use the language 'shall be construed' to describe the limitations and boundaries of a congressional delegation of authority").

Plaintiffs concede, as they must, that Congress can amend substantive law prospectively, even in an appropriations measure of limited duration and even when the law applies to a specific case. Pl.Br. 41. As they acknowledge, the appropriations measure sustained in Robertson v. Seattle Audubon Soc'y, 503 U.S. 429 (1992), reflected both of these features. The Northwest Timber Compromise at issue in Robertson was an appropriations measure that expired by its terms at the end of the fiscal year, and that was enacted to resolve two pending lawsuits in which injunctions had already been entered. See id. at 432-33. The measure provided that Congress "determines and directs that" the actions already taken by the government constituted "adequate consideration for the purpose of meeting the statutory requirements that are the basis for the consolidated cases" cited in the legislation. Id. at 434-35.

The Supreme Court rejected the contention that the Northwest

Plaintiffs alternatively suggest that Pub. L. No. 108-108 deprives them "of their vested property interests," thus

which "may be altered according to subsequent changes in the law." Miller v. French, 530 U.S. 327, 347 (2000). The

be claimed here) does not vest until it has been reduced to an unreviewable final judgment. See, e.g., Lyon v. Agusta SPA, 252

removes any legal basis for the injunctions.

II. THE INJUNCTIONS ARE WITHOUT FACTUAL PREDICATE.

[illegible] unsupported by any factual showing.

A. The Only Relevant Fact-Findings Preclude

on "findings of fact," Pl.Br. 16, the district court conducted virtually no evidentiary proceedings on the issue of IT security.

It never found that a single class-member had suffered injury as a result of a security defect.[3]

In issuing its July 28, 2003 injunction, the court made no factual findings regarding alleged inadequacies in IT security. In a statement ignored by plaintiffs, the court expressly recognized 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. As discussed in our opening brief, that conclusion should have been dispositive of plaintiffs' claims. See Govt. Br. 37-38.

The March 15, 2004 injunction generally required internet disconnection with respect to all of Interior's computer systems, whether or not a particular system housed or provided access to individual Indian trust data. JA 507-12. No new evidence supported that action, and the court did not suggest that

only new evidence before it, the declarations provided by Interior. The court issued its injunction on the basis that the

[3] For the record, we note that plaintiffs represent that the class includes "all original allottees," Pl.Br. i n.1, but the class that was certified (over the government's objection) was defined solely in terms of IIM account holders. Dkt. 27, at 2-3.

"under penalty of perjury that the foregoing is true and correct

B. The Record Amply Demonstrates Interior's IT Security Achievements.

fact, secure." Pl.Br. 16. It is unclear whether plaintiffs have reviewed our opening brief. See Govt. Br. 31-37.

response to the court's July 28, 2003 order. At the same time, however, they make no serious attempt to refute the showing in

Pl.Br. 26-28.[4]

Plaintiffs gain no traction by suggesting that the court also found the government's showing to be "substantively" deficient. See Pl.Br. 26. As plaintiffs effectively concede, the district court undertook no real substantive assessment of the government's August 2003 showing. See ibid. [illegible]

public reports issued in late 2003. See JA 484, 493-500. However, as our opening brief demonstrated (at 41-43), and as detailed again below, the cited reports lend no support to the proposition that the integrity of IITD is at risk from unauthorized internet access.

In any event, plaintiffs do not dispute that Interior submitted 900 pages - consisting of twelve declarations by agency officials and signed under penalty of perjury - detailing the substantial steps taken to date with respect to computer security. See JA 924-1790 (8/11/03 Certifications).

The filing demonstrated that Interior has implemented, among other measures, perimeter scanning regimens, multiple internal and external firewalls, router protections, advanced "DMZ" technology, enhanced physical access controls, and stringent password protocols. See, e.g., JA 1486-1579 (MMS Certification). In connection with these efforts, Interior explained that it has expended millions of dollars on security improvements, and that it has also contracted with independent experts to help maximize results. See, e.g., JA 1536-37; see generally JA 924-1790 (8/11/03 Certifications).

Nor do plaintiffs acknowledge, much less seek to refute, our showing that Interior's current improvements with respect to IT

See Govt. Br. 34-36. As outlined in Interior's Sixteenth Quarterly Report, Interior has now "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." JA 622 (Sixteenth Quarterly Report at 5); see also JA 694-98 (Seventeenth Quarterly Report at 5-9). Significantly, the record shows that, against this backdrop, Interior has now "driven the vulnerabilities down close to zero for our perimeter security at the Department overall." JA 841 (Testimony of James A. Cason at Phase 1.5 Trial).[5]

C. The 2001 TRO And Consent Order Provide No Support For The Present Injunctions.

In the absence of record evidence, plaintiffs seek to justify the present injunctions by reference to the 2001 TRO and subsequent consent order. In particular, plaintiffs repeatedly quote the provision of the December 17, 2001 consent order stating that "Interior Defendants recognize significant deficiencies in the security of information technology systems protecting individual Indian trust data. Correcting these deficiencies merits Interior Defendants' immediate attention." JA 412. See, e.g., Pl.Br. 1.

