

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

| | | |
|--------------------------------|---|--------------------------------|
| ELOUISE PEPION COBELL, et al., |) | |
| |) | |
| Plaintiffs, |) | Civil Action No. 96-1285 (RCL) |
| |) | |
| v. |) | |
| |) | |
| DIRK KEMPTHORNE, et al., |) | |
| |) | |
| Defendants. |) | |

**DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION
FOR ORDER TO SHOW CAUSE WHY INTERIOR SECRETARY
DIRK KEMPTHORNE AND ASSOCIATE DEPUTY SECRETARY
JAMES CASON SHOULD NOT BE HELD IN CONTEMPT
IN THEIR OFFICIAL CAPACITIES
UNDER THE COURT'S OCTOBER 20, 2005 PRELIMINARY INJUNCTION**

Plaintiffs contend that Interior Secretary Dirk Kempthorne and Associate Deputy Secretary James Cason¹ should be held in civil contempt, in their official capacities, for failing to comply with this Court's October 20, 2005 Preliminary Injunction (the "PI"), notwithstanding that the Court of Appeals has stayed the PI and has already heard argument on the Government's appeal to vacate the PI in its entirety. Plaintiffs mischaracterize both the stay and the scope of the Government's appeal as "narrow" (Plaintiffs' Motion at 3, 5 n.10, 6-7), and urge the Court to hold Defendants in contempt for failing to file declarations under two sections of the PI – Sections II.B and II.C. In fact, the Court of Appeals granted the Government's motion for a stay

¹ Plaintiffs characterize Mr. Cason as the Acting Assistant Secretary for Indian Affairs. While Mr. Cason has been delegated certain duties of the Assistant Secretary, he has not been appointed to that position. Mr. Cason is not a named defendant in this case, and Plaintiffs have not articulated an independent reason for naming him in their motion.

of the PI. That stay extends to Sections II.B and II.C. Further, these provisions are ancillary to the disconnection order set forth in Section II.A of the PI because they exist to provide procedures to determine if disconnections should be ordered in addition to those made under Section II.A. Even Plaintiffs concede that Section II.A has been stayed. The admitted stay of Section II.A plainly relieves Defendants of any obligations under Sections II.B and II.C. At a bare minimum, Defendants' belief that the stay applies to Sections II.B and II.C is reasonable. Further, Plaintiffs have not demonstrated how coercive relief would "restore" any claimed deprivation, given that disconnections under the PI have unequivocally been stayed, nor have they demonstrated any basis for compensatory relief. In sum, Plaintiffs have not made a *prima facie* showing of civil contempt, and the motion to show cause should be denied forthwith.

Background

A. Relevant Provisions of the Preliminary Injunction

After an extended hearing concerning the Department of the Interior's information technology ("IT") systems, the Court entered the PI on October 20, 2005. Sections II.A, II.B, and II.C directed Interior as follows:

- A. Subject to the exceptions outlined in Section II(C) and II(D), it is hereby ORDERED that Interior defendants forthwith shall disconnect all Information Technology Systems that House or provide Access to Individual Indian Trust Data:
 - 1. from the Internet;
 - 2. from all intranet connections, including but not limited to the VPX, ESN, or any other connection to any other Interior bureau or office;
 - 3. from all other Information Technology Systems; and
 - 4. from any contractors, Tribes, or other third parties.

- B. It is further ORDERED that within twenty (20) days of this date, Interior defendants must submit declarations to the Court, in compliance with 28 U.S.C. § 1746 and LCvR 5.1(h)(2), identifying any Information Technology Systems that do not House or provide Access to Individual Indian Trust Data and explaining

why such Information Technology Systems do not House or provide Access to Individual Indian Trust Data. The plaintiffs, in accordance with their discovery rights reaffirmed in Section II(F), may take discovery regarding the Interior defendants' declarations. The plaintiffs must file any response to Interior's submissions under this section within thirty (30) days of the completion of the plaintiffs' discovery. The Court will consider the parties' submissions, conduct any necessary evidentiary hearing, and order further relief as appropriate.

- C. To protect against fires or other such threats to life, property, or national security, it is further ORDERED that:
1. all Information Technology Systems necessary for protection against fires or other such threats to life, property, or national security may remain connected and are exempted from disconnection under Section II(A); and
 2. Interior defendants shall, within twenty (20) days of this date, provide declarations, in compliance with 28 U.S.C. § 1746 and LCvR 5.1(h)(2), specifically identifying each and every Information Technology System that remains connected to protect against fires or other such threats to life, property, or national security. The declarants shall attest to: (a) the specific reasons such Information Technology Systems are essential to protect against fires or other such threats to life, property, or national security; (b) the specific connections that are necessary to protect against fires or other such threats to life, property, or national security; and (c) the compensating security controls and measures that defendants have implemented, or plan to implement, to protect Individual Indian Trust Data from loss, destruction, or unauthorized manipulation as a consequence of remaining connected.
 3. The plaintiffs shall have twenty (20) days to file any response to Interior defendants' submission.
 4. This Court will review Interior defendants' submission and declarations, and the plaintiffs' response thereto, but absent any contrary order from the Court, such systems may remain connected.

PI at 3-5.

The PI defined "Individual Indian Trust Data" as

Information stored in, or transmitted by or through, any Information Technology System that evidences, embodies, refers to, or relates to – directly or indirectly and generally or specifically – a Federal Record that reflects the existence of Individual Indian Trust Assets, and that at any time either: (1) has been, or is now, used in the Management of Individual Indian Trust Assets; (2) is a title or ownership record; (3) reflects the collection, deposit, and/or disbursement or withdrawal of income or interest – imputed or actual – relating to Individual Indian Trust Assets whether or not such assets are held in a particular account or

are identifiable to any particular individual Indian trust beneficiary by name, number, or other specific identifier; (4) reflects a communication with, or on behalf of, an individual Indian trust beneficiary; or (5) has been, or is now: (a) created for, or by, Interior or any bureau, office, agency, agent, or contractor thereof, or for, or by a Tribe in connection with the Management of Individual Indian Trust Assets; (b) provided to, or received by, Interior or any such bureau, office, agency, agent, or contractor thereof, or any Tribe, for use in the Management of Individual Indian Trust Assets; (c) used or housed by Interior or any such bureau, office, agency, agent, or contractor thereof, or any Tribe, in connection with the government's Management of Individual Indian Trust Assets.

Id. at 2-3.

Additionally, the PI defined "Information Technology System" as:

Any computer, server, equipment, device, network, intranet, enclave, or application, or any subsystem thereof, that is used by Interior or any of its employees, agents, contractors, or other third parties in the electronic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or other information, including without limitation computers, wireless devices (e.g. Blackberrys) and networks, voice over the Internet protocol (VOIP), ancillary equipment, devices, or similar services or protocols, including support services, software, firmware, and related resources.

Id. at 1-2.

B. The Court of Appeals' Stay Orders and the Government's Appeal

The Government successfully sought an emergency stay and then a full stay pending its appeal of the PI. While Plaintiffs concede that the Court of Appeals' administrative stay, entered October 21, 2005, relieved Defendants of all their obligations under the PI, including under Sections II.B and II.C, they claim that the Court of Appeals' December 9, 2005 order granting the Government's motion for a stay pending appeal somehow narrowed the administrative stay. Plaintiffs' contention is meritless. The Government requested a stay to preserve the status quo – which would necessarily obviate the need to file declarations under Sections II.B and II.C.

Moreover, the issues before the Court of Appeals fundamentally affect whether and how Defendants would be obligated to meet the requirements of Sections II.B and II.C.

1. The Emergency Motion for Stay Pending Appeal

On October 21, 2005 – the day after the Court issued the PI – the Government filed its Emergency Motion for Temporary Stay Pending Appeal. Plts’ Ex. 2 (“Emergency Motion”). There, the Government sought relief from the PI on the grounds that it was “materially broader and more disruptive” than the previous shutdown order vacated by the Court of Appeals in December 2004, which the Court of Appeals had also stayed pending its resolution of the matter. *See Cobell v. Norton*, 391 F.3d 251 (D.C. Cir. 2004). Emergency Motion at 1. Among the issues raised by the Government in the Emergency Motion was the breadth of the Court’s definitions of “Individual Indian Trust Data” and “Information Technology System.” *Id.* at 6. Further, the Government observed that the PI lacked any specific standards for reconnection. *Id.* at 7.

The Court of Appeals granted the Government’s Emergency Motion on the same date. Plts. Ex. 3. The Court of Appeals ordered: “that the district court’s order filed October 20, 2005, granting appellees’ motion for a preliminary injunction, be stayed pending further order of the court. The purpose of this administrative stay is to give the court sufficient opportunity to consider the merits of appellants’ full motion for stay. . . .” *Ibid.*

2. The Full Motion for Stay

On October 27, 2005, the Government filed its Motion for Stay Pending Appeal and Expedited Briefing. Govt. Ex. 1 (“Full Stay Motion”). Among other things, the Government reiterated its concerns about the sweeping nature of the PI (Full Stay Motion at 1-2); emphasized the breadth of the Court’s definitions of “Individual Indian Trust Data” and “Information

Technology System” (*id.* at 7-8); and described the “devastating impact” that would ensue if the PI were not stayed (*id.* at 10-11).

The Government supported its motion with a declaration by Mr. Cason attesting to the harm that would be caused to Interior’s operations by the PI, noting, among other things, that “because of the extraordinary breadth of the various definitions contained in the injunction, it is possible that if and when the Interior Department were actually required to implement the order, serious issues would be raised as to whether the injunctive provisions must be construed even more broadly than contemplated herein.” Cason Dec. at 3.² Mr. Cason also noted that the exemption from disconnection set out in Section II.C of the PI “does not address the practical reality that underlying data networks are commonly shared by employees with a broad range of missions, some of which would be permitted and some of which are prohibited.” *Ibid.*

Significantly, the Full Stay Motion urged the Court of Appeals to grant a stay in order to preserve the status quo. Full Stay Motion at 9. Indeed, as the Government explained in its Reply brief in support of the Full Stay Motion, “Although our appeal will challenge the court’s order in its entirety, including its application to computers currently disconnected, our stay motion would only preserve the status quo as of the time of the October 20 injunction.” Reply to Opposition to Motion for Stay Pending Appeal, and Opposition to Motion to Vacate This Court’s Administrative Stay, No. 05-5388 (D.C. Cir.) (filed Nov. 21, 2005) at 2 n.2 (Govt. Ex. 2). Thus, the Government’s Full Stay Motion did not seek reconnection of systems that had been

²During oral argument on April 11, 2006, the Court of Appeals panel hearing this case felt obliged to admonish Plaintiffs for both the tone of their briefs and their unfounded attacks upon the Defendants. It is unfortunate that Plaintiffs have chosen to disregard this admonition, further imperiling their own credibility with their baseless invective against Mr. Cason and Government counsel. *See* Plaintiffs’ Motion at 8 n.15.

disconnected from the internet by the 2001 Consent Decree and not reconnected since then (*e.g.*, the Bureau of Indian Affairs).

On December 9, 2005, consistent with the Government's request to preserve the status quo, the Court of Appeals granted the Government's motion for a stay pending appeal and for expedition, and also denied as moot Plaintiffs' motion to vacate the administrative stay. In relevant part, the Court of Appeals stated:

ORDERED that the administrative stay issued October 21, 2005 be dissolved and that the motion for stay pending appeal be granted. The district court's order filed October 20, 2005 granting appellees' motion for a preliminary injunction shall be stayed insofar as it requires disconnection of computers and information technology systems connected as of the date of the order. Appellants have satisfied the stringent standards required for a stay pending appeal. See Washington Metropolitan Area Transit Commission v. Holiday Tours, Inc., 559 F.2d 841, 843 (D.C. Cir. 1977); D.C. Circuit Handbook of Practice and Internal Procedures 33 (2005).

Cobell v. Norton, Order, No. 05-5388 (D.C. Cir. Dec. 9, 2005) (Plts' Ex. 4).³

3. The Government's Appeal from the PI

On January, 11, 2006, the Government filed its opening merits brief in the appeal of the PI. The brief restated and amplified arguments made in the Emergency Motion and the Full Stay Motion regarding the broad sweep of the PI, particularly in light of the Court's definitions of "Individual Indian Trust Data" and "Information Technology System." *See* Brief for Appellants at 3-4, 17-18 (Govt. Ex. 3). The Government stated the issue on appeal as whether the Court of

³The standards set out in the *Holiday Tours* case are: "(1) Has the petitioner made a strong showing that it is likely to prevail on the merits of its appeal? Without such a substantial indication of probable success, there would be no justification for the court's intrusion into the ordinary processes of administration and judicial review. (2) Has the petitioner shown that without such relief, it will be irreparably injured? . . . (3) Would the issuance of a stay substantially harm other parties interested in the proceedings? . . . (4) Where lies the public interest? . . ." *Holiday Tours*, 559 F.2d at 843 (internal citation omitted).

Appeals “should vacate an injunction that requires components of the Department of the Interior to disconnect their computers from the internet and from internal computer networks, and that precludes some previously disconnected components from reestablishing internet access.” Brief for Appellants at 1. Thus, the Government’s brief sought vacatur of the PI in its entirety.

The Court of Appeals heard argument on the Government’s appeal on April 11, 2006, and the case is presently under advisement.

Applicable Legal Standard

Standards for civil contempt have been set forth in the contempt hearings in this case, *Cobell v. Babbitt*, 37 F. Supp. 2d 6 (D.D.C. 1999) (*Cobell II*), and *Cobell v. Norton*, 226 F. Supp. 2d 1 (D.D.C. 2002) (*Cobell VII*), *rev’d*, 334 F.3d 1128 (D.C. Cir. 2003) (*Cobell VIII*), and the elements have been described by controlling authority in other cases in this circuit. The Court of Appeals held in *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1289 (D.C. Cir. 1993):

“There can be no question that courts have inherent power to enforce compliance with their lawful orders through civil contempt.” *Shillitani v. United States*, 384 U.S. 364, 370 (1966). Nevertheless, “civil contempt will lie only if the putative contemnor has violated an order that is clear and unambiguous,” *Project B.A.S.I.C. v. Kemp*, 947 F.2d 11, 16 (1st Cir. 1991), and the violation must be proved by “clear and convincing” evidence. *Washington-Baltimore Newspaper Guild, Local 35, v. Washington Post Co.*, 626 F.2d 1029, 1031 (D.C. Cir. 1980).

Thus, a party seeking a finding of civil contempt must initially show, by clear and convincing evidence, that (1) a court order was in effect, (2) the order clearly and unambiguously required certain conduct by the respondent, and (3) the respondent failed to comply with the court's order. *SEC v. Bilzerian*, 112 F. Supp. 2d 12, 16 (D.D.C. 2000); *Petties v. District of Columbia*, 897 F. Supp. 626, 629 (D.D.C. 1995). As explained in *Project B.A.S.I.C.*:

A court order, then, must not only be specific about what is to be done or avoided, but can only compel action from those who have adequate notice that they are within the order's ambit. For a party to be held in contempt, it must have violated a clear and unambiguous order that left no reasonable doubt as to what behavior was expected and who was expected to behave in the indicated fashion. "In determining specificity, the party enjoined must be able to ascertain from the four corners of the order precisely what acts are forbidden."

947 F.2d at 17 (internal citation omitted).

Civil contempt sanctions are used either to obtain compliance with a court order or to compensate for damages sustained as a result of noncompliance. *Food Lion, Inc. v. United Food & Commercial Workers Int'l Union*, 103 F.3d 1007, 1016 (D.C. Cir. 1997). Coercive contempt sanctions are intended to force the offending party to comply with the court's order. *Coleman v. Espy*, 986 F.2d 1184, 1190 (8th Cir.), *cert. denied*, 510 U.S. 913 (1993).

As the D.C. Circuit recognized in *Cobell v. Norton*, 334 F.3d 1128, 1147 (D.C. Cir. 2003) (*Cobell VIII*), a fundamental concept of civil contempt is that the contemnor "carries the keys of his prison in his own pocket." *Gompers v. Bucks Stove & Range Co.*, 221 U.S. 418, 442 (1911), *cited in International Union, United Mine Workers of America v. Bagwell*, 512 U.S. 821, 828 (1994). Thus, the individual found in civil contempt must be afforded the opportunity to purge the contempt. *See Bagwell*, 512 U.S. 821, 829 (1994) ("Where a fine is not compensatory, it is civil only if the contemnor is afforded an opportunity to purge."). Purgation conditions are a necessary component of a civil contempt proceeding because civil contempt is "a remedial sanction used to obtain compliance with a court order or to compensate for damage sustained as a result of noncompliance." *Food Lion*, 103 F.3d at 1016, quoting *NLRB v. Blevins Popcorn Co.*, 659 F.2d 1173, 1184 (D.C. Cir. 1981). The goal of a civil contempt order is not to punish, but to exert only so much of the court's authority as is required to assure compliance. *Petties*,

897 F. Supp. at 629. “Civil contempt does not exist to punish the contemnor or to vindicate the Court’s integrity.” *Morgan v. Barry*, 596 F. Supp. 897, 899 (D.D.C. 1984), citing *Blevins Popcorn*.

In accordance with the Court of Appeals’ holding in *Blevins Popcorn*, a civil contempt order should be imposed, if at all, only at the conclusion of a three-stage proceeding involving “(1) issuance of an order; (2) following disobedience of that order, issuance of a conditional order finding the recalcitrant party in contempt and threatening to impose a specified penalty unless the recalcitrant party purges itself of contempt by complying with prescribed purgation conditions; and (3) exaction of the threatened penalty if the purgation conditions are not fulfilled.” *Blevins Popcorn*, 659 F.2d at 1184-85 (citing *Oil, Chem. & Atomic Workers Int’l Union v. NLRB*, 547 F.2d 575, 581 (D.C. Cir. 1977)); see also *Bilzerian*, 112 F. Supp. 2d at 16 (penalty should be imposed only after recalcitrant party has been given an opportunity to purge itself of contempt by complying with prescribed purgation conditions).