Interior's 2001 declaration that it should devote immediate attention to improving security was not a statement that

---

[5] Plaintiffs' assertion that Interior's August 2003 showing was "unable to identify with any precision which systems or computers even housed or accessed the Trust Data," Pl.Br. 6, is difficult to comprehend. The declaration of Associate Deputy Secretary Cason and accompanying declarations of component officials expressly articulated which parts of the agency have IITD and which parts do not. See, e.g., JA 931 (Cason Decl.).

plaintiffs had suffered or would suffer imminent harm as a result

contrary, as Interior emphasized in opposing plaintiffs' preliminary injunction motion filed in December 2001.

> individual Indian trust data. The only evidence of actual intrusion and alteration of data is that performed by Predictive Systems under the direction of the Special Master

be no dispute that Interior has invested massive resources in IT

that much is evident from the court's recognition in 2003 that plaintiffs had not established an ongoing security threat.

the present injunctions. See, e.g., Pl.Br. 4-5, 8. Apart from the evidence of his unauthorized hacking, the report recounted

issues dating as far back as the 1980's and 1990's. See, e.g.,

JA 1877-83 (Special Master Report at 17-18) (discussing 1989 and

report are similarly flawed. See Pl.Br. 5, 16-17 n.37.

Plaintiffs refer to problems resulting from the absence of an

in the context of this litigation, as reflected in both the July

2003 and March 2004 injunctions. See 274 F. Supp. 2d at 135; JA

court's IT takeover is misguided as well. The government agreed

to the 2001 consent order at a time when an internet shutdown

[6] Plaintiffs inaccurately suggest that the Master "penetrated" Interior systems in a relevant way in February and March 2003. See Pl.Br. 20; see also JA 481. In the spring of 2003, the Master's contractor was able to penetrate four of BIA's

certification, Aug. 11, 2003).

[7] Plaintiffs also purport to take issue with Interior's assertion that only approximately 6,600 of its 110,000 computers house or provide access to IITD. See Pl.Br. 16-17 n.37

apples and oranges. A "computer system" may consist of one computer, or as many as several hundred or even thousands of computers. The 6,600 to 110,000 ratio noted in the declaration of Interior's Chief Information Officer presents no inconsistency. See JA 1813 (Minton Decl.).

of as many of its computer systems as possible, as speedily as possible. In signing the consent order, Interior never agreed that it was appropriate for the court to have ordered its systems disconnected in the first place.

More to the point, as plaintiffs do not dispute, the consent order regime has ceased to exist. Faced with the government's motion to end the Special Master's oversight, the court concluded that era and issued the first of the two preliminary injunctions now on review. The only issue at this point is whether the court's rulings have any basis in law or fact.[8]

D. The Reports On Which Plaintiffs Rely Provide No Support For The Injunctions.

Ultimately, plaintiffs seek to make their case by referring to reports discussing government computer security. See Pl.Br. 17-19. As our opening brief discussed (at 41-43), those reports do not supply the evidence that is wholly absent from the record.

Plaintiffs begin with a congressional subcommittee report giving Interior a grade of "F" for computer security. See Pl.Br. 17. As our opening brief noted, the subcommittee's scorecard was concerned with computer security in general, which includes such matters as environmental and physical facilities security,

---

[8] Whether or to what extent Interior "consented" to any of the Special Master's hacking activities is now likewise moot. See Pl.Br. 9. Plaintiffs do not contend, however, that Interior was aware of the Master's alteration of data and creation of a fictitious account when those activities took place in 2001.

personnel qualifications, and protections against data loss. Nothing in the scorecard 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. And, as our opening brief also explained (at 42), the subcommittee also gave a generic "F" grade to a number of other agencies, including the Departments of Justice, State, and Homeland Security. JA 2195.

The other reports cited are equally inapt. Plaintiffs quote a September 2003 GAO report to the effect that Interior "is carrying out few of the activities that support critical foundational processes," and that an internal Interior order intended to strengthen the agency's ability to manage its IT investments "has not been fully implemented." Pl.Br. 18 (quoting GAO Report). These statements have no evident connection to computer security, nor do they touch upon issues regarding IITD in particular. Indeed, as our opening brief explained (at 43), the cited GAO report is not devoted to security questions, but to an analysis of Interior's overall management of IT investments.