As this Court has noted, “the ‘extraordinary nature’ of the remedy of civil contempt leads courts to ‘impose it with caution.’” *SEC v. Life Partners, Inc.*, 912 F. Supp. 4, 11 (D.D.C. 1996) (quoting *Joshi v. Professional Health Services, Inc.*, 817 F.2d 877, 879 n.2 (D.C. Cir. 1987)). The party seeking a contempt finding bears the burden of establishing its claim by the heightened clear and convincing evidence standard. *Bilzerian*, 112 F. Supp. 2d at 16; *Petties*, 897 F. Supp. at 629. Further, in light of the severity of the contempt sanction, it should not be resorted to “if there are any grounds for doubt as to the wrongfulness of the defendants’ conduct.” *Life Partners*, 912 F. Supp. at 11 (citing *MAC Corp. v. Williams Patent Crusher & Pulverizer Co.*, 767 F.2d 882, 885 (Fed. Cir. 1985)).

Argument

Plaintiffs' assertion that Defendants' failure to file declarations under Sections II.B and II.C of the PI constitute civil contempt completely misunderstands the proceedings before the Court of Appeals. While this Court's directives when issued required Defendants to take specified actions, those directives were stayed by the Court of Appeals, and the premises underlying those directives are the subject of the Government's appeal. Civil contempt cannot lie for failure to adhere to an order that has been stayed. Indeed, Plaintiffs' motion raises obvious jurisdictional issues, given that the matter is plainly before the Court of Appeals, which has heard the case on an expedited basis.

I. PLAINTIFFS HAVE FAILED TO DEMONSTRATE DISOBEDIENCE OF A CLEAR AND UNAMBIGUOUS ORDER.

The Court of Appeals unquestionably stayed the PI pending its ruling on the Government's request that the PI be vacated in its entirety. Plaintiffs concede, as they must, that the Court of Appeals has stayed the PI's direction that Interior must disconnect any IT systems housing or providing access to Individual Indian Trust Data, as those terms are defined in the PI, that were connected as of the date the PI was entered. Despite the stay, Plaintiffs contend that Defendants should have filed declarations under Sections II.B and II.C of the PI, even though the sole purpose of those provisions was to provide information to the Court about whether additional Interior IT systems should or should not be disconnected. Since the Court of Appeals has made clear that no disconnection is required while it is considering the Government's appeal, there can be no serious assertion that Interior is nevertheless obligated to supply declarations that would have no purpose and the essential terms of which are presently before the Court of Appeals. Plaintiffs' failure to seek enforcement of Sections II.B and II.C for some six months

demonstrates that they too understood the Court of Appeals' stay to apply to Sections II.B and II.C.

A. The December 9, 2005 Stay Order Plainly Applies to Sections II.B and II.C.

Plaintiffs contend that, while the October 21, 2005 administrative stay applied to all the provisions of the PI, the December 9, 2005 stay was limited to Part II.A. This argument is manifestly incorrect. As with the administrative stay, the Court of Appeals **granted** the Government's motion for a stay pending appeal. Plaintiffs simply ignore the first sentence of the order. Instead, they seek to misconstrue the Court of Appeals' statement that "[t]he district court's order filed October 20, 2005 granting appellees' motion for a preliminary injunction shall be stayed insofar as it requires disconnection of computers and information technology systems connected as of the date of the order." This statement cannot be seen as "narrowing" the scope of the stay. As noted above, the Government expressly excluded from its stay motion any request for relief from the Court of Appeals to reconnect systems that had been disconnected under the 2001 Consent Decree. Thus, the Court of Appeals' order simply confirmed that the status quo would be preserved pending appeal, as specifically requested by the Government in its Full Stay Motion. Defendants' obligations under Sections II.B and II.C were, therefore, stayed along with their obligations under Section II.A, and hence no violation has occurred.

B. Sections II.B and II.C Are Ancillary to Section II.A.

In any event, sections II.B and II.C are entirely ancillary to Section II.A, which even Plaintiffs concede has been stayed. The Plaintiffs' insistence upon compliance with these provisions is thus nonsensical. At a minimum, the Court of Appeals' stay of Section II.A rendered Defendants' obligations under II.B and II.C unclear and ambiguous. Either way,

Plaintiffs cannot demonstrate disobedience of a clear and unambiguous court order by the requisite clear and convincing evidentiary standard.

Section II.A requires Interior to disconnect “all Information Technology Systems that House or provide Access to Individual Indian Trust Data.” Section II.B would require Interior to submit declarations identifying the systems that it had **not** disconnected pursuant to Section II.A. The stated purpose of requiring the Section II.B submissions is to permit Plaintiffs to challenge Interior’s determination as to which systems needed to be disconnected under Section II.A and which did not. Indeed, the PI provides that following such a challenge, “[t]he Court will consider the parties’ submissions, conduct any necessary evidentiary hearing, **and order further relief as appropriate.**” PI, Section II.B (emphasis added). Clearly, the “further relief” contemplated would be an order directing Interior to disconnect additional systems pursuant to Section II.A. However, the obligation to disconnect systems under II.A has been stayed. Accordingly no reason exists for Interior to engage in the exercise of filing declarations on systems that Interior might deem outside the reach of II.A when the Court is, in any event, prevented by the stay from ordering the disconnection of **any** Interior systems connected as of October 20, 2005.

Section II.A is expressly made “subject to the exceptions outlined” in Section II.C. While Section II.C permits systems needed “[t]o protect against fires or other such threats to life, property, or national security” to remain connected, like Section II.B, it requires Interior to identify these systems and file declarations explaining why the systems are necessary and what steps Interior has taken or will take to protect Individual Indian Trust Data while leaving the systems connected. Section II.C permits these systems to remain connected “absent any contrary order from the Court.” “[A]ny contrary order” would necessarily direct disconnection if the

Court were dissatisfied with Defendants' submissions. Further disconnection has been stayed. Here again, no purpose would be served by Interior identifying systems excepted from the requirements of Section II.A, when II.A has been entirely stayed.

Further, Defendants' obligations under the PI are intertwined with the Court's definitions of "Individual Indian Trust Data" and "Information Technology System." These definitions undergird Sections II.B and II.C as much as they do Section II.A, and these definitions are a part of the Government's stay motions and its appeal. The Government has repeatedly noted this Court's recognition that "Individual Indian Trust Data," as defined by this Court, "is suffused in varying forms and amounts throughout Interior's network environment. . . ." *Cobell v. Norton*, 394 F. Supp. 2d 164, 271 (D.D.C. 2005). The Court of Appeals has plainly given Defendants a respite from reporting on which of its "Information Technology Systems" house or provide access to "Individual Indian Trust Data" and which do not.

As explained in *Project B.A.S.I.C.*, civil contempt will lie only if the person against whom sanctions are sought "ha[s] adequate notice that they are within the order's ambit" and the order has "left no reasonable doubt as to what behavior was expected and who was expected to behave in the indicated fashion." *Project B.A.S.I.C.*, 947 F.2d at 17. Here, the Court of Appeals' stay order has fundamentally altered the behavior expected of Defendants. Indeed, the stay serves as notice that they need **not** behave in the manner set forth in the PI. Defendants can hardly be deemed in contempt for believing that their obligations to comply with the requirements of Sections II.B and II.C have been stayed, given (1) that the first sentence of the Court of Appeals December 9, 2005 order **granted** the motion for stay; (2) that Sections II.B and II.C are ancillary to the primary disconnection directive in Section II.A; and (3) that those sections are dependent upon the scope of the definitions of "Individual Indian Trust Data" and

“Information Technology System.” There is, at an absolute minimum, “reasonable doubt” that Defendants have any obligation to file declarations under Section II.B or II.C while the Court of Appeals’ stay remains in place.

Indeed, Plaintiffs aptly cite *United States v. Young*, 107 F.3d 903 (D.C. Cir. 1997). There, the Court of Appeals held that to determine whether an order is reasonably clear and specific for contempt purposes, courts apply “an objective standard that takes into account both the language of the order **and the objective circumstances surrounding the issuance of the order. . . .**” *Ibid.* at 907 (emphasis added). Here, the language of the PI and the circumstances of its issuance make clear that, if the Court had not required the disconnections set forth in Section II.A, it would not have included Sections II.B and II.C in the order because they would have served no purpose. Sections II.B and II.C plainly do not require the filing of declarations just for the sake of filing declarations, as Plaintiffs appear to believe; rather, they were placed in the PI to establish procedures that would allow the Court to determine whether other Interior systems should be disconnected, in addition to those disconnected pursuant to Section II.A.

Whether the Court’s directives under II.B and II.C were clear and unambiguous when issued is now beside the point. The Court of Appeals’ stay orders have altered the compliance landscape. At a minimum, it is plainly reasonable for Defendants to believe that they are no longer required to file declarations under those sections while the stay is in place. Accordingly, no basis for civil contempt exists.

II. PLAINTIFFS HAVE FAILED TO IDENTIFY APPROPRIATE RELIEF FOR THE ALLEGED VIOLATION OF THE PI.

Civil contempt is “a remedial sanction used to obtain compliance with a court order or to compensate for damage sustained as a result of noncompliance.” *Food Lion*, 103 F.3d at 1016.

Plaintiffs have alleged no compensatory damages resulting from the non-filing of declarations under Sections II.B and II.C, and there are none because the disconnections contemplated by the PI – including possible additional disconnections under II.B and/or II.C – have been stayed. Indeed, Plaintiffs’ claim of aggrievement is hardly credible when they allowed six months to pass before even mentioning what they now call a contempt of court.

Plaintiffs complain that Defendants are “concealing” information. Plaintiffs’ Motion at 10. But the risks they cite – the alleged compromise of electronic trust data and harm to beneficiaries (*ibid.*) – were cited by this Court’s opinion accompanying the PI, *see* 394 F. Supp. 2d at 273-75, and the Court of Appeals nevertheless stayed the PI. This is not the proper forum for Plaintiffs to reiterate arguments they have made to the Court of Appeals. Indeed, the Court of Appeals has necessarily concluded, by finding that the Government has met the standards required for a stay pending appeal, that the harm posed to Interior’s operations and, by extension, to the public by compliance with the PI are graver than the harm claimed by the Plaintiffs. In fact, Plaintiffs have suffered no harm at all from Defendants’ non-filing of declarations under Sections II.B and II.C because the only relief contemplated by those sections is the disconnection of additional Interior systems – and such disconnections have been stayed.

Assuming the Court found that Defendants had violated a clear and unambiguous order, notwithstanding the stay, the Court would have to give Defendants an opportunity to purge the contempt before imposing any sanctions. *Blevins Popcorn*, 659 F.2d at 1184-85. As shown above, Sections II.B and II.C rely upon definitions that are part of the Government’s challenge to the PI. Consequently, if this Court were to enter a show cause order and direct Defendants to purge by filing the declarations demanded by Plaintiffs, such an order would run afoul of the Court of Appeals stay order.

That there is no remedial relief the Court can award Plaintiffs only confirms that Defendants have properly relied upon the stay in not filing the declarations contemplated by Sections II.B and II.C of the PI.

Conclusion

There is no basis for a show cause order, and Plaintiffs' motion should be swiftly denied.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

STUART E. SCHIFFER
Deputy Assistant Attorney General

MICHAEL F. HERTZ
Director

/s/ Tracy L. Hilmer
Dodge Wells
Assistant Director
D.C. Bar No. 425194
Tracy L. Hilmer
D.C. Bar No. 421219
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 261
Ben Franklin Station
Washington, D.C. 20044
(202) 307-0474

DATED: June 23, 2006

CERTIFICATE OF SERVICE

I hereby certify that, on June 23, 2006 the foregoing *Defendants' Opposition to Plaintiffs' Motion for Order to Show Cause Why Interior Secretary Dirk Kempthorne and Associate Deputy Secretary James Cason Should Not Be Held in Contempt in Their Official Capacities Under the Court's October 20, 2005 Preliminary Injunction* was served by Electronic Case Filing, and on the following who is not registered for Electronic Case Filing, by facsimile:

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

/s/ Kevin P. Kingston
Kevin P. Kingston

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.

No. 05-5388

[Civil Action No. 96-1285 (D.D.C.)]

MOTION FOR STAY PENDING APPEAL AND EXPEDITED BRIEFING

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room, 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

EXHIBIT 1

Defendants' Opposition to Plaintiffs' Motion for Order to Show Cause Why
Interior Secretary Dirk Kempthorne and Associate Deputy Secretary
James Cason Should Not Be Held in Contempt in Their Official Capacities
under the Court's October 20, 2005 Preliminary Injunction

INTRODUCTION AND SUMMARY

On October 20, 2005, the district court issued a preliminary injunction that required disconnection of Department of Interior computers from the internet and also from intra-Departmental communications. On October 21, this Court granted an emergency administrative stay of the injunction. As contemplated by this Court's order, we now file our motion in support of a stay pending appeal, including the declaration of James E. Cason, Associate Deputy Secretary of the Interior. We also ask for expedited briefing to resolve the issues presented by the district court's order at the earliest possible time and to minimize any conceivable harm asserted to arise from the granting of a stay.

The injunction requires Interior to "disconnect all Information Technology Systems that House or provide Access to Individual Indian Trust Data" not merely from the internet, but also from Interior's internal "intranet" systems; from all other Department computers, networks, or electronic devices; and from any computers or computer networks operated by contractors, Indian Tribes, or other third parties. Injunction § II.A.

"Individual Indian Trust Data" ("IITD") is broadly defined to encompass all "[i]nformation * * * that evidences, embodies, refers to, or relates to — directly or indirectly and generally or specifically — a Federal Record that reflects the existence of Individual Indian Trust Assets." § I.E. As the district court understood, given the breadth of this definition, "IITD in one form or another permeates Interior's IT environment fairly completely." Op. 171.

The injunction thus compels Interior to embark immediately on a broad disconnection of computer systems, rendering affected computers incapable of communication with the public, other government agencies, or with other computers at Interior itself. In so doing, the injunction would impair or preclude performance of a whole host of critical functions, and would in large measure incapacitate a Cabinet agency, especially insofar as Native American programs are concerned. See Cason Decl. 4.

As the Cason declaration indicates, the grave and disabling harm resulting from this injunction would, in part, replicate that which would have stemmed from the district court's March

2004 injunction, which was stayed and ultimately vacated by this Court. See also Declaration of W. Hord Tipton (submitted with regard to the 2004 injunction and attached to the government's October 21, 2005 motion for an emergency administrative stay of the October 20 order). Because the October 20 order mandates not only an internet disconnection, but further requires that Interior bureaus sever access internally between their computers and other Interior systems and computers, the damage is even more debilitating.

The loss in work efficiency resulting from disconnection of thousands of computers, used by Interior employees nationwide, can hardly be overstated. The cost to businesses, state and local governments, and members of the public who rely on computer connections to Interior will likewise be extraordinary.

The district did not seriously question the harm resulting from the injunction, but its order suggests that its effect would in some respects be mitigated by allowing disconnected systems to reconnect for 5 days a month. Injunction, § II.D. The proposition that a Cabinet agency can conduct a month's business in 5 days is extraordinary on its face. Moreover, as the Cason declaration explains at length, this provision embodies elementary misconceptions about how these computer systems work. Contrary to the court's premise, "[c]omplex, integrated computer systems that continuously process massive amounts of data in real time cannot feasibly be operated on the kind of 'up and down' basis contemplated by the court's order." Cason Decl. 13.

It is unclear what type of imminent, irreparable harm might ever justify such a draconian injunction. What is plain, however, is that no such harm exists here. The avowed purpose of the injunction is to protect the security of Indian trust data to ensure Interior's ability to provide accurate account statements. The Individual Indian money accounts at issue in this suit contain a total of approximately \$400 million. There is no evidence that any of the Individual Indian account holders in this suit has suffered injury as a result of "hacking." Moreover, as discussed below, all Interior computer systems currently connected to the internet were previously approved by the Court's own Special Master. Further, as the decision acknowledges, Interior has made significant progress in IT

security and has responded to potential weaknesses as they have been identified; indeed, in the last several years, the Department has invested more than \$100 million in IT security. Op. 189

That personnel retained by Interior's Inspector General ("IG") were able to "hack" into some of Interior's systems could provide no plausible justification for the court's disconnection order. The IG's "penetration testing" was initiated by senior management officials as part of the agency's self-testing, pursuant to which weaknesses discovered would be subject to agency remediation. It is commonplace for testing of this kind to result in successful penetration. Indeed, an employee of the firm retained to hack into Interior's computers, who actually conducted hacking himself, estimated that 75% of penetration tests conducted by his firm for government and corporate entities result in successful penetration. (Testimony of Scott Miles, Trans. 5/18/2005 PM, at 62.)

Nor is there good reason to conclude that the harm from such hacking, even if it occurred, would be irreparable. Indeed, although incidents of actual and significant hacking at financial institutions are legion, the district court cited no instance in which a disconnection order was deemed necessary to enforce a legal duty or protect against irreparable harm. At a minimum, it cannot plausibly be contended that the granting of a stay would threaten imminent irreparable harm even remotely comparable to the immediate and catastrophic harm that will certainly result absent a stay.

The government is highly likely to prevail on appeal not only because the court's order departs from basic principles of equitable jurisprudence, but because it lacks a legal and factual basis. The injunction is in all respects standardless. It is not based on findings that Interior has failed to comply with any specific standard of internet security established by statute or governing regulation. Nor did the court find that security standards at Interior pose significantly greater risks than security conditions at other government agencies or in the private sector.

Just as the court pointed to no identifiable standards that had been violated, it likewise articulated no standards that could be achieved to terminate its oversight. The court simply announced that perceived security threats to IIM accounts trump all other concerns and that the district court would sever computer connections until, by its own lights, this priority has been

satisfied. Indeed, each proposal to reconnect any computer system is explicitly made the subject of additional litigation, with plaintiffs authorized to take discovery prior to an evidentiary hearing. Injunction § II.E. At that point, the district court may permit reconnection or impose new requirements as it deems appropriate in its sole discretion. When this Court sanctioned the district court's authority to consider issues of IT security within the scope of this case, it did not thereby approve an order of this kind. Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004).

To the contrary, the injunction embodies the principal vices of structural injunctions already condemned by this Court. The district court has arrogated to itself the functions assigned to the agency head under the Federal Information Security Management Act ("FISMA"). Recognizing that computer security is always relative, the statute requires that responsible agency officials assess security risks presented and determine how to respond to those risks in light of cost considerations and other relevant factors. The injunction wrests that judgment from the hands of responsible officials and vests it in the district court. Indeed, the court's decision is particularly anomalous insofar as it rests on concerns raised by the Interior IG. Under the statute (44 U.S.C. § 3545), the IG is charged with developing an independent assessment of security problems to furnish guidance for the Secretary and for Congress in its oversight capacity. It is the responsibility of the Secretary, not a court, to develop a response. And that response must reflect not only the concerns raised by the IG but other priorities established by Congress and the agency, and the resources made available by Congress in response to the IG's reports.

The court's order thus suffers from the same flaws inherent in structural injunctions already noted by this Court. As this Court explained, a district court may order that action be taken, but it may not supervise compliance with broad mandates, interjecting itself into day-to-day agency management. 392 F.3d at 472. An order requiring reordering of computer security priorities for a Cabinet agency within an ongoing litigation framework turns its back on this guidance. We are unaware of any principle of law that would permit a district court to assume responsibility for overseeing the computer security of an entire Cabinet department, much less any principle that would

authorize the court to direct the “forced disassembly” (Cason Decl. 4) of an agency’s communications networks until it deemed matters satisfactory.

STATEMENT

A. Background.

Plaintiffs filed this class action in 1996 to require Interior to take actions with respect to individual Indian money (“IIM”) accounts. The district court issued a declaratory judgment in 1999, Cobell v. Babbitt, 91 F. Supp. 2d 1 (D.D.C. 1999), which this Court largely affirmed, concluding that the agency had improperly delayed performance of accounting activities. Cobell v. Norton, 240 F.3d 1081, 1108-09 (D.C. Cir. 2001).

Since that initial decision, this Court has heard argument five times in government appeals and has issued four stays pending appeal.

1. In Cobell v. Norton, 334 F.3d 1128 (D.C. Cir. 2003), the Court reversed a judgment of contempt that had been based in part on the district court’s conclusion that the Secretary of the Interior had failed to initiate an historical accounting. Id. at 1150.

2. In September 2003, the district court issued a “structural injunction” that purported to assert control over virtually all accounting and trust operations to be overseen by a Monitor and agents with unlimited powers of access. This Court stayed the structural injunction pending appeal, later reversing except with respect to one reporting requirement. See Cobell v. Norton, 392 F.3d 461, 478 (D.C. Cir. 2004).

3. In February 2005, the district court reissued the accounting portions of the structural injunction verbatim, following expiration of statutory provisions contained in Interior’s FY 2004 appropriations relied upon in this Court’s decision. This Court issued a stay pending appeal and heard argument on September 16, 2005 (No. 05-5068).

4. In October 2003, the government filed in this Court a petition for a writ of mandamus seeking the disqualification of Special Master Alan Balaran under 28 U.S.C. § 455. Mr. Balaran resigned on the eve of oral argument originally scheduled for April 2004. The government believes

that Mr. Balaran's status continues to present a live controversy, and this Court heard oral argument on that matter on October 14, 2005. See No. 03-5288. (This Court had previously held that Mr. Balaran should have been disqualified from certain contempt proceedings on a petition brought by a number of individuals. See In re Brooks, 383 F.3d 1036, 1044-46 (D.C. Cir. 2004)).

5. In August 2005, this Court granted a stay pending appeal of a district court order requiring that the Department of the Interior include in all written communications with any of the hundreds of thousands of Indians comprising the class a notice that all information relating to trust lands or assets is of "questionable reliability." See No. 05-5269 (opening brief due November 21, 2005).

B. The Previous Disconnection Order.

The final appeal to date in which this Court issued a stay and reversed after argument arose from the computer disconnection order issued in March 2004.

On November 14, 2001, Special Master Balaran issued a Report and Recommendation Regarding the Security of Trust Data at the Department of the Interior, which identified deficiencies in the security of Interior's IT systems that the Master believed could detrimentally affect the integrity of Individual Indian Trust Data ("IITD"). Op. 2-3. Following the issuance of the Master's report, the district court on December 5, 2001 entered a temporary restraining order that required Interior to disconnect from the internet all systems housing IITD.

In response, Interior agreed to a Consent Order, issued on December 17, 2001, by which it agreed to a procedure for restoring internet connections. Op. 3. The Consent Order provided that offices would be restored to the internet upon agreement by the Master that the systems were secure or that they provided no access to IITD. Op. 4. Pursuant to the Consent Order, Interior reconnected to the internet systems which did not house or provide access to IITD. Interior also reconnected to the internet several systems which were shown to be adequately secure from unauthorized access. The reconnected systems housing or providing access to IITD included the Minerals Management Service, the Inspector General, the Bureau of Land Management, and the National Business Center.

Other systems housing or providing access to IITD, including the Bureau of Indian Affairs (BIA) and the Office of Special Trustee, remained offline.

On July 28, 2003, the district court entered a preliminary injunction by which the court, rather than the Special Master, assumed full authority over internet access. 274 F. Supp. 2d 111 (D.D.C. 2003). (That order formally “stayed” the Consent Order regime which has thus ceased to operate, as of today, for more than two years. See October 20 Op. 6). The order required Interior immediately to disconnect from the internet all IT systems that house or access IITD, but allowed Interior 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.

On March 15, 2004, the district court issued a preliminary injunction requiring Interior immediately to disconnect all IT systems from the internet, with limited exceptions. This Court stayed the injunction. In December 2004, it vacated the injunction. Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004). Noting that “there was no evidence that anyone other than the Special Master’s contractor had ‘hacked’ into any Interior computer system housing or accessing IITD,” id. at 259, the Court remanded for further proceedings, id. at 262.

C. The October 20, 2005 Injunction.

From May through July 2005, the district court conducted a 59-day evidentiary hearing on Interior’s IT security. Much of the hearing focused on reports and testimony of Interior’s Inspector General’s Office, which had been engaged in ongoing evaluations of Interior’s IT security, including “penetration testing” of some of the agency’s systems.

The injunction requires Interior “forthwith” to “disconnect all Information Technology Systems that House or provide Access to Individual Indian Trust Data” not merely from the internet, but also from Interior’s internal “intranet” systems; from all other Department computers, networks,

or electronic devices; and from any computers or computer networks operated by contractors, Indian Tribes, or other third parties. Injunction § II.A.

The sweep of this requirement is further amplified by the district court's definitions of "Information Technology System," and "Individual Indian Trust Data." An "Information Technology System" is defined to include "[a]ny computer, server, equipment, device, network, intranet, enclave, or application, or any subsystem thereof" used by Interior in any number of ways, "including without limitation computers, wireless devices (e.g. Blackberrys) and networks," as well as any "ancillary equipment, devices, or similar services or protocols." § I.A.

"Individual Indian Trust Data" is not limited to records of IIM account balances, withdrawals, and deposits. Instead, it encompasses all "[i]nformation * * * that evidences, embodies, refers to, or relates to — directly or indirectly and generally or specifically — a Federal Record that reflects the existence of Individual Indian Trust Assets," provided that information was used or produced in some way related to the administration of the trust or in Interior's relationship with individual Indian trust beneficiaries. § I.E. In turn, "Federal Record" includes all federal documentary materials in any physical form whatsoever that are preserved, or are appropriate for preservation, because of their informational content. § I.D. "Individual Indian Trust Assets" include all lands, natural resources, monies, and other assets held in trust for individual Indians by the federal government. § I.B.

The district court fully understood the breadth of the resulting injunctive provisions. "Individual Indian Trust Data," as defined by the court, largely permeates the Department, or, as the district court put it, "[t]he evidence shows that IITD is suffused in varying forms and amounts throughout Interior's network environment" Op. 196.

The injunction exempts from its scope only those systems "necessary for protection against fires or other such threats to life, property, or national security." Injunction § II.C.1. To avail itself of this exemption, agency officials must provide sworn declarations attesting to the need for each exempted network connection on a connection-by-connection basis and explaining the "compensating security controls" that the agency plans to implement to protect trust data. § II.C.2.

The injunction purports to mitigate its impact by allowing Interior to reconnect computer systems for up to five business days per month “for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions.” § II.D. Before it may do so, however, Interior must provide five days advance notice to the court and to the plaintiffs, together with a plan for interim “security controls and measures to cover such reconnection.” Ibid.

Although styled as a preliminary injunction, the order is not preliminary in any generally understood sense. The injunction contemplates no further “merits” proceedings and will continue indefinitely unless and until Interior (and not the moving party) persuades the court to authorize connection of one or more systems. The injunction specifies that Interior may urge such reconnections in proposals that include “a uniform standard to be used to evaluate the security of all Information Technology Systems which House or provide Access to Individual Indian Trust Data,” including data in the custody of contractors and third parties; “a detailed process whereby the uniform standard will be applied to each such” system; “a detailed explanation” of how the system proposed to be reconnected “complies with the uniform standard”; copies of “all documentation relevant” to the security of that system; and a plan to provide “monitoring and testing on an ongoing basis and quarterly reporting to this Court” of the security of the reconnected system. § II.E.1.

Each proposal will then become the subject of additional adversary litigation. The plaintiffs are authorized to take discovery regarding the proposal, following which the district court “will conduct any necessary evidentiary hearing and decide whether a proposed Information Technology System may be reconnected and order further relief, as appropriate.” § II.E.2, 3. The injunction provides no indication of the standard that the district court will apply in that inquiry.

I. A STAY IS NECESSARY TO PRESERVE THE STATUS QUO AND TO AVOID DIRE HARM TO THE GOVERNMENT AND THE PUBLIC INTEREST.

The district court has required a Cabinet department to disassemble much of its electronic communications network, both with respect to the public and other federal agencies, and with respect to its own, internal communications links. While the intended purpose of the injunction is far

different, its effect is the same as an act of computer sabotage designed to bring a government agency to its knees.

To list the specific harms flowing from the injunction is to understate its impact. The consequences of an order severing the internet and internal computer communications of the federal courts can be readily apprehended. The fallout of such an order on an executive branch agency of 70,000 employees is no less significant. The injunction would have a devastating effect on even the most routine communications within and among the Interior bureaus, components, and field offices that handle trust-related information.

It is impossible to prepare an exhaustive list of all operations impaired by the injunction. However, even a partial list leaves no doubt as to the immediate injury inflicted by the ruling in vital areas.

Royalties. Interior receives about \$650 million in royalties every month, which it distributes to parties entitled to revenues, including Tribes and individual Indians. To accept incoming monies, process funds, and disburse payments, Interior depends on automated systems and the internet. The injunction would prevent Interior from making hundreds of millions of dollars in distributions. Cason Decl. 6-7.

Indian Social Services. Interior uses an electronic data processing system to manage and implement social services programs providing qualifying Indians with public assistance for such expenses as child care, adult institutional care, and special needs. Absent access to this system, which would be precluded by the court's order, such assistance payments would grind to a halt. Cason Decl. 5.

Procurement. The preliminary injunction would impair access to systems essential to the Department's procurement activities. Overall, the Department averages more than 50 announcements per business day on requirements that exceed \$4billion annually. Cason Decl. 8-9.

Pay and Personnel. The Federal Personnel Payroll System provides pay and payroll services to about 300,000 employees in 37 federal agencies. The functioning of this and related systems requires that they be connected to the internet and internally to other Interior components and systems. Cason Decl. 10.

E-mail. Because the injunction requires affected bureaus to disconnect individual computers from individual computers, it would deprive users of those computers of even the most basic e-mail capability. This aspect of the order would, by itself, have a crippling effect on the agency's ability to do business. Cason Decl. 10-11.

Telephones. Important parts of the Department's telephone system operate by Voice-Over-Internet-Protocol (VOIP). VOIP is expressly included within the court's

disconnection order. Thus, the order in significant respects would shut down the agency's phone system. Of special but by no means exclusive concern is the BIA's national help desk, which runs on VOIP. Cason Decl. 10-11.

IT Security. The order would have the perverse consequence of degrading Interior's IT security. Disconnected computers would have no ready access to standard security upgrades and "patches," which are downloaded via the Internet. And the process of repeatedly disconnecting and reconnecting complex computer networks, as contemplated in the court's order, is itself a significant security risk. Cason Decl. 11.

Accountings. Ironically, the injunction would stop in their tracks Interior's ongoing efforts to perform the accountings that are at the heart of this litigation. The accounting function, like other Department processes, requires the use of information technology. The agency's accounting work could not proceed if computers and computer systems were disconnected from each other. Cason Decl. 4.

The district court did not seriously take issue with the devastating impact of its injunction. The impact of the injunction is in no way alleviated by its provision that Interior may, after providing written notice to the court and plaintiffs' counsel, "reconnect, for specified periods not to exceed five (5) business days per month, any Information Technology System that Houses or provides Access to Individual Indian Trust Data, for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." Injunction § II.D. As explained by Associate Deputy Secretary Cason, "the apparent premise of this provision – that Interior's interconnected computer systems can be brought 'down' (disconnected) for substantial periods of time, and then brought 'up' (reconnected) for short periods, and then 'down' and 'up' over and over again, and still retain their functional capacity – misunderstands on the most fundamental level how such complex, integrated computer systems work." Cason Decl. 3; see id. at 12-14. As Mr. Cason also noted at length, and as should be self-evident, Interior cannot accomplish in 5 days each month what currently requires an entire month to do. Id. at 3, 12-14.

Granting a stay to preserve the status quo and to avoid immediate harm to the public interest and the operation of a major federal agency will result in no countervailing irreparable harm to plaintiffs. There is no indication that any named plaintiff or any member of the class has ever experienced injury, or that any trust data has ever been manipulated, as a result of hacking into

Interior systems by persons other than the IG team and the former Special Master. Indeed, all the systems now on-line were approved for reconnection by the court's own Special Master.

As the district court itself repeatedly stressed, Interior has made substantial and ongoing progress in IT security. E.g., Op.154 (“substantial progress . . . in a very short time”); Op.197 (“has made strides”; “laudable”). Even the IG, despite his calls for further improvements, observed in a 2004 report to Secretary Norton and Congress that “DOI has effectively designed its information security management program to meet [statutory requirements] and continued to improve security over its information systems.” FY2004 FISMA Report, quoted at Op.153. The district court did not explain why, despite these comprehensive and ongoing improvements, immediate disconnection of systems was needed to prevent imminent irreparable harm to the plaintiff class. Nor is there any finding that penetration of Interior's computer systems by a hacker, if it occurred at all, would necessarily produce irremediable harm.

In short, a stay pending appeal is necessary to avoid overwhelming harm to a Cabinet agency and the public it serves, and will result in no countervailing harm to plaintiffs. The expedition proposed by the government further minimizes any conceivable harm that plaintiffs might claim results from a stay.

II. THE GOVERNMENT IS HIGHLY LIKELY TO PREVAIL ON APPEAL.

A. The Order Cannot Be Reconciled With Basic Principles of Equity.

The manner in which the district court balanced the relative harms at issue bespeaks a fundamental misunderstanding of the limitations of a court's equitable powers.

1. The classic purpose of a preliminary injunction is to maintain the status quo. University of Texas v. Camenisch, 451 U.S. 390, 395 (1981) (“The purpose of a preliminary injunction is merely to preserve the relative positions of the parties until a trial on the merits can be held.”); FTC v. Weyerhaeuser Co., 665 F.2d 1072, 1094 (D.C. Cir. 1981). The injunction fails even this threshold standard: the injunction destroys crucial communications networks of a Cabinet department while

requiring disconnection of systems approved for reconnection by the court's own special master. Moreover, the injunction is not "preliminary" to any pending "merits" dispute. It will remain in effect until Interior carries a burden of persuading in further adversary proceedings that individual systems should be reconnected.

2. No injunction may issue unless the movant demonstrates that "irreparable injury is 'likely' to occur. Bare allegations of what is likely to occur are of no value since the court must decide whether the harm will in fact occur. The movant must provide proof that the harm has occurred in the past and is likely to occur again, or proof indicating that the harm is certain to occur in the near future." Wisconsin Gas Co. v. FERC, 758 F.2d 669, 674 (D.C. Cir. 1985) (per curiam) (citation omitted, emphasis in original).

Even with the benefit of a 59-day trial, plaintiffs have manifestly failed to demonstrate that harm to be avoided has occurred in the past. That the Special Master and the IG, armed with expertise, resources and immunity from prosecution, were able to penetrate Interior systems does not demonstrate that other persons will have the motivation or means of doing so, let alone that irreparable harm to trust data would result from such a penetration.

3. Injunctive relief should be no more burdensome to the defendant than necessary to provide complete relief to the plaintiffs. See ALPO Petfoods, Inc. v. Ralston Purina Co., 913 F.2d 958, 972 (D.C. Cir. 1990) ("The law requires that courts closely tailor injunctions to the harm that they address."); Gulf Oil Co. v. Brock, 778 F.2d 834, 842 (D.C. Cir. 1985). Computer security, as the district court itself acknowledged, is never absolute, and, Interior's security has not been found to be in violation of any specific substantive standard. Nor has it been shown that Interior's systems are less secure than those of other government agencies or of private sector institutions. Even assuming that plaintiffs had demonstrated entitlement to some relief to provide additional security, it would be inconceivable that large-scale disconnection of Interior computers would be the best or only way of providing security enhancement.

4. As this Court has long made clear, a preliminary injunction must “eventuate from a careful consideration of all important factors of relevance, not the least of which is the public interest.” Udall v. D.C. Transit System, Inc., 404 F.2d 1358, 1360 (D.C. Cir. 1968) (per curiam); see Yakus v. United States, 321 U.S. 414, 440-41 (1944). The injunction treats the protection of IIM accounts from hacking as an absolute imperative, to be achieved regardless of the actual risk to IIM accountholders of imminent or irreparable injury, and without regard to the vast array of public services that will be undermined. Principles of equity do not enable a court, acting without statutory mandate, to curtail services to millions of Americans in the name of protecting the IIM accounts from the theoretical threat of hacking. The court’s disregard of the public interest is all the more extraordinary because the adverse impact of its injunction will be felt by many class members to an extent at least as great as the public generally. Nor can class members take solace in the belief that the injunction, whatever hardships it may impose, at least advances their interest in obtaining timely and accurate account statements. An injunction that destroys external and internal computer communications links can hardly be said to advance the goal of providing effective computer systems that this Court noted would be necessary to accounting activities. 391 F.3d at 256-57; 240 F.3d at 1106. The asserted gain in security – which is itself chimerical (Cason Decl. 11) – comes at the price of disabling or impairing all other computer functions crucial to accounting activities. Cason Decl. 4.