Plaintiffs' citation to a September 2003 Interior financial report to OMB is similarly unavailing. See Pl.Br. 18. That report concerned financial management, including financial reporting and the preparation of financial statements. The report noted that Interior "administers several financial

management systems for its bureaus and external agency customers," and that inadequate controls could affect its "ability to prevent and detect unauthorized access and changes to its financial information." JA 2101. It was in that context that the report stated, in the passage partially quoted by plaintiffs, Pl.Br. 18, that "[i]n 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 and confidential data." Ibid. The quoted language has nothing to do with the topic of Indian trust data; it concerns Interior's overall financial management and the exercise of appropriate controls over the agency's commercial and financial information. And even on this score, it speaks only to problems that exist "in some instances."[9]

Plaintiffs' attempted reliance on a September 2003 report by Interior's Inspector General fares no better. That report

---

[9] The same holds true with regard to the second passage that plaintiffs recite, which plaintiffs also quote selectively and without context. See Pl.Br. 18; see also id. at 2 n.2. The sentence in question states in full: "The increasing growth in electronic commerce and the growing vulnerabilities of information systems to unauthorized access have resulted in the need for a comprehensive improvement to IT security." JA 2103 (Financial Management Report). This statement contains no Interior "admission," Pl.Br. 18, much less one that would shed any light on the particular issue of access to IITD by unauthorized persons via the internet.

concluded that while "DOI continues to improve the security of

systems supporting DOI operations and assets are adequately protected." JA 2165. In the Inspector General's view, areas

information security as a performance-rating factor (JA 2168); ensuring that facilities housing information systems are properly

sign-in logs (JA 2169); ensuring that information system

behalf of DOI, including outsourced web sites (JA 2170); and ensuring that system security plans are of a sufficiently high

security policies and procedures" and "fully integrate corrective action plans," "DOI should continue to report to the Congress the

Plaintiffs quote this statement selectively and without context. See Pl.Br. 19. Contrary to plaintiffs' suggestion,

nothing in the cited passages even remotely indicates that any

trust data is at risk of improper access by unauthorized Internet users. Nor are plaintiffs correct in urging that Interior has no incident tracking system to monitor and report possible security

report upon which plaintiffs also seek to rely,

> In June 2003, a centralized computer security handling capability was implemented within the Department. Incidents are reported to the Homeland Security

coordination and reports.

JA 2136.

Plaintiffs place significant reliance on assertions devoid of citation of any kind. Plaintiffs' "Statement" asserts, for

plague Interior's systems and cause further irreparable injury to the Plaintiffs-Beneficiaries," Pl.Br. 1 (emphasis in original);

Trust Data continues to be at imminent risk of further loss, destruction, or corruption," id. at 5; and that "the protection

of Trust Data has become more problematic due to Trustee-

[illegible] electronic records of the agency," Ibid.

Plaintiffs' "Argument" asserts similarly that "Interior's IT systems are woefully insecure and continue to place the Trust

[illegible] there is conclusive evidence that the IT security has eroded and that Trust Data is in more jeopardy now than [in December 2011]," id. at 17, and that Interior has "failed to

Id. at 22.

These and other similar statements strewn throughout plaintiffs' brief show [illegible]

III. THE BALANCE OF HARMS AND THE PUBLIC INTEREST REQUIRE REVERSAL.

As shown, reversal is required because the injunctions are

integrated into the web of electronic communications as

thus, Internet communication is not merely a useful tool - it is essential to much of what we do." Ibid.

The record makes clear that cutting off Interior's computers

serve the nation. Basic functions such as contracting and procurement, financial management, and hiring and recruitment,

Similarly, key services upon which millions of citizens depend - including in particular the maintenance and provision of vital

Interior activities that would be disabled operate for the specific benefit of tribes and individual Indians, e.g., Indian

were required to undergo a Department-wide disconnection of its computer systems. And, of course, a number of systems were

Once more, plaintiffs' response to this showing is silence. Plaintiffs cannot avoid these and the other fundamental errors in the court's rulings by ignoring them.

CONCLUSION

For the foregoing reasons, and those set forth in our opening brief, the July 28, 2003 and March 15, 2004 preliminary injunctions should be reversed and vacated, and the district court's oversight of IT security should be terminated.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
Acting 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

JUNE 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 reply brief contains 6,884 words, according to the count of Corel WordPerfect 9.

Charles W. Scarborough

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of June, 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