The district court was aware of “the ways in which the department’s operations were disrupted by this Court’s last disconnection order,” and noted in passing “the effects that a loss of Internet connectivity would have on the department’s ability to service its customers, many of whom are other governmental agencies.” Op.201. The court’s response was to declare that “[t]he relief granted today is not likely to prove popular in governmental circles. The Court is not, however, in the business of doing the popular thing, or the politically savvy thing. The Court must evaluate the evidence presented, and take the action that is warranted by that evidence.” Op.201. At the most fundamental level, the court failed to apprehend that its equitable powers to not authorize it to

frustrate the communications of an executive branch agency, undermining its “ability to service its customers,” many of whom are not only government agencies but members of the plaintiff class.

B. The Injunction Is Without Any Basis And Improperly Asserts Continuing Control Over The Communications Networks of An Executive Branch Agency.

1. As an initial matter, there can be no question that the Interior Department under Secretary Norton has not only taken action, but taken effective action, to remedy IT security weaknesses that existed at the inception of the Special Master regime in 2001. (Indeed, under that regime, the Special Master had approved 95% of Interior computer systems for Internet reconnection. Op. 5.) As the district court observed, “[t]here can be no doubt that Interior has made substantial progress in implementing a comprehensive departmental IT security program in a very short time” Op. 154. See also Op. 197 (“It is * * * undeniable that Interior has made great strides in the IT security arena”; “Interior’s progress in a period of five years is laudable”).

Similarly, notwithstanding its criticisms of aspects of IT security, Interior’s IG has also recognized Interior’s substantial progress. A 2003 IG report stated that “during fiscal year 2003 Interior has undergone monumental change to improve its information security program. These changes[] serve as a springboard for the DOI to ensure that all information and information systems and assets are cost-effectively secure. The Secretary, the Deputy Secretary, the Assistant Deputy Secretary, and the Assistant Secretary for Policy, Management, and Budget have demonstrated strong support in addressing DOI’s information security weaknesses.” Op.151 (quoting report). Similarly, a 2004 IG report declared that “DOI has effectively designed its information security management program to meet the requirements of FISMA and continued to improve security over its information systems.” Op.153. Indeed, the IG accepted the Secretary’s request to have penetration testing performed in FY2005 precisely because he felt the agency had improved its IT security systems to the point that penetration testing would be a useful diagnostic tool. Op. 64- 65. The penetration tests using skilled experts undertaken with the encouragement and support of Associate Deputy Secretary Cason, who contacted the IG in 2003 and said that “he was at a point where he wanted to

begin to see if the systems would withstand penetration.” Op.68. Mr. Cason offered to provide the IG funding to hire an appropriate contractor to conduct such testing. Op. 68. This offer allowed the IG “to jump start [a] program that I was trying desperately to find funds” to implement. Op. 68-69.

In short, whatever circumstances may have prompted the Special Master regime in 2001 cannot serve as the basis for a sweeping new injunction in 2005, an injunction that extends beyond a debilitating Internet disconnection and requires as well the severing in critical respects of internal communications links within the Department and among and between Interior components. The injunction must rest on a firm legal and factual foundation, which is plainly lacking in these circumstances.

2. Federal law, like private sector practice, does not establish specific, substantive standards of IT security. Instead, it establishes a process for assessing risks and responding to those risks in a cost-effective manner. The Federal Information Security Management Act (“FISMA”) requires agency heads to provide security protections “commensurate with the risk and magnitude of the harm resulting from unauthorized access. . . .” 44 U.S.C. § 3544(a)(1)(A). These protections must be implemented through security processes “integrated with agency strategic and operational planning processes.” Id. § 3544(a)(1)(C). The agency must design an “agencywide information security program” that must be “develop[ed], document[ed] and implement[ed],” § 3544(b), including policies and procedures that “cost-effectively reduce information security risks to an acceptable level” on the basis of “the risk assessments required by [the statute.]” § 3544(b)(2)(A),(B).

The Director of OMB is to supervise compliance with FISMA by, inter alia, “reviewing at least annually, and approving or disapproving, agency information security programs.” § 3543(a)(5); see also § 3544(b). OMB is also responsible for “developing and overseeing the implementation of policies, principles, standards, and guidelines on information security.” § 3543(a)(1). OMB’s principal IT security policy is set forth in Appendix III to OMB Circular A-130, which “establishes a minimum set of controls to be included” in IT security programs. App. III A(1)

“[A]dequate security,” the organizing principle of the policy, is defined as “security commensurate with the risk and magnitude of the [potential] harm [to a system].” App. III A(2)(a). “This definition explicitly emphasizes the risk-based policy for cost-effective security” embraced by FISMA. App. III B.

FISMA requires annual, independent evaluations of the information security program and practices of each agency to be performed by the agency Inspector General. 44 U.S.C. §§ 3545(a)(1), (b)(1). That delegation to the IG is consistent with the broader role envisioned for Inspector Generals within the executive branch. The IG is generally authorized to make “investigations and reports relating to the administration of the programs and operations of the applicable” agency, 5 U.S.C. App. 3, § 6(a)(2), and is given a right of access to “all records, reports, audits, reviews, documents, papers, recommendations, or other material” in the agency, *id.* § 6(a)(1), as well as the power to subpoena any other “data and documentary evidence necessary in the performance of the functions assigned by this Act,” *id.* § 6(a)(4). The IG reports to the agency head, but is required to submit semiannual reports that are transmitted by the agency to Congress. *Id.* §§ 5(a) & (b).

In sum, governing law requires agencies to take cost-effective measures based on risk-evaluation. It establishes procedural requirements subject to review by the Inspector General that facilitate oversight within the executive branch as well as congressional oversight.

3. The injunction sets aside this nuanced scheme. It not only imposes the district court’s own, standardless assessment of priorities and risks (without regard to cost as required by the statute) but requires disconnection of essential communications links, a remedy nowhere contemplated by the governing scheme. In so doing, the court explicitly reordered not only the agency’s priorities but even those of the IG. The court thus criticized the IG’s “failure to place special emphasis on scrutinizing Interior’s efforts to provide adequate security for IITD housed on or accessed by Interior’s IT systems,” believing this to demonstrate “a serious deficiency in Interior’s overall IT security program with respect to Interior’s fiduciary obligations.” Op. at 193.

The district court's belief that the fiduciary nature of the trust relationship authorized it to assume responsibility for Interior's computer systems and direct its security priorities is wholly without basis. Whatever role the fiduciary relationship may play in elaborating Interior's duties to account holders, it does not provide a basis for subordinating all other concerns and duties owed to millions of Americans to the perceived threat to IIM accounts from computer hackers.

Moreover, as this Court has recognized, in private trusts, the costs of trust administration are met from the trust itself, 392 F.3d at 473, and decisions necessarily incorporate a cost-benefit analysis. Private beneficiaries would be unlikely to authorize staggering expenditures wholly incommensurate with any real threat of irreparable harm to their accounts. Nor, of course, would a private trustee be told to cease services to millions of clients to achieve purported gains in computer security for one group of beneficiaries.

As this Court has also explained, general principles of fiduciary law do not contemplate a judicial takeover of trust activities. "[P]rivate trustees, even though held to high fiduciary standards, are generally free of direct judicial control over their methods of implementing these duties, and trustee choices of methods are reviewable only 'to prevent an abuse by the trustee of his discretion.'" 392 F.3d at 473 (citing Restatement (Second) of Trusts §§ 186-87 (1959)). Thus, as Professor Langbein explained earlier in this litigation, under common law principles, a court would be reluctant to interfere with the manner in which a trustee seeks to implement its duties, particularly when the trustee must determine how best to use limited funds to achieve an objective. See Tr., June 3, 2003 p.m., at 74-76, 78-79; Tr., June 3, 2003 a.m., at 33-34, 39, 67-68.

4. Although not styled as such, the present order is a structural injunction of the same type as the two structural injunctions that the district court issued in 2003 with respect to accounting and non-accounting activities. The difference in this instance is that the district court has not only undertaken to determine how the agency should meet its responsibilities, but has issued an order that would cripple its operations across-the-board in areas wholly unconnected to this lawsuit.

As the Court held in reversing the structural injunction governing non-accounting matters, a district court is empowered “only to compel an agency ... to take action upon a matter, without directing how it shall act.” 392 F.3d at 475 (quoting Norton v. Southern Utah Wilderness Alliance, 124 S. Ct. 2373, 2379 (2004)). The purpose of “[t]he APA’s requirement of ‘discrete agency action,’ ... was ‘to protect agencies from undue judicial interference with their lawful discretion, and to avoid judicial entanglement in abstract policy disagreements which courts lack both expertise and information to resolve.’” 392 F.3d at 472 (quoting Southern Utah, 124 S. Ct. at 2381). “If courts were empowered to enter general orders compelling compliance with broad statutory mandates, they would necessarily be empowered, as well, to determine whether compliance was achieved – which would mean that it would ultimately become the task of the supervising court, rather than the agency, to work out compliance with the broad statutory mandate, injecting the judge into day-to-day agency management.” Ibid. (quoting Southern Utah, 124 S. Ct. at 2381).

This structural injunction is no more defensible than that vacated by this Court. It does not purport to compel discrete action or to compel compliance with any identifiable standard. Instead, it interjects the district court into the oversight of all IT security at the Department of Interior for the foreseeable future, compelling a reordering of priorities to meet an unstated standard of safety while thoroughly vitiating the electronic communications structure of an executive branch agency. The order is unprecedented and, prior to this litigation, would have been inconceivable.

CONCLUSION

The district court's October 20, 2005 preliminary injunction should be stayed pending appeal. We further ask that the Court order expedited briefing to resolve the issues presented by the district court's order at the earliest possible time.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room, 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

Robert E. Kopp
Mark B. Stern
Thomas M. Bondy
Alisa B. Klein
Mark R. Freeman
I. Glenn Cohen

OCTOBER 2005

CERTIFICATE OF SERVICE

I hereby certify that on this 27TH day of October 2005, I caused copies of the foregoing motion to be sent to the Court and to the following 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
Mark I. Levy
Kilpatrick Stockton
607 14th Street, N.W.
Washington, D.C. 20005
(202) 508-5800

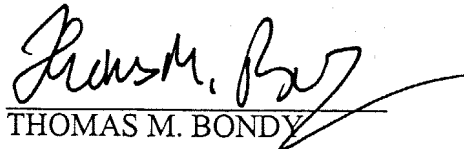
and to the following by federal express, overnight mail:

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


THOMAS M. BONDY

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

ELOUISE PEPION COBELL, et al.,)
)
Plaintiffs-Appellees,)
)
v.)
)
GALE A. NORTON,) No. 05-5388
Secretary of the Interior, et al.,)
)
Defendants-Appellants.)
)
_____)

**DECLARATION OF JAMES E. CASON IN SUPPORT OF
MOTION FOR STAY PENDING APPEAL**

I, James E. Cason, am the Associate Deputy Secretary of the United States Department of the Interior (Interior, or the Department). In my capacity as Associate Deputy Secretary, I share authority and responsibility at the Secretarial level for the oversight and management of the Department's Indian trust and associated reform efforts. In that role, I coordinate with the Department's Chief Information Officer (CIO) and with Bureau/Office CIOs in the management and supervision of Interior's information technology (IT) portfolio, and I am involved in the development and maintenance of the Department's IT systems. In my capacity as Associate Deputy Secretary, I rely upon information from Interior management and staff to make program management decisions and to prepare communications with the Court, as is the case with this declaration.

The Department of the Interior is a Cabinet level agency with an approximate annual budget of \$11 billion and employing approximately 70,000 employees. It provides an array of crucial services for individual Indians and Indian Tribes. The Department also manages 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. In addition, the Department performs a variety of critical functions on which other federal agencies rely.

To meet its responsibilities, the Department manages a portfolio of approximately \$1 billion of information technology, including approximately 100,000 computers. Generally speaking, those computers have access to the Internet through specified gateways ("Points of Presence"), and to each other through multiple networks internal to Interior.

I. OVERVIEW

In March 2004, the district court issued an order generally requiring disconnection of Interior computer systems from the Internet. The March 2004 order was promptly stayed, and eventually vacated, by the Court of Appeals. Had it been allowed to go into effect for any significant period of time, the order would have been devastating in its impact, largely crippling the Department and its ability to serve the Nation.

The October 20, 2005 order issued by the district court is potentially much more damaging than the earlier disconnection order. Like the March 2004 order, the October 20, 2005 order contains an Internet disconnection component, requiring immediate disconnection of specified systems from the Internet. As explained in more detail below, that component of the October 20 order, in and of itself, would have a debilitating effect on the Department's capacity to carry out essential functions, reflecting the reality that, in this day and age, the Internet is integral to much of what Interior and its components do.

The October 20, 2005 order goes even further than the March 2004 order. The definitions in the order are extraordinarily broad, underscoring the order's reach. The disconnection order applies to "all Information Technology Systems that House or provide Access to Individual Indian Trust Data." Under the order, the term "Information Technology System" means "Any computer, server, equipment, device, network, intranet, enclave, or application, or any subsystem thereof, that is used by Interior or any of its employees, agents, contractors, or other third parties in the electronic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or other information * * *."

Perhaps even more broadly, "Individual Indian Trust Data" is defined by the order to include "Information stored in, or transmitted by or through, any Information Technology System that evidences, embodies, refers to, or relates to – directly or indirectly and generally or specifically – a Federal Record that reflects the existence of Individual Indian Trust Assets, and that at any time" has been or is now used in any number of specified ways.

Under the Order "Interior defendants forthwith shall disconnect all Information Technology Systems that House or provide Access to Individual Indian Trust Data" from the Internet, the Intranet (the Department's internal data communications networks), all other information technology systems and any contractors, tribes or other third parties. Hence, in addition to disconnection of external links, the Internet and to contractor/Tribal/third party organizations supporting Departmental activities, the order also requires disconnection of internal computer links (Intranet) between departmental organizations, and within the bureaus and offices themselves.

Indeed, the order goes so far that to comply individual computers that house IITD would need to be disconnected from all other individual computers and devices and the underlying data network. Computer systems networking is critical to the Department's complex, sophisticated

and often time-sensitive operations (e.g., preparation of accounting statements, processing of leasing and title information, calculation and disbursement of royalty payments, etc.), many of which are conducted for the direct benefit of individual Indians and Tribes. The operations must rely upon networks of automated electronic systems that are fundamentally integrated and must continually communicate with each other in order to fulfill their designated tasks.

E-mail service would also be adversely affected. The order makes clear that the computers to be disconnected must be disconnected from all other computers. Thus, users of the disconnected computers would be deprived of even the most basic e-mail capacity.

Implementing the court's order would result in the loss of telephone service for employees who depend on "Voice Over Internet Protocol" (VOIP) telephone systems. VOIP is expressly included in the order's definition of "Information Technology Systems" to which the court's injunction applies (as are hand-held wireless "Blackberry" devices, which provide both telephone and e-mail services).

The injunction contains an exception for systems that are "necessary for protection against fires or other such threats to life, property, or national security." However, this exception does not address the practical reality that underlying data networks are commonly shared by employees with a broad range of missions, some of which would be permitted and some of which are prohibited. The Order contains no exception for programs that are otherwise crucial to the Department's operations and to the public welfare.

The injunction also provides for the possibility that disconnected systems could be reconnected, for specified periods not to exceed 5 business days per month, "for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." Interior cannot accomplish in 5 days each month what currently requires an entire month to do. Moreover, even if some limited portion of essential services could be provided during the 5-day window, the apparent premise of this provision – that Interior's interconnected computer systems can be brought "down" (disconnected) for substantial periods of time, and then brought "up" (reconnected) for short periods, and then "down" and "up" over and over again, and still retain their functional capacity – misunderstands on the most fundamental level how such complex, integrated computer systems work. As detailed below, the "5 days per month" provision does not mitigate the extraordinary harm that the order would inflict on the Department and on the public that it serves.

Finally, because of the extraordinary breadth of the various definitions contained in the injunction, it is possible that if and when the Interior Department were actually required to implement the order, serious issues would be raised as to whether the injunctive provisions must be construed even more broadly than contemplated herein. In that event, the harms to the Department, to other federal agencies, and to the public would be even graver and more wide-ranging than those set forth in this declaration.

It is impossible to catalogue briefly the full range of programs adversely affected by this court's injunction, although it is clear that Native American programs would be dealt a devastating blow. The following discussion only begins to catalogue the anticipated harms associated with implementing the district court's Order.

II. IRREPARABLE HARM THAT WOULD RESULT FROM IMPLEMENTATION OF THE INJUNCTION

Four primary Interior components have been disconnected from the Internet since 2001: the Bureau of Indian Affairs (BIA); the Office of Special Trustee for American Indians (OST); the Office of Hearings and Appeals (OHA); and the Office of the Solicitor (SOL). It is important to understand that, even with respect to these disconnected components, the October 20, 2005 injunction would inflict massive, disabling harm. Under the terms of the order, these components not only would be unable to access the Internet, but, in addition, they would be unable to communicate with each other. Perhaps even more destructive, individual computers within the same network, bureau, or office would be disconnected from every other individual computer, in effect leaving each affected computer as a stand-alone unit isolated from every other computer in the Department of the Interior. Thus, the power and productivity provided by Interior's networked computer systems would be terminated in order to reduce some perceived, but unquantified risk, that the systems may be compromised at some point in the future.

This forced disassembly of the networked capability of the Departments complicated computer systems would materially undermine our ability to undertake and successfully complete many of our statutory and regulatory missions, particularly those that provide services for Native Americans. Some key examples of anticipated adverse impacts include:

Historical Accounting

One of the direct effects of the district court's injunction would be to halt Interior's ongoing efforts to provide the historical accountings that are at the heart of this litigation. As should be self-evident, the Department's functions in general, including the accounting function, rely in critical respects upon interconnected, large-scale computer networks. The complex task of performing the accountings for IIM beneficiaries and preparing account statements simply cannot be accomplished without use of the Department's computer systems and access to underlying data.

Management of Indian Trust Funds.

OST's access to the Trust Funds Accounting System ("TFAS") is another example of third-party connectivity that would be severed by the Preliminary Injunction. TFAS is the accounting and investing system that controls and enables the processing of Indian trust funds; it is hosted by SEI, a major contractor in the field of trust management and banking. The loss of access to TFAS would have a broad and devastating impact upon individual Indians and Tribes.

Among other things, OST utilizes TFAS to make payments on behalf of beneficiaries to nursing homes, foster care facilities, automobile and mortgage financing institutions, hospitals, and schools. The disconnection of access to TFAS would have a crippling effect on OST's ability to make these and related kinds of payments, and also upon Interior's basic ability to prepare account statements for hundreds of thousands of Individual Indian Money (IIM) account holders and holders of other accounts.

OST also utilizes TFAS as the primary accounting and investing system for over \$3.2 billion of Tribal and individual Indian funds. Loss of access to TFAS would thus impact tribal operations, tribal infrastructure development, economic development, and would affect payments for services as diverse as education, loans, and burials.

Indian Land-Ownership Records Data.

The Trust Asset Accounting Management System ("TAAMS"), which is hosted by a contractor (CGI, Inc.), is used to provide nationwide access to trust land ownership data and trust asset management tools. If BIA's access to TAAMS were disconnected, which would be required by the terms of the order, BIA would lose the ability to provide accurate, timely and cost-effective land title services for individual Indians and Tribes. In fact, field offices would not be able to respond to a variety of inquiries from beneficiaries regarding the status of their holdings, except to the extent such inquiries could be addressed by the presence of "hard copies" of reports in a particular office. The severance of this connection would cause serious record-keeping backlogs in areas as diverse as the recording of leasing encumbrances, the provision of certified titles and inventories for realty transactions, and probate matters.

The Land Records Information System (LRIS) is used for limited reporting purposes by a small number of BIA agency offices to verify records and by the Office of Historical Trust Accounting (OHTA) to access data from historical title records. Access to this system, too, would be cut off by the October 20 injunction.

Interrupted Social Services to Indians.

BIA is responsible for generating and distributing social services payments for individual Indians. To perform that function, it relies upon the automated Social Services Assistance System (SSAS). The SSAS system is used by BIA's field locations (agency and tribal locations) and Regional Offices to approve and authorize such payments. The SSAS system, used by BIA and Tribes, contains the financial, budgetary and statistical data used to generate checks for public assistance and maintain individual's files. The payments generated from this application relate to child care, general assistance, adult institutional care, special needs and emergency aid. Absent access to SSAS, which would be precluded under the court's order, such payments would grind to a halt.

Indian Land Irrigation Operations.

The National Irrigation Information Management System ("NIIMS") provides irrigation billing and collection for operations and maintenance, as well as construction assessments for certain projects. BIA would also lose access to NIIMS under the court's order. BIA's loss of access to NIIMS would seriously undermine, if not eliminate, its ability to provide required irrigation services, generate associated irrigation services billings, or to manage debt in connection with those billings.

Federal, State and Indian Royalties Payments

The Minerals Management Service (MMS) receives, processes, and disburses over \$650 million in mineral revenues on Federal and Indian leased lands each month. Of the \$650 million, approximately 2.0 % belongs to Indian Tribes and approximately 0.5% belongs to individual Indians.

MMS accomplishes its assigned royalty management mission through delivery of reporting, accounting, and financial services. About 2,000 companies report and pay royalties to MMS each month. All such functions are heavily reliant on automated systems and access to the Internet. In particular, hundreds of millions of dollars in royalty and lease payments are made electronically to MMS using the Internet.

Minerals revenues are a major source of income for 41 Indian Tribes; approximately 20,000 individual Indian minerals owners; the federal government, and 38 states. The court's injunction would effectively disable MMS from being able to make timely monthly disbursements of over \$650 million in mineral revenues not only to tribal governments and 20,000 Indian accounts, but would also have the same effect on state and public land accounts now disbursed to the States or the U.S. Treasury as revenues. In and of itself, this would be an immense and severe consequence of the October 20, 2005 injunction.

The proper and timely processing of payments of royalties, rents, and bonuses to individual Indians and Tribes stemming from leasing activities is dependent, not only upon an MMS Internet connection, but also upon internal connections (intranet) between two other Interior bureaus: OST and BIA. In connection with activities as diverse as agricultural leases, forestry leases, and sand and gravel leases, amounts are paid to individual Indians and Tribes only after mutual, integrated processing by multiple bureaus and offices.

The interrelationships among MMS, OST, and BIA are illustrative of why the Preliminary Injunction's Intranet disconnection requirement would cause immediate, severe and irreparable harm. Over the course of every month, MMS receives over 550,000 lines of revenue and production data from oil and gas lessees, a small portion of which pertains to leases that benefit individual Indians, with the greater portion benefitting Tribes, States and the federal government. Lessees make payments in gross, which are deposited in the Treasury. The incoming payments

and related royalty data are unsegregated and do not distinguish among beneficiaries with an interest in each lease; interests in a single lease may include a Tribe and individual Indians.

After MMS initially enters the incoming royalty information, information is communicated to BIA and OST for the additional processing needed to identify payments to be made to the Tribes and individual Indians. OST is responsible for accounting for the receipt, investment, and disbursement of monies to individual Indians and Tribes. OST, in turn, cannot disburse the amounts received without receipt of ownership information from BIA that is provided through an Intranet connection with BIA. OST also receives through the Intranet information to produce an explanation of payment statement, which is required by law to accompany royalty checks to beneficiaries. The October 20, 2005 injunction would sever that access.

Interior's National Business Center (NBC), BIA and OST currently process the information described above using an internal connection. Relying upon this internal connection, BIA is able to take a gross receipt for a lease, access ownership records, and determine which beneficiaries have an interest in the lease. Using this information, BIA identifies who should receive a payment from a gross lease payment, the amount of the payment to each beneficiary, and processes timely payments by printing checks and electronic funds transfers to individual Indian beneficiaries and Tribes.

If the internal connection among NBC, OST, and BIA were disconnected, as required by the Preliminary Injunction, it would not be possible to provide timely and accurate royalty, leasing, and bonus payments to individual Indians and Tribes. This is separate from and in addition to the dislocation that would flow from cutting off MMS access to the Internet.

MMS also utilizes contractors in the processing of hundreds of millions of dollars in royalties, rents, and bonuses each month. MMS requires the use of its MMSNet (Intranet) to communicate with the contractors, who in turn process the royalty and production information received from oil and gas producers. Without MMSNet (and the connections to the contractors), MMS would be unable to process data relating to recipients of oil and gas royalties and other revenues. Among the contractors involved in this process is USi, which maintains a "data center" for processing receipts of royalties, rents, and bonuses. If MMS's connection to USi were severed, as mandated by the October 20, 2005 injunction, MMS would lose timely access to data warehoused at USi, and this loss would further critically disable the processing of timely and accurate payments of royalties, rents, and bonuses to individual Indians, Tribes, and States.

Offshore Energy Operations.

Current supply disruptions from offshore energy production, as precipitated by recent hurricanes, are causing serious negative impacts to the nation's economic and energy security. At present, MMS is actively implementing a Continuity-of-Operations Plan to expedite the approval of plans and permits to enable the return and recovery of offshore production to meet

the nation's energy needs. Web-based electronic processing of permits is an integral tool employed by MMS to expedite this recovery operation. Curtailment of multiple applications of electronic business under the October 20, 2005 order would forestall these processes and detract from the flow of our domestic energy supply.

MMS's Public Information Data System (PIDS) is a huge electronic repository of publicly available document images, consisting of documents such as geophysical and geological permits, plans of exploration and development, and drilling permits. This system contains over one million documents and approximately 2,000 documents are added weekly on average. Prior to the implementation of PIDS, it was necessary for customers to visit the Public Information Office in order to obtain copies of the paper documents. PIDS is used over 6,000 times per month. (This does not represent the actual number of documents viewed during these visits.) Many of the paper copies of documents contained within PIDS are no longer immediately accessible at MMS's offices, as they have been archived at Federal Records Centers.

Maintaining the availability of this database is crucial at this point in time, when industry and government agencies are stretched thin to restore oil and gas production vital to our nation's well-being. Disconnecting this system would forego efficiencies in locating and retrieving information needed for renewed exploration and development in the Gulf of Mexico. Delays could reasonably be expected to adversely impact the return of full production following Hurricanes Katrina and Rita from the Gulf of Mexico, which supplies 27% of our nation's oil production and 20% of the natural gas production.

A particular Government website – <http://www.gomr.mms.gov/index.html>, which is associated with the MMS Gulf of Mexico Region (GOMR) – is used by industry to download the location of platforms, pipelines wells, etc. This information is used to conduct exploration, drilling, and production operations, and its availability is critical to ongoing operations. Access to GOMR by pertinent Interior components would be disconnected under the terms of the district court's order.

Departmental Procurement Activities.

Implementation of the court's order would have a similarly consequential impact on the Department's procurement activities. In particular, it would prevent key Interior users from accessing the Interior Department Electronic Acquisition System-Electronic Commerce (IDEAS-EC) via the Internet to obtain procurement data necessary to perform their duties. A significant number of users would be unable to initiate or complete any contract actions in the system. Vendors would be unable to obtain electronically contract actions such as delivery orders, modifications, change orders to contracts, or to provide proposals to active procurement actions, and the Department's solicitations for vendor response through the electronic commerce process would be blocked because vendors would be unable to submit the required electronic offers. A particular impact would be to Small and Disadvantaged Business Owners, which constitute a significant portion of the procurement transactions and payments for impacted bureaus such as

BIA and MMS. Further, a significant number of the Department's contracting officers and grants officials would be unable to access the Excluded Parties Listing System (EPLS), which identifies people and companies that have been suspended or debarred from doing business with the federal government.

The cumulative impact of these disabilities would be very substantial. The Department averages more than 50 announcements per business day on requirements that exceed \$4 billion dollars in obligations annually.

Departmental Financial Management Activities.

The Federal Financial System (FFS) provides financial accounting, funds control, management accounting, and financial reporting processes for the Department's bureaus and offices, as well as approximately twenty entities outside the Department. Most of the Department's bureaus use FFS to manage and control financial activity related to appropriated funds (approximately \$11 billion annually), including funds management, payments to vendors, reimbursement of charge card transactions, travel reimbursements, and other financial transactions.

The Department's Consolidated Financial Statement (CFS) system is critical for the preparation of bureau and Department financial statements. The CFS System provides financial statement management and reporting capabilities to all Department bureaus and offices and to non-Interior clients. In addition, the CFS System also supports the annual financial statement audits of the Department and its bureaus and provides access to the KPMG audit team engaged by the Department's Inspector General. Under the court's order, the Department would not be able to meet monthly, quarterly, and year-end financial statement deadlines, would be unable to reconcile account balances, and it would be unlikely that the Department could complete its annual financial statement audit, in violation of the Government Management Reform Act and OMB Circular A-136. Further, delays in the completion of bureau financial statements would substantially increase the audit costs and jeopardize the data submission to Treasury for the consolidated financial statements of the federal government.

Similarly, the Department uses the automated CASHLINK system to view daily receipts and disbursements for daily reconciliation of account balances with Treasury. Without daily reconciliation, funds may be either over- or under-invested, with associated financial repercussions, as manual processes cannot be done timely.

In order to function properly, core systems such as FFS must have an internal (Intranet) connection within Interior to Department bureaus and offices, even apart from any Internet connection. The court's order severs those internal links, at least with respect to those bureaus that house or have access to Individual Indian Trust Data (IITD), including, for example, MMS, BIA, and OST. The aggregate effect of destroying those links would be enormous: it would remove the Department's basic ability to sustain the integrity of its financial management operations.

BIA also uses the Fixed Asset Subsystem (FAS) of FFS to manage personal and real property assets, including schools and law enforcement facilities, valued at more than \$2.6 billion. Without access to FAS, BIA would not be able to provide information to Tribes of surplus property or ensure accountability for property. BIA has been working to overcome a material weakness in property management. Without access to its system of record for property management, it would be unable to respond to auditors or perform the necessary functions to properly manage property assets.

Departmental Hiring and Personnel Support.

The Federal Personnel Payroll System (FPPS) currently provides pay and payroll services to about 300,000 employees in 37 federal agencies. Without proper information from FFS and FPPS, employees could still be paid, but there would be errors, and corrections would have to be made manually. The disconnection of both Internet and intranet connections would, for a significant part of the Department, result in an inability to process personnel actions in a timely or effective manner. This includes appointment of new hires, promotions, awards, reassignments, retirements, transfers to other government agencies, and changes in employee benefit options (e.g., the Thrift Savings Plan). In addition, withholding and deposit of taxes and payment of alimony and child support would be adversely impacted.

Automated systems such as FFS, FPPS, and IDEAS are absolutely critical to the ability of the Department to maintain the basic electronic infrastructure that allows it to perform such fundamental operations as financial management, payroll and personnel, and procurement. For Interior's purposes, the functioning of these systems requires that they be connected not only to the Internet, but also internally to other Interior components and systems (Intranet).

Managing The Freedom of Information Act (FOIA) Program.

The Department has Electronic Freedom of Information Act ("E-FOIA") capabilities required by 5 U.S.C. § 552(a)(2)(E). E-FOIA requires the Department to make records subject to FOIA electronically available. Given the broad definition of IITD, the E-FOIA system would be disconnected from the Internet and DOI's intranet. The total number of FOIA requests would likely increase as a result of disconnection because some of the public information currently available on the Department's websites would no longer be available on-line. The time required to process the average FOIA request would increase because the FOIA guidance currently available on the Department's website would no longer be available.

Terminating E-Mail and Telephone Service.

The Preliminary Injunction's requirement that the Interior Department disconnect specified Intranet connections would also prevent employees of the affected bureaus and offices from communicating with each other by e-mail. This is because e-mail communication is dependent upon access to a mail server, and for bureau-to-bureau or bureau-to-office connections, access to the Virtual Private Exchange (the "VPX"). Virtually every major

organization, whether inside or out of the government, is dependent upon the ability to communicate by e-mail; the Interior Department is no exception, particularly given the geographic breadth of areas under Interior's stewardship. Wholly apart from all of its other effects, the Preliminary Injunction's disconnection order would cripple the operations of the Department by stripping affected bureaus of this vital means of internal communications.

Some of Interior's telephone systems would also be disabled under the court's order. The order's disconnection provisions expressly encompass Voice Over Internet Protocol (VOIP) phone systems. For example, several MMS offices are provided with VOIP telephone services, and it is a noteworthy concern that BIA's national help desk (designed to resolve computer system problems) would be unavailable because the help desk system employs VOIP technology.

Undermining The Security Of Information Technology Systems.

Ironically, one of the consequences of the injunction would be to undermine and impede the progress the Department has already made with regard to IT security. Interior has made very significant strides in IT security in the last few years, reflecting an investment in IT security in excess of \$100 million. These efforts to enhance security measures have been undertaken in accordance with guidance provided to federal agencies by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), and against the backdrop of the Federal Information Security Management Act of 2002 (FISMA), which addresses information security in the federal sector.

Removing connectivity between computers would make it infeasible to timely and routinely obtain security software updates and patches, including anti-virus definition files and intrusion detection systems signature files. Disconnected bureaus and offices would also lose the capability to electronically report and coordinate with the Department of Homeland Security, which operates the United States Computer Emergency Readiness Team (US-CERT). Disconnection from the Internet would impede security managers and other network operations personnel in accessing the Department's website that provides IT security policy, patch updates, and a library of information relevant to system management.

Additional technical challenges would include inability to perform information systems vulnerability scans to detect and address newly identified weaknesses, inability to effectively and efficiently perform tape backups, inability to manage password changes for users and administrators, and potential degradation of IT system component performance due to environmental changes.

The mandated disconnection from the Enterprise Services Network (ESN) would remove a crucial layer of security protection for currently connected systems and data. The ESN offers multiple layers of firewalls, intrusion detection, intrusion prevention, and "24x7" security monitoring for connected bureaus' connection to the Internet and the VPX. In addition, ESN provides a proactive vulnerability discovery and management system that operates on a continuous basis.

III. THE INJUNCTION'S "5-DAY" PROVISION DOES NOT MITIGATE THE HARM THAT WOULD RESULT FROM THE INJUNCTION

As an exception to its disconnection mandate, the Preliminary Injunction permits the Department, after providing written notice to the court and Plaintiffs' counsel, to "reconnect, for specified periods not to exceed five (5) business days per month, any Information Technology Systems that Houses or provides Access to Individual Indian Trust Data, for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." Whether viewed in terms of manpower or computer resources, a month's work cannot be done in 5 days, particularly in the case of large-scale, interconnected computer systems that receive and process millions of units of data continually over the course of an entire month. The five-day provision does not alleviate the impact of the court's order.

At the outset, reconnecting disconnected computer systems is not an instantaneous process. It takes time, and if not done in an orderly manner, the process may itself damage the system's integrity and the integrity of the system's stored data. The same holds true in regard to disconnecting a connected system. Thus, some part or all of the court's 5-day window would be consumed by the reconnection and disconnection processes themselves.

Also, even once an automated Interior system that had been disconnected were to be reconnected, as envisaged under the court's order, the system could not begin immediately to process current work. Many of the systems in question, for example the MMS systems that receive electronically hundreds of millions of dollars in various revenue payments for distribution to Indians and others, would have amassed huge backlogs of unprocessed work during the lengthy period the systems were "down." Thus, before even starting to move forward, such a system would have to "catch up" on its backlog of unprocessed data, again all within the limited, 5-day window.

Moreover, many of the automated processes at issue – *e.g.*, the processing of royalties and other monies involving MMS, BIA, and OST – entail the reconciliation of information between and among different Interior components and systems. Thus, a system in one Interior component would not only have to become current on its own backlog of unprocessed data, presumably it would also have to wait for other, re-interconnected systems to get up to date as well. This is no abstract matter; information such as who owns a particular piece of land, and in what proportion, can and does change over time, often frequently, and such changes would continue to occur while automated systems that would normally process such updates were disconnected. No productive purpose would be served if a newly reconnected system were to begin its processing activities without first having recognized and accounted for changes in status that had occurred since the previous reconnection period.

Even apart from these kinds of technical difficulties, which are of major significance in themselves, repeatedly taking a large-scale computer system "up and "down" over a period of time would tend to degrade the system's information security. For example, during the time that an IT system is deprived of its connection to the Internet, it would be unable to avail itself of

many of the normal processes for maintaining and enhancing IT security. This is because many updates and "patches" are provided through the Internet and are then passed down to subordinate servers and individual computers through intranet connections. The short time frame for connection provides insufficient opportunity to bring security patches current. With interconnected systems, this would also result in increased risk to other systems with a cascading effect of potential vulnerabilities across multiple systems. For these reasons, the 5-day provision would, in itself, have an adverse effect on the Department's computer security.

None of this is in any significant respect peculiar to Interior, or even to the government. Complex, integrated computer systems that continually process massive amounts of data in real time cannot feasibly be operated on the kind of "up and down" basis contemplated by the court's order. Further, Interior's network bandwidth and load capacity of computing resources would be at risk because of the need to process a large volume of transactions occurring over a short interval.

These issues can be briefly illustrated in the case of MMS. The limited, five-day reconnection window would not enable MMS to properly distribute anywhere near the \$650 million of monthly royalty payments it receives. To begin with, the narrow reconnection window would actually only provide, at most, four days of "up" time, as at least one entire day would be required to reestablish both Internet and Intranet connections for MMS computers and then, near the end of the five day window, provide sufficient time for an orderly process to disconnect all of the affected computers and systems. More fundamentally, the applicable Minerals Revenues Management (MRM) information technology system is a large, complex, geographically dispersed, financial system incorporating a host of internal controls and security safeguards. The considerable volume of information received – 260,000 royalty transactions and 300,000 lines of production information per month – is so large that it would not be practicable for the information to be received, processed and verified within the short time available. In addition, MRM would have to coordinate its abbreviated connection period with oil, gas and mineral industry payors, MMS support contractors and with other Interior bureaus and offices that need the MRM-processed data to perform their own, inter-related missions.

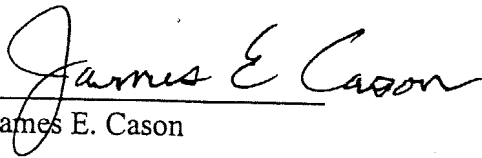
It is clear that MMS would not have the manpower options to perform a month's work in a few days, or that such manpower could actually be deployed even if theoretically available. It is equally clear that the court's five-day window of connectivity is adequate neither to accomplish substantive tasks, nor to maintain requisite MMS systems security.

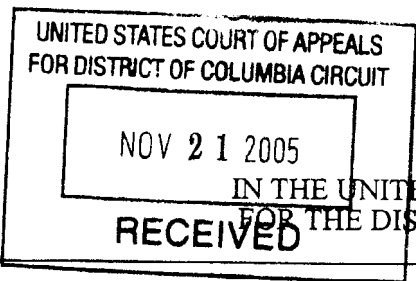
The same holds true for BIA and OST. Normally, after MRM processes royalty and production data, information is communicated to BIA and OST for the additional processing needed to identify payments to be made to Tribes and individual Indians. This step requires daily interactions between BIA and OST information technology systems to make accurate royalty, rent or bonus payments to the proper beneficiaries in a timely manner, and to ensure that funds are properly invested and interest credited to the proper accounts. Without timely exchange of information from MRM and updates from BIA, OST cannot ensure that payments are made to the proper individuals or that accounts are properly credited.

OST currently operates 12-15 hours a day, 6 days a week, to process information (more than 300 hours per month). In addition, 5-6 hours a day are required by the contractor to do end-of-day and backup processing. OST cannot undertake these tasks within the circumscribed time frame permitted in the October 20, 2005 order.

Similarly, BIA's IRMS application operates 16 hours per day, 5 days a week, processing four million transactions per month, and it normally exchanges information with the OST/TFAS system as part of its processing. It is simply not possible to transmit all the monthly land record transactions to IRMS and process that information in a five-day period. In short, like MMS, BIA and OST have neither the manpower nor the information technology capability to complete a full month's work in 5 days. As noted above, for analogous reasons, the same conclusion would hold true for other components as well.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed on October 27, 2005.


James E. Cason



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.)

No. 05-5388

[Civil Action No. 96-1285 (D.D.C.)]

**REPLY TO OPPOSITION TO MOTION FOR STAY PENDING APPEAL, AND
OPPOSITION TO MOTION TO VACATE THIS COURT'S ADMINISTRATIVE STAY**

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room, 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

EXHIBIT 2

Defendants' Opposition to Plaintiffs' Motion for Order to Show Cause
Why Interior Secretary Dirk Kempthorne and Associate Deputy Secretary
James Cason Should Not Be Held in Contempt in Their Official
Capacities under the Court's October 20, 2005 Preliminary Injunction

INTRODUCTION AND SUMMARY

The October 20, 2005 injunction requires Interior to disconnect from the internet all computers and computer systems housing or having access to individual Indian trust data, as broadly defined in the court's order. It further requires that those computers be disconnected from Interior's internal networks ("intranet"); from each other; and from third parties such as tribes and contractors. Preliminary Injunction, § IIA.¹

Plaintiffs quarrel with the precise impact of the injunction on Interior's ability to perform its functions and to serve its clients (including the plaintiff class), but, for obvious reasons, they cannot disguise the sweeping effect of the ruling. On the other side of the scale, plaintiffs demonstrate no imminent irreparable harm that would result from granting a stay. The connections at issue have been in place for years. In that time, security has continually improved, as both the district court and the Inspector General observed. Plaintiffs have not demonstrated that a single class member has ever been harmed as a result of any security weaknesses.

Plaintiffs nevertheless urge that the government "make[s] no attempt to demonstrate that the district court abused its discretion," and that its "failure to challenge that exercise of discretion establishes that [it has] no probability of success" on appeal. Stay Opposition at 11.

Plaintiffs apparently do not comprehend the government's motion. In the first section of our argument ("The Order Cannot Be Reconciled With Basic Principles Of Equity" (Stay Motion at 12)),

¹Subject to its exception for "protect[ion] against fires or other such threats to life, property, or national security," the order requires that any "Information Technology System," which is defined to include (among other things) "any computer," that houses or provides access to individual Indian trust data must "forthwith" be disconnected as follows:

1. from the Internet;
2. from all intranet connections, including but not limited to the VPX, ESN, or any other connection to any other Interior bureau or office;
3. from all other Information Technology Systems; and
4. from any contractors, Tribes, or other third parties.

we identified the principal respects in which the district court's order departed from fundamental equitable canons.

First, although the chief purpose of a preliminary injunction is to maintain the status quo, this preliminary injunction would extend internet disconnection well beyond those bureaus already subject to disconnection, and would require extraordinary bureau-to-bureau and computer-to-computer disconnections that have never been required even under the terms of any prior order in this case. Preliminary Injunction, § IIA.² Plaintiffs do not and cannot argue otherwise.

Second, a preliminary injunction may not issue unless the plaintiffs have proven “ that the [alleged] harm has occurred in the past and is likely to occur again, [or] that the harm is certain to occur in the near future.” Stay Motion at 13 (quoting Wisconsin Gas Co. v. FERC, 758 F.2d 669, 674 (D.C. Cir. 1985) (per curiam)). Plaintiffs do not and cannot show that any named plaintiff or any member of the plaintiff class has ever experienced injury, or that any individual Indian trust data has ever been manipulated, as a result of hacking into Interior systems by persons other than the IG team and the court's former Special Master.

Third, the preliminary injunction gives short shrift to the crucial principle that equity must take into account an injunction's adverse effect on third parties and on the public. See Stay Motion at 14. The computer networks subject to the district court's order are relied upon not only by Interior itself in serving the public, but also by a host of other persons and entities, including, among others, federal agencies and members of the plaintiff class. See id. at 14-15. Plaintiffs make no attempt to explain how the injunction's real and immediate impact on the public is outweighed by the wholly speculative harm to themselves.

²Although our appeal will challenge the court's order in its entirety, including its application to computers currently disconnected, our stay motion would only preserve the status quo as of the time of the October 20 injunction.

In short, quite apart from the other legal defects in the court's analysis, principles of equity require issuance of a stay pending an expedited appeal, and will ultimately compel vacation of the injunction on the merits.

ARGUMENT

I. FUNDAMENTAL PRINCIPLES OF EQUITY REQUIRE ISSUANCE OF A STAY PENDING APPEAL.

A. The Injunction Would Cause Grave, Immediate and Irreparable Harm to Interior's Services To the Public Including the Plaintiff Class.

Our stay motion demonstrated that the preliminary injunction would in large measure incapacitate a cabinet Department of the United States, especially insofar as Native American programs are concerned. Plaintiffs offer no plausible reason to disagree with this conclusion.

Plaintiffs repeatedly quote the district court's statement that "BIA [the Bureau of Indian Affairs] and OST [Office of Special Trustee] have been disconnected from the Internet for years, yet still manage to carry out their Indian-related missions. Solutions implemented to allow these bureaus to function without access to the Internet should be fairly easily adapted and exported to other bureaus and offices." Op. 204 (quoted in Stay Opposition at 17, 29 n.44). This casual and unexplained assessment is incorrect in every relevant respect.

First, as Interior has prominently noted in its quarterly reports filed with the district court, ongoing internet disconnections have significantly hampered the agency's ability to carry out its missions. See, e.g., Quarterly Report No. 21 (5/2/05), at 9-10 [Docket #2950]. The court was simply wrong to suggest otherwise.

Second, neither plaintiffs nor the district court grasp the fundamental point that disconnecting one component may affect the operations of another component. For example, the October 20, 2005 order would require the Minerals Management Service (MMS) to sever its internet connection. That disconnection would undermine the MMS's own, very significant Indian-related functions. In addition, however, key Indian-related tasks performed by the Bureau of Indian Affairs and the Office

of Special Trustee also rely on the Minerals Management Service connection. Severing the MMS connection would thus cripple BIA and OST as well. See Cason Decl. 6-7.

Third, plaintiffs and the district court entirely overlook the impact of the required intranet disconnection. Under the court's October 20 decree, BIA, OST, and other affected components, including various systems of MMS and Interior's National Business Center (NBC), are not simply cut off from the internet; they are cut off from each other and from every other office and bureau within the Department. Preliminary Injunction, § IIA. To make the calamity complete, these systems must also dismantle internally within each office and bureau. Thus, every BIA computer must be disconnected from every other BIA computer, every OST computer must be disconnected from every other OST computer, and so on. Ibid. As the Cason declaration makes plain: "Under the terms of the order, these components not only would be unable to access the Internet, but, in addition, they would be unable to communicate with each other. Perhaps even more destructive, individual computers within the same network, bureau, or office would be disconnected from every other individual computer, in effect leaving each affected computer as a stand-alone unit isolated from every other computer in the Department of the Interior." Cason Decl. 4 (emphasis added). Severance of these multiple, internal communications links as required by the court's order would in and of itself disable critical functions performed by BIA, OST, and other bureaus, separate and apart from the harm that would flow from any internet disconnections. See Cason Decl. 6.

In a similar vein, plaintiffs urge that the court's order would not hinder the processing and disbursement of royalty payments to Indians and others because Interior has continued to make such payments notwithstanding the fact that BIA and OST have been disconnected from the internet since 2001. Stay Opposition at 18. As Mr. Cason explains, "[t]he proper and timely processing of payments of royalties, rents, and bonuses to individual Indians and Tribes stemming from leasing activities is dependent, not only upon an MMS Internet connection, but also upon internal connections (intranet) between two other Interior bureaus: OST and BIA." Cason Decl. 6. "If the internal connection among NBC, OST, and BIA were disconnected, as required by the Preliminary

Injunction, it would not be possible to provide timely and accurate royalty, leasing, and bonus payments to individual Indians and Tribes. This is separate from and in addition to the dislocation that would flow from cutting off MMS access to the Internet.” Id. at 7.

Plaintiffs are likewise mistaken in claiming that delivery of social services benefits to Indians will not be interrupted as a result of the October 20 order because they have not been interrupted under the BIA internet disconnection that has been in place since 2001. Stay Opposition at 18. As Mr. Cason explains, and as plaintiffs do not dispute, the benefit programs in question rely upon a BIA computer system (the “SSAS” system) that is subject to the preliminary injunction’s intranet disconnection mandate wholly apart from any existing internet disconnection. See Cason Decl. 5. “The SSAS system, used by BIA and Tribes, contains the financial, budgetary, and statistical data used to generate checks for public assistance and maintain [each] individual’s files.” Ibid. Thus, “[a]bsent access to SSAS, which would be precluded under the court’s order, such payments would grind to a halt.” Ibid.

Plaintiffs’ cryptic remarks regarding the harm to Departmental procurement, pay and personnel activities are equally wide of the mark. Stay Opposition at 18-19. As the Cason declaration makes plain, “[i]n order to function properly, core systems such as FFS [the Federal Financial System] must have an internal (Intranet) connection within Interior to Department bureaus and offices, even apart from any Internet connection.” Cason Decl. 9. But “[t]he court’s order severs those internal links, at least with respect to those bureaus that house or have access to [IITD], including, for example, MMS, BIA, and OST.” Ibid. “The aggregate effect of destroying those links would be enormous: it would remove the Department’s basic ability to sustain the integrity of its financial management operations.” Ibid. As Mr. Cason reiterates, “[a]utomated systems such as FFS, FPPS, and IDEAS are absolutely critical to the ability of the Department to maintain the basic electronic infrastructure that allows it to perform such fundamental operations as financial management, payroll and personnel, and procurement. For Interior’s purposes, the functioning of these systems requires that they be connected not only to the Internet, but also internally to other

Interior components and systems (Intranet).” Cason Decl. 10; see also ibid. (“The disconnection of both Internet and intranet connections would, for a significant part of the Department, result in an inability to process personnel actions in a timely or effective manner.”).

The same holds true for plaintiffs’ comments regarding the preliminary injunction’s impact on e-mail and telephone service. Stay Opposition at 19. Referring to ongoing internet disconnections, plaintiffs note that “for years, the BIA, among others, has had no email capacity.” Ibid. This assertion encompasses only external, internet-based email, and overlooks the Department’s intranet-based email that has not been disturbed by previous internet disconnections. As Mr. Cason attests in his declaration, the disruption of the latter email capability imposed by the October 20 order’s internal bureau-to-bureau and computer-to-computer disconnection requirements would be crippling to the Department:

The Preliminary Injunction’s requirement that the Interior Department disconnect specified Intranet connections would also prevent employees of the affected bureaus and offices from communicating with each other by e-mail. This is because e-mail communication is dependent upon access to a mail server, and for bureau-to-bureau or bureau-to-office connections, access to the Virtual Private Exchange (the “VPX”). Virtually every major organization, whether inside or out of the government, is dependent upon the ability to communicate by e-mail; the Interior Department is no exception, particularly given the geographic breadth of areas under Interior’s stewardship. Wholly apart from all of its other effects, the Preliminary Injunction’s disconnection order would cripple the operations of the Department by stripping affected bureaus of this vital means of internal communications.

Cason Decl. 10-11 (emphases added). And, while plaintiffs seek to quibble with the precise extent of the order’s reach regarding Voice-Over-Internet-Protocol (VOIP) telephones, they do not dispute that the order covers such devices, nor do they mention much less contest that, under the order, the BIA’s national help desk “would be unavailable because the help desk system employs VOIP technology.” Cason Decl. 11.

Next, plaintiffs purport to take issue with our extensive showing that the preliminary injunction, by requiring widespread severing of Interior’s external and internal electronic communications links, would itself undermine IT security. See Cason Decl. 11; see also id. at 12-13. Plaintiffs’ sole point is that the hearing testimony, including testimony of government witnesses,

shows that a user of a stand-alone computer could, if necessary, download a “patch” from a non-Interior computer and then “upload” the update. See Stay Opposition at 19. In other words, if we understand plaintiffs correctly, an Interior employee whose computer is subject to the court’s disconnection order could download needed software from a separate computer not covered by the court’s order, save it on a diskette, and then load the software onto his work computer. See ibid. Under this scenario, the employee could not electronically transfer the software from his computer to any other Interior computer, because the court’s order would have severed such computer-to-computer links. Preliminary Injunction, § IIA. Thus, what plaintiffs appear to be proposing is that Interior employees could individually obtain diskette copies of security updates and load them on to their computers, on an ongoing, piece-by-piece and computer-by-computer basis. The fact that plaintiffs would claim with a straight face that this kind of scheme could in any setting reflect an appropriate (and secure) way to operate a massive IT portfolio is itself extraordinary. Perhaps more fundamentally, plaintiffs simply fail to address the many other aspects of computer security that would be degraded if the court’s preliminary injunction were to go into effect. See Cason Decl. 11.

Finally, plaintiffs declare that “it is illogical that accountings * * * would be impaired by the October 20 injunction,” Stay Opposition at 20, and that “[n]othing in the injunction suggests, under even the most strained reading, that it would adversely impact the accounting process.” Ibid. Plaintiffs do not reveal how they expect the agency to continue its ongoing accounting work without use of its computer networks. Nor do they directly confront Associate Deputy Secretary Cason’s assessment that “[t]he complex task of performing the accountings for IIM beneficiaries and preparing account statements simply cannot be accomplished without use of the Department’s computer systems and access to underlying data.” Cason Decl. 4.

As Mr. Cason stressed, in a part of his declaration to which plaintiffs make no reference, the October 20 order provides that computers subject to the court’s disconnection requirement must be disconnected not only from the internet and from each other, but also “from any contractors, Tribes, or other third parties.” Preliminary Injunction, § IIA. And, “OST’s access to the Trust Funds

Accounting System ('TFAS') is [an] example of third-party connectivity that would be severed by the Preliminary Injunction." Cason Decl. 4. In particular, "TFAS is the accounting and investing system that controls and enables the processing of Indian trust funds; it is hosted by SEI, a major contractor in the field of trust management and banking. The loss of access to TFAS would have a broad and devastating impact upon individual Indians and Tribes." *Ibid.* "Among other things, OST utilizes TFAS to make payments on behalf of beneficiaries to nursing homes, foster care facilities, automobile and mortgage financing institutions, hospitals, and schools. The disconnection of access to TFAS would have a crippling effect on OST's ability to make these and related kinds of payments, and also upon Interior's basic ability to prepare account statements for hundreds of thousands of Individual Indian Money (IIM) account holders and holders of other accounts." *Id.* at 5. Nothing in plaintiffs' conclusory assertions provides even the slightest basis for calling this analysis into this question.

B. A Stay Would Result In No Countervailing Harm to Plaintiffs.

Plaintiffs bear the burden of demonstrating that they have, in fact, been harmed; that recurrence of such harm is imminent; and that the harm would be irreparable.

Plaintiffs have not satisfied any of these requirements. They have not shown that a single plaintiff has ever been harmed by unauthorized hacking. Inasmuch as no plaintiff has ever experienced harm in the past, and inasmuch as Interior's security is indisputably subject to significant and continuing improvement, there is no basis for concluding that the harm that has never previously occurred is likely to occur for the first time in the near future. Finally, if hacking did occur, there is no reason to believe that its effects would be irremediable.

Plaintiffs assert that Interior's "widespread failure to implement the most basic protections, such as intrusion detection systems, audit logs and monitoring, ensures that whatever harm comes to Plaintiffs-Beneficiaries will not be detected and cannot be cured" (Stay Opposition at 24); that Interior's "IT systems lack intrusion detection systems, auditing logs, monitoring and other controls whereby unauthorized access would ever be detected" (*id.* at 25); and that "[t]he truth is that

Interior's IT security is so poor that Trustee-Delegates cannot detect or monitor unauthorized intrusions" (*id.* at 27). What these statements have in common is that none of them is supported by a record citation. In reality, Interior's systems feature a "defense in depth" (Op. 101) approach to IT security, involving multiple firewalls and routers, intrusion detection mechanisms, and security monitoring, *see, e.g.*, McWhinney, 7/20/05 PM at 37 ("[e]ach of these entities has their own series of firewalls, network intrusion detection sensors, and routers"). Even in instances where the IG's professionals were able to exploit potential weaknesses, they "noted the presence of several kinds of security controls that [were] in keeping with the 'best practices' of the IT security community," Op. 81, and system elements "that were compromised ... exhibited a number of good security practices such as up to date security patches, security monitoring software, and strong password policies that eliminate many common vulnerabilities and reduced the impact of identified vulnerabilities," Op. 89 (quoting contractor report).

Of course, the fact that a security architecture is in place does not mean that Interior's systems are impervious to penetration. The ultimate question for the agency is whether its IT security is adequate, not whether its systems are impregnable.

It does not assist plaintiffs that, in August 2005, subsequent to the close of the district court's evidentiary hearing, MMS detected four instances of unauthorized access to one of its reporting applications. *See* Stay Opposition at 26. The application in question was a "portal" site (which posts reports for industry users to view), and, as the government noted in reporting the matter to the court, "there is no reason to believe that the integrity of any data has been compromised." Docket #3147 at 1 (8/25/05). Based on its external penetration testing of MMS, Interior's IG had concluded around the same time that no significant vulnerabilities were found that allowed penetration into MMS networks or unauthorized access to information. *See ibid.*

C. Plaintiffs' Efforts To Have This Court Disregard The Cason Declaration Are Meritless.

Plaintiffs urge that the Court should disregard the showing of harm set forth in the Cason declaration, insisting that evidence of harm should have been introduced at the hearing itself and was not.

This argument is without basis. First, if plaintiffs mean to suggest that the government did not present evidence of harm at the hearing, they are entirely incorrect. Several witnesses testified that an order destroying electronic communications would make it virtually impossible for the agency to carry out essential functions. See, e.g., Brown, 6/30/05 PM at 67-74; Ekholm, 7/8/05 AM at 11-14; Smith, 7/12/05 PM at 56-57; Haycock, 7/14/05 PM at 70-74; McWhinney, 7/21/05 PM at 4-7. Moreover, the disruption caused by an internet disconnection had already been amply set out in the record even prior to this summer's IT hearing, in the government's declarations submitted to the district court in March 2004, in connection with the request for a stay of its March 15, 2004 IT injunction. See Declaration of Interior CIO W. Hord Tipton (3/22/04); Declaration of Interior Secretary Gale A. Norton (3/22/04) [Docket #2549]; see also Op. 201 ("To be sure, Interior put on evidence of the ways in which the department's operations were disrupted by this Court's last disconnection order," and "Interior has also made much of the financial functions carried out by NBC and MMS, and the effects that a loss of Internet connectivity would have on the department's ability to service its customers, many of whom are other governmental agencies.").

It should also be noted, however, that certain significant features of the injunction could not have been addressed directly at the hearing, because they emerged for the first time in the order itself. For example, the October 20 order contains extraordinarily broad definitions of IITD and "Information Technology System" that extend well beyond any previous definitions of those terms in this case. These definitions were not proposed at any time during the presentation of evidence at the hearing and appeared, for the first time, in a proposed order submitted by plaintiffs after the government's evidence had closed. See Docket #3107 (7/28/05). Similarly, the injunction provides

that under specified conditions Interior may “reconnect” disconnected computers and computer systems for up to five business days per month. That provision likewise was never proposed prior to the close of the government’s evidence. See *ibid.* Thus, these features of the injunction, and their substantial implications for Interior, could not have been the subject of the government’s hearing testimony because they came into play only after the testimony had concluded. (The district court had also made clear that there would be no post-trial submissions of proposed findings of fact or conclusions of law.)³

Plaintiffs also present the declaration of Mona Infield, a BIA employee based in Albuquerque, New Mexico who has IT-related job responsibilities. Stay Opposition at 12-13. In her declaration, Ms. Infield complains that, prior to preparing his declaration in support of a stay, Mr. Cason should have spoken with her and did not. See Infield Decl., ¶4. Mr. Cason is the Associate Deputy Secretary of the Department, with offices at headquarters in Washington, D.C. Prior to signing a litigation declaration in a short time frame, Mr. Cason cannot feasibly consult with each employee nationwide who may be involved with IT-related tasks, and is under no requirement to do so. As explained in his declaration, Mr. Cason, in fulfilling his Secretarial-level trust reform responsibilities, is involved at the Departmental level with the overall development and maintenance of Interior’s IT systems, and, in that capacity, coordinates with the Department’s Chief Information Officer (CIO) and the CIO’s for the Department’s separate bureaus and offices. See Cason Decl. 1. Accordingly, with respect to BIA’s systems, Mr. Cason consults with the BIA’s CIO, who in turn may and does rely upon the expertise of BIA staff in the field.

³Plaintiffs’ suggestion that the government cannot complain about the “5 day” provision because it was the government that suggested it borders on the absurd. See Stay Opposition at 12, 14. Plaintiffs seek to point to a provision in the agreed-upon December 17, 2001 consent order that plaintiffs portray as analogous. See *ibid.* The cited provision, however, contained no 5-day time limitation at all, and it was also issued in a context that involved internet but not intranet disconnections. See 12/17/01 Order at p.6.

In any event, Ms. Infield's attempt to call Mr. Cason's declaration into question fails on its own terms. Ms. Infield seeks to impugn Mr. Cason's statement that "even if some limited portion of essential services could be provided during the 5-day window, the apparent premise of this provision – that Interior's interconnected computer systems can be brought 'down' (disconnected) for substantial periods of time, and then brought 'up' (reconnected) for short periods, and then 'down' and 'up' over and over again, and still retain their functional capacity – misunderstands on the most fundamental level how such complex, integrated computer systems work." Cason Decl. 3. According to Ms. Infield, "it would be difficult for me to conclude that 'functional capacity' would be materially reduced by compliance with the Preliminary Injunction." Infield Decl., ¶7. Ms. Infield, however, focuses on a single, general sentence in the initial "Overview" section of the Cason declaration. Mr. Cason's statement is comprehensively explained and elaborated upon in a three-page substantive section of his declaration of which Ms. Infield makes no mention and with which she does not take issue. See Cason Decl. 12-14. As fully set forth in that section of the Cason declaration, which Ms. Infield does not dispute, "[c]omplex, integrated computer systems that continually process massive amounts of data in real time cannot feasibly be operated on the kind of 'up and down' basis contemplated by the court's order." Cason Decl. 13. Ms. Infield's suggestion that disconnecting and reconnecting large-scale, interconnected automated data processing systems is analogous to switching on and off a light bulb in one's home blinks reality. See Infield Decl., ¶8 ("the solution is as simple as turning on and off a light switch in a house").⁴

As a further part of their effort to discredit his 2005 declaration, plaintiffs also seek to attack Mr. Cason's trial testimony from 2003, in which Mr. Cason invoked the concept of "bulletproof[ing]" to describe ongoing efforts to improve aspects of Interior's IT security, and spoke

⁴In her declaration, Ms. Infield makes a number of other assertions, including assertions regarding her employment status at Interior. This stay reply is not the place to debate those statements, but we note that we by no means necessarily agree with them, and the government reserves the right to respond in the district court, as appropriate, to plaintiffs' November 8, 2005 notice calling Ms. Infield's declaration to the district court's attention.

in terms of having “driven the vulnerabilities down close to zero for our perimeter security at the Department overall.” Stay Opposition at 22. This assault on Mr. Cason’s 2003 testimony was a significant theme of plaintiffs’ 2005 hearing presentation, see, e.g., 7/18/05 PM at 45, 54-55 (Cason), but it was not accepted by the district court. Nowhere in its 205-page opinion did the district court endorse plaintiffs’ theory that Mr. Cason’s prior testimony in this case (or the government’s briefs citing that testimony) was in any material way false or misleading. As Mr. Cason took pains to emphasize with respect to the Department’s IT security in his 2003 testimony, in a portion of the transcript that plaintiffs ignore, “It’s not perfect, it will probably never be perfect, it’s better now, and the direction we’re headed at the moment is we feel pretty confident that our external perimeter security is reasonably good and that we’re starting reviews of all the internal systems to harden them further[.]” Cason, 6/4/03 AM at 38. This testimony cannot plausibly be described as even remotely false or misleading.

Indeed, as plaintiffs essentially admit, their contentions regarding Mr. Cason’s 2003 testimony ultimately center around the choice of scanning standards that are utilized to test perimeter security. See Stay Opposition at 23. Mr. Cason’s 2003 testimony was made in the context of the “SANS Top 20 List,” which is an accepted industry standard for critical vulnerabilities scanning of IT systems within the government and the private sector. See ibid.; see also Op. 58 (SANS Top 20 List includes “the ones that come from the FBI that have been identified as the most critical weaknesses throughout the IT world”) (citation omitted). In contrast, the penetration testing conducted by the Inspector General and featured at the 2005 hearing went beyond the “SANS Top 20” vulnerabilities, as part of a larger and more comprehensive program undertaken with the encouragement of Interior’s senior management to monitor and assess fuller security controls that had been placed on Interior’s IT systems, see Stay Motion at 15-16. As plaintiffs’ argument reflects, the choice of scanning regimens is inherent in the kind of security testing at issue here, and judgments about which scanning standards are appropriate for which purposes are an intrinsic element of any institution’s self-testing program.

Finally, to the extent that plaintiffs seek to call into question Mr. Cason's declaration, we note that, in its recent, November 15, 2005 decision ruling vacating the district court's re-issued accounting injunction, this Court placed prominent reliance upon two separate declarations of Mr. Cason. One of those declarations, like Mr. Cason's declaration here, was filed directly in this Court. See Cobell v. Norton, No. 05-5068 (D.C. Cir. Nov. 15, 2005), Slip op. at 3, 5, 15.

II. THE GOVERNMENT IS HIGHLY LIKELY TO PREVAIL ON APPEAL.

As we have shown, the government is highly likely to prevail on appeal because the preliminary injunction departs from basic principles of equity. The order is also vulnerable on a host of other grounds.

A. Plaintiffs Do Not Cite A Single "Finding of Fact" That Could Justify The District Court's Disconnection Order.

Plaintiffs declare that the government "do[es] not challenge the district court's findings of fact" and thus "concedes the factual findings below." Stay Opposition at 10. See also id. at 2 (arguing that "[i]n their motion to stay, Trustee-Delegates fail to even challenge the district court's findings, much less show any to be clearly erroneous").

It is unclear what plaintiffs mean by this. As emphasized in our stay motion, and as plaintiffs do not dispute, the district court's principal "finding of fact" underlying the entire preliminary injunction was that experts retained by Interior's Inspector General's Office were able in certain respects to "hack" into some of Interior's systems. The question is not whether this fact-finding is correct; the question is its significance. As noted in our stay motion, the individual who personally conducted much of the hacking in question testified at the hearing that the kind of "penetration testing" conducted by his firm on behalf of government and private clients is generally successful about 75 percent of the time. Miles, 5/18/05 PM at 62; see also Brass, 5/9/05 PM at 85 (same).

Indeed, although plaintiffs' opposition purports to stress the district court's fact-findings, Stay Opposition at 10-11, the court conspicuously made no finding that computer security standards at Interior pose significantly greater risks than security conditions at other government agencies or

in the private sector. Plaintiffs do not claim otherwise and cite no fact-finding that could, on any plausible theory, compel affirmance of the injunction.

It is unclear what if any fact-finding could ever justify an order requiring a cabinet agency to disassemble its electronic communications networks. Plaintiffs identify no such finding here, and none exists.

B. The District Court Has Improperly Arrogated To Itself The Computer Security Responsibility For A Federal Agency.

The fundamental premise of the injunction is that the court can properly weigh the significance of computer security problems and direct the expenditure of scarce resources to deal with those problems while shutting down an array of other services. As this Court explained in vacating the district court's first structural injunction, it is not for a "supervising court, rather than the agency, to work out compliance with the broad statutory mandate," a regime that would improperly "inject[] the judge into day-to-day agency management." Cobell v. Norton, 392 F.3d 461, 472 (D.C. Cir. 2004) (quoting Norton v. Southern Utah Wilderness Alliance, 124 S. Ct. 2373, 2381 (2004)). The court's error in undertaking supervision of computer security is further highlighted by this Court's November 15, 2005 decision vacating the district court's re-issued accounting injunction. Cobell v. Norton, No. 05-5068 (D.C. Cir. Nov. 15, 2005). In vacating that injunction, this Court emphasized that the district court had "erroneously displaced Interior as the actor with primary responsibility for 'work[ing] out compliance with the broad statutory mandate.'" Slip op. 10 (citation omitted). The Court further explained that the district court had failed to accord appropriate deference to the agency in making choices that "required both subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." Ibid.

The present injunction is similarly flawed. It does not conclude that Interior's computer infrastructure is less reliable than that of other agencies or private entities housing equally or more sensitive data, or that it fails to comply with any specific, substantive requirement of federal law.

Because it identifies no objective security standard that has been violated, it also cites no standard that Interior could satisfy to ensure a right to operate its computers. Preliminary Injunction, § IIE.3.

In effect, the order concludes that security should be better, and that scarce dollars should be shifted to protect IIM accounts because of the special nature of a fiduciary duty. Indeed, to a large extent, the district court's injunction is based on the court's explicitly calling into question whether the more than \$100 million that Interior has committed to IT security in recent years has been "allocated" appropriately, and on the court's related belief that it, rather than Interior, should be the ultimate arbiter of the agency's "priorities." See, e.g., Op. 189 ("Interior's relatively large financial commitment to IT security means nothing if those resources are not properly allocated."); Op. 191 ("Interior's fiduciary obligation to preserve IITD requires that IT security take a prominent position among the department's priorities."); see also Op. 182 ("To be sure, certification and accreditation is the standard with which Interior must comply to adhere to OMB's guidance for complying with FISMA. However, the Court cannot accept certification and accreditation alone as sufficient to show that Interior's IT systems are presently adequately secure to comply with Interior's fiduciary obligations as Trustee-delegate for the IIM trust."); Op. 193 (criticizing IG's "failure to place special emphasis on scrutinizing Interior's efforts to provide adequate security for IITD housed on or accessed by Interior's IT systems," which demonstrated "a serious deficiency in Interior's overall IT security program with respect to Interior's fiduciary obligations").

With considerable understatement, the court acknowledged that compliance with its order would be "difficult," and that "[p]riorities will likely have to be shuffled, resources will likely have to be redirected[.]" Op. 203. This Court's decisions, including its most recent decision of November 15, 2005, make clear that the court has no authority to reset priorities based on its own calculus and to undertake direction of a cabinet agency's computer security.⁵

⁵Plaintiffs maintain that this Court's 2004 decision vacating the March 2004 IT injunction "stressed the broad authority of the district court as a court of equity in this Indian trust case," Stay (continued...)

C. Plaintiffs Mistakenly Seek To Invoke Internal Executive Branch Policies Under Which The Decision Whether To Authorize Operation Of An IT System Would Never Be Made Without Regard To Operational Needs.

Plaintiffs seek to place reliance upon guidelines promulgated by the National Institute of Standards and Technology (NIST), arguing that those guidelines “endorse[]” the kind of relief ordered here. Stay Opposition at 15-16. As noted in the district court’s opinion, the cited NIST publications provide guidance to federal agencies regarding various aspects of information security. See generally Op. 13-37. They provide no basis for a court to order an executive Department to disconnect its computers from the internet or from each other. Indeed, plaintiffs embrace the proposition that it is “best practice” for an agency’s CIO to retain the authority to disconnect a system if warranted by security concerns. See Stay Opposition at 16 & n.19. The district court’s order openly usurps that authority.

However, even considered on its own terms, plaintiffs fundamentally misapprehend the NIST framework. Plaintiffs posit that external and internal disconnection of Interior computer systems were required because the IG had conducted successful “penetration testing” of some of those systems. But under the NIST guidelines to which plaintiffs refer, it is basic that an agency may keep a system on-line notwithstanding perceived security risks if, in the agency’s judgment, there is an “important mission-related need to place the information system into operation.” NIST SP 800-37, at 41 (cited at Op. 20). Plaintiffs’ treatment of security as an absolute imperative that trumps all other considerations thus violates not only fundamental principles of equity (and common sense), but is also at odds with the very NIST guidelines which plaintiffs purport to invoke. Under those guidelines, an agency’s determination whether to authorize operation of a system in light of inevitable security risks simply cannot be made without regard to the agency’s operational needs. See ibid.

⁵(...continued)

Opposition at 9, and in that respect is “binding” (id. at 10). This Court’s November 15, 2005 ruling leaves no doubt that plaintiffs’ view of the district court’s role in this litigation (see id. at 8-10) is overly expansive and incorrect.

Plaintiffs give short shrift to another critical aspect of the NIST framework: “likelihood of exploitation.” NIST SP 800-30 (cited at Op. 28). As NIST’s guidelines also make clear, “the notion of a ‘threat’ is not to be confused with the likelihood of exploitation, which is a separate concept[.]” Ibid. As NIST explains, a vulnerability to an IT system may exist in the abstract, without regard to the likelihood that the vulnerability may actually be exploited. Thus, “the likelihood of exploitation is a distinct step in [the] risk assessment.” Ibid. In particular, the likelihood of exploitation of a given vulnerability will be deemed low if the threat-source “lacks motivation or capability,” or if controls are in place to impede the vulnerability from being exercised. Ibid. As noted in our stay motion, the district court, in assuming responsibility for IT security and ordering the immediate, sweeping disconnection of Interior computers and computer systems, disregarded entirely the issue of the “motivation or capability” (ibid.) of potential hackers other than the IG’s retained professionals.

Plaintiffs cite hearing testimony suggesting that it is possible that a hacker “could be successful” in breaching Interior’s computer security “with time, patience, and access to a community of other hackers.” Stay Opposition at 27. Even assuming this speculation were correct in theory, it begs the question whether hackers might realistically have any interest in Interior’s systems, let alone those housing or accessing IITD. It also skips over the point that a malicious hacker seeking to break into government computer files, unlike authorized personnel retained by the IG, faces the possibility of criminal sanctions for doing so. See 18 U.S.C. § 1030; see also Brass, 5/9/05 AM at 64 (“a long stay in Leavenworth”). In the end, plaintiffs offer no evidence of any kind, and the district court cited none, that any relevant “community of hackers” (Stay Opposition at 27) would be motivated to hack in to the Interior systems at issue in this case.

Plaintiffs do not advance their argument by seizing upon the suggestion in the district court’s opinion that Interior’s computers may be subject to “hundreds of millions” of intrusion attempts. See Stay Opposition at 28 (citing Op. 195). Any computer that is connected to the internet, even a basic home computer with a standard firewall, is subject to constant scanning from outside sources,

much of which is automatically generated. The fact that a large IT portfolio such as Interior's will over time be subject to many such "pings" says absolutely nothing, one way or the other, about the underlying nature or quality of its IT security.

CONCLUSION

For the foregoing reasons, and for the reasons stated in our stay motion, the district court's October 20, 2005 preliminary injunction should be stayed pending appeal. We also reiterate our request that the Court order expedited briefing to resolve the issues presented by the district court's order at the earliest possible time.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room, 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

Robert E. Kopp

Thomas M. Bondy

NOVEMBER 2005

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of November 2005, I caused copies of the foregoing reply and opposition to be sent to the Court and to the following 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
Mark I. Levy
Kilpatrick Stockton
607 14th Street, N.W.
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


THOMAS M. BONDY

[NOT YET SCHEDULED FOR ORAL ARGUMENT]

No. 05-5388

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

ELUISE 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

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
ISAAC J. LIDSKY
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530-0001

EXHIBIT 3

Defendants' Opposition to Plaintiffs' Motion for Order to Show Cause Why
Interior Secretary Dirk Kempthorne and Associate Deputy Secretary
James Cason Should Not Be Held in Contempt in Their Official
Capacities under the Court's October 20, 2005 Preliminary Injunction

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

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

A. Parties and Amici:

The named plaintiffs-appellees in this class action are Elouise Pepion Cobell; Earl Old Person; Penny Cleghorn; Thomas Maulson; and James Louis Larose. The district court has certified a plaintiff class consisting 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.

The defendants-appellants are Gale A. Norton, as Secretary of the Interior; the Assistant Secretary of Interior-Indian Affairs; and John W. Snow, as Secretary of Treasury.

B. Rulings Under Review:

Appellants seek review of the opinion and order issued on October 20, 2005, by Judge Royce C. Lamberth, United States District Court for the District of Columbia, in Civ. No. 96-1285 (RCL). The opinion and order are published at 394 F. Supp. 2d 164.

C. Related Cases:

This Court has issued six decisions in appeals arising out of this litigation. See Cobell v. Norton, 428 F.3d 1070 (D.C. Cir. 2005); Cobell v. Norton, 392 F.3d 461 (D.C. Cir. 2004); Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004); In re Brooks, 383 F.3d 1036 (D.C. Cir. 2004); Cobell v. Norton, 334 F.3d 1128 (D.C. Cir. 2003); and Cobell v. Norton, 240 F.3d 1081 (D.C. Cir.

2001). In addition to this appeal, two other appeals are currently pending. See In re Norton, No. 03-5288 (oral argument heard October 14, 2005); Cobell v. Norton, No. 05-5269 (not yet scheduled for oral argument).



THOMAS M. BONDY
Attorney

TABLE OF CONTENTS

Page

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

GLOSSARY

| | |
|---|----|
| STATEMENT OF JURISDICTION | 1 |
| STATEMENT OF THE ISSUE | 1 |
| STATEMENT OF THE CASE | 2 |
| STATEMENT OF FACTS | 4 |
| I. General Background | 4 |
| A. This Court's Initial 2001 Decision | 5 |
| B. This Court's 2003 Contempt Decision | 6 |
| C. This Court's 2004 Structural Injunction Decision | 7 |
| D. Reissuance of the Structural Injunction | 8 |
| E. Mandamus Petitions Seeking Disqualification Of Special Master Balaran | 9 |
| F. Pending Appeal From The Order Of July 12, 2005. | 10 |
| II. Computer Disconnection Orders Prior to 2005 | 11 |
| A. The 2001 Temporary Restraining Order | 11 |
| B. The 2003 and 2004 Disconnection Orders | 12 |
| III. The October 20, 2005 Disconnection Order | 13 |
| A. Statutory Provisions Governing Information Security. | 13 |
| B. District Court Proceedings | 14 |

| | | |
|----|---|----|
| 1. | Testing by the Inspector General | 14 |
| 2. | The Order and Injunction | 15 |
| | SUMMARY OF ARGUMENT | 19 |
| | STANDARD OF REVIEW | 23 |
| | ARGUMENT | 24 |
| I. | The District Court Improperly Set Aside The Information Safety Plan Developed Under The Comprehensive FISMA Scheme And Wrongly Assumed Authority For Directing Agency Security | 24 |
| A. | The FISMA Establishes A Highly Discretionary Comprehensive Scheme Of Cost-Effective Risk Assessment | 24 |
| B. | Governmentwide Experience Under The FISMA Underscores The Difficulty And Complexity Of The Security Problems Faced By Agencies And OMB. | 29 |
| C. | The Record Provides No Basis For Continuing Judicial Intervention In Computer Security ... | 32 |
| 1. | A Court Should Properly Defer To Decisions Taken As Part Of The FISMA Scheme | 32 |
| 2. | No Basis Exists For Setting Aside Executive Branch Security Decisions And Substituting Judicial Controls | 34 |
| a. | The Record Demonstrates Unstinting Commitment To The FISMA Process And Substantial Progress In IT Security | 34 |
| b. | The Problems Cited By The District Court Provide No Basis For Judicial Intervention | 36 |

| | | |
|-----|--|----|
| 3. | No Evidence Exists Of Past Or Imminent Threats To Accountholder Security That Would Warrant Judicial Intervention | 39 |
| 4. | The District Court's Belief That IITD Should Be "Segregated" Reflects a Fundamental Misunderstanding Of Computer Systems And Limitations Of Judicial Expertise | 41 |
| D. | In Assuming Control Of Interior Computer Systems, The District Court Replicated The Errors Underlying Its Previous Structural Injunctions | 44 |
| II. | The Injunction Cannot Be Reconciled With Basic Principles of Equity | 49 |
| A. | The Injunction Is In No Meaningful Way "Preliminary." | 49 |
| B. | An Injunction Must Take Into Account The Public Interest And Be Tailored To Limit Its Adverse Impact On The Defendant | 50 |
| C. | Plaintiffs Have Failed To Demonstrate That An Injunction Is Needed To Avoid Likely Irreparable Harm | 58 |
| | CONCLUSION | 61 |
| | CERTIFICATE OF COMPLIANCE WITH RULE 32(a)(7)(c) OF THE FEDERAL RULES OF APPELLATE PROCEDURE | |
| | CERTIFICATE OF SERVICE | |
| | STATUTORY ADDENDUM | |

TABLE OF AUTHORITIES

| Cases: | <u>Page</u> |
|---|-----------------------|
| <u>In re Barr Laboratories, Inc.</u> , 930 F.2d 72 (D.C. Cir. 1991) | 33 |
| <u>In re Brooks</u> , 383 F.3d 1036 (D.C. Cir. 2004) | 9 |
| <u>Central & Southern Motor Freight Tariff Ass'n v. United States</u> , 757 F.2d 301 (D.C. Cir. 1985) | 33 |
| <u>Cobell v. Babbitt</u> , 91 F. Supp. 2d 1 (D.D.C. 1999) | 5 |
| <u>Cobell v. Norton</u> , 226 F. Supp. 2d 1 (D.D.C. 2002) | 6 |
| <u>Cobell v. Norton</u> , 226 F. Supp. 2d 163 (D.D.C. 2002) | 6 |
| <u>Cobell v. Norton</u> , 274 F. Supp. 2d 111 (D.D.C. 2003) | 3, 12 |
| <u>Cobell v. Norton</u> , 283 F. Supp. 2d 66 (D.D.C. 2003) | 7 |
| <u>Cobell v. Norton</u> , 310 F. Supp. 2d 98 (D.D.C. 2004) | 3, 12 |
| <u>Cobell v. Norton</u> , 357 F. Supp. 2d 298 (D.D.C. 2005) | 8 |
| <u>Cobell v. Norton</u> , 229 F.R.D. 5 (D.D.C. 2005) | 10 |
| <u>Cobell v. Norton</u> , 394 F. Supp. 2d 164 (D.D.C. 2005) | <u>passim</u> |
| <u>Cobell v. Norton</u> , 240 F.3d 1081 (D.C. Cir. 2001) | 5, 59 |
| <u>Cobell v. Norton</u> , 334 F.3d 1128 (D.C. Cir. 2003) | 6 |
| <u>Cobell v. Norton</u> , 391 F.3d 251 (D.C. Cir. 2004) | 3, 12, 59 |
| * <u>Cobell v. Norton</u> , 392 F.3d 461 (D.C. Cir. 2004) | 8,22,33,46,47 |
| * <u>Cobell v. Norton</u> , 428 F.3d 1070 (D.C. Cir. 2005) | 7,8,20,23,33 44,47 |

* Authorities chiefly relied upon are marked with an asterisk.

| | |
|---|--------------|
| <u>Heckler v. Chaney</u> , 470 U.S. 821 (1985) | 33 |
| <u>Koon v. United States</u> , 518 U.S. 81 (1996) | 24 |
| * <u>Norton v. Southern Utah Wilderness Alliance</u> , 542 U.S. 55 (2004) | 8, 9, 33, 47 |
| <u>Steel Manufacturers Ass'n v. EPA</u> , 27 F.3d 642 (D.C. Cir. 1994) | 33 |
| <u>Udall v. D.C. Transit System, Inc.</u> , 404 F.2d 1358 (D.C. Cir. 1968) | 50 |
| <u>University of Texas v. Camenisch</u> , 451 U.S. 390 (1981) | 50 |
| <u>Washington Metropolitan Area Transit Comm'n v. Holiday Tours, Inc.</u> , 559 F.2d 841 (D.C. Cir. 1977) | 50 |
| <u>Weinberger v. Romero-Barcelo</u> , 456 U.S. 305 (1982) | 50 |
| <u>Wisconsin Gas Co. v. FERC</u> , 758 F.2d 669 (D.C. Cir. 1985) .. | 58 |

Statutes:

| | |
|--|--------|
| American Indian Trust Fund Management Reform Act, Pub. L. No. 103-412, 108 Stat. 4239 | 4 |
| Pub. L. No. 108-108 | 7 |
| 117 Stat. 1263 | 8 |
| 5 U.S.C. App.3 | 25 |
| 5 U.S.C. § 706(1) | 5 |
| 18 U.S.C. § 1030 | 40 |
| 28 U.S.C. § 1292(a) | 1 |
| 28 U.S.C. § 1331 | 1 |
| 28 U.S.C. § 1361 | 1 |
| 44 U.S.C. § 3541(1) | 13 |
| * 44 U.S.C. § 3543 | 27 |
| 44 U.S.C. § 3543(a) | 14, 27 |
| 44 U.S.C. § 3543(a)(5) | 14, 25 |

| | |
|------------------------------|------------|
| * 44 U.S.C. § 3544 | 27 |
| 44 U.S.C. § 3544 (a) (1) (A) | 13, 24, 28 |
| 44 U.S.C. § 3544 (a) (1) (C) | 13, 24 |
| 44 U.S.C. § 3544 (a) (2) | 24 |
| 44 U.S.C. § 3544 (a) (2) (B) | 25 |
| 44 U.S.C. § 3544 (b) (2) (A) | 13, 25 |
| 44 U.S.C. § 3544 (b) (2) (B) | 13, 25 |
| 44 U.S.C. § 3544 (b) (8) | 29 |
| 44 U.S.C. § 3544 (c) | 25 |
| 44 U.S.C. § 3544 (c) (1) | 14 |
| * 44 U.S.C. § 3545 | 14, 25 |
| 44 U.S.C. § 3545 (a) (1) | 14, 25 |
| 44 U.S.C. § 3545 (b) (1) | 13, 25 |

Miscellaneous:

| | |
|---|----------------|
| 2004 Subcommittee Scorecard, http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%20%20years.pdf . | 29 |
| <u>40 Million Cards May Be Affected By Breach</u> , Washington Post, 6/19/05, at A21 | 31 |
| Associated Press, <u>Computer Breach at U. of Connecticut</u> , N.Y. Times, 6/25/05, at C13 | 31 |
| <u>Hacker Accesses USC Files</u> , L.A. Times, 7/9/05, at B3 | 31 |
| Identity Theft Resource Center, http://www.idtheftcenter.org/breaches.pdf | 31 |
| Information Technology, DOD FY 2004 Implementation of FISMA, http://www.dodig.osd.mil/Audit/reports/FY05/05-025.pdf . | 30-31 |
| NIST Special Publication 800-30 | 27 |
| NIST Special Publication 800-37 | 26 |
| OMB Circular A-130, App. III | 25, 26, 28, 56 |
| Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, http://www.privacyrights.org/ar/ChronDataBreaches.htm | 31 |
| Restatement (Second) of Trusts (1959) | 46 |

GLOSSARY

| | |
|--------------|--|
| 1994 Act | American Indian Trust Fund Management Reform Act |
| APA | Administrative Procedure Act |
| BIA | Bureau of Indian Affairs |
| CIO | Chief Information Officer |
| FISMA | Federal Information Security Management Act |
| GAO | Government Accountability Office |
| IG | Inspector General |
| IIM Accounts | Individual Indian Money Accounts |
| IITD | Individual Indian Trust Data |
| IT | Information Technology |
| MMS | Minerals Management Service |
| NBC | National Business Center |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| OST | Office of Special Trustee |

[NOT YET SCHEDULED FOR ORAL ARGUMENT]

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

No. 05-5388

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. The order on appeal was issued on October 20, 2005, and styled as a preliminary injunction. 394 F. Supp. 2d 164. The government filed a timely notice of appeal on October 21, 2005. This Court has jurisdiction pursuant to 28 U.S.C. § 1292(a).

STATEMENT OF THE ISSUE

Whether this Court should vacate an injunction that requires components of the Department of the Interior to disconnect their computers from the internet and from internal computer networks, and that precludes some previously disconnected components from reestablishing internet access.

STATEMENT OF THE CASE

This is an appeal from an injunction that requires the Department of the Interior to immediately sever internet connections for major computer systems now on-line and precludes reconnection of other systems already disconnected. The injunction further requires that all these systems dismantle their internal communications capacities, so that computers within a particular Interior component cannot communicate with each other or with other Interior components.

The order issued on October 20, 2005, nine years after this class action was filed in 1996, seeking relief including an accounting of funds in Individual Indian Money ("IIM") accounts. As described below, this Court has, to date, issued six published opinions in this case. Oral argument in a seventh appeal was heard in October 2005. Briefing in an eighth appeal will be completed on January 20, 2006.

The district court issued its first order with respect to computer disconnection in December 2001. Although no evidence suggested that any class member had been injured by computer tampering, the district court issued a temporary restraining order requiring Interior to immediately disconnect from the internet all computers that might provide access to Individual Indian Trust Data ("IITD"). Because such data is contained in many computer systems and because computer systems are interconnected, the TRO required broad, agencywide disconnections.

To regain internet access, Interior agreed to a consent order which set out a procedure for restoring internet connections upon agreement by the court's Special Master. Order of 12/17/01. With the Master's approval, Interior reconnected a number of major systems to the internet. However, by the time the regime established by the consent order concluded in 2003, several significant Interior components remained off-line.

In July 2003, the district court entered a preliminary injunction by which the court, rather than the Special Master, assumed full authority over internet access. Cobell v. Norton, 274 F. Supp. 2d 111 (D.D.C. 2003). In March 2004, the district court issued a superseding preliminary injunction requiring Interior immediately to disconnect its computer systems from the internet, with limited exceptions. Cobell v. Norton, 310 F. Supp. 2d 98 (D.D.C. 2004).

This Court stayed and later vacated the injunction. Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004). Noting that "there was no evidence that anyone other than the Special Master's contractor had 'hacked' into any Interior computer system housing or accessing IITD," id. at 259, this Court remanded for further proceedings, id. at 262.

In 2005, plaintiffs again moved for an injunction, following which the district court conducted a 59-day evidentiary hearing on the security of Interior's information systems. On October 20, 2005, the district court issued a "preliminary injunction" requiring Interior "forthwith" to disconnect all computer systems

that provide access to Individual Indian Trust Data, defined broadly so that, as the court noted, "IITD is suffused in varying forms and amounts throughout Interior's network environment." Cobell v. Norton, 394 F. Supp. 2d 164, 271, 277-78 (D.D.C. 2005). This Court granted an administrative stay on October 21, 2005, and a stay pending appeal on December 9, 2005.

STATEMENT OF FACTS

Because the computer disconnection order cannot be fully understood without regard to the litigation as a whole, we first briefly describe, in Section I, the prior decisions relating to accounting duties and the conduct of the case generally. In Section II, we describe prior computer disconnection orders. In Section III, we discuss the framework for government computer security oversight enacted in 2002 as the Federal Information Security Management Act ("FISMA") and the order now on appeal.

I. General Background.

The Department of the Interior administers roughly 260,000 Individual Indian Money trust accounts with balances totaling approximately \$400 million. In 1994, Congress enacted the American Indian Trust Fund Management Reform Act, Pub. L. No. 103-412, 108 Stat. 4239, which requires the Secretary of the Interior to "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" a 1938 statute addressing investment of trust monies. In 1996, a class of present and former IIM

accountholders filed this lawsuit, claiming among other things that the government had failed to provide a timely, adequate accounting.

A. This Court's Initial 2001 Decision.

In 1999, the district court issued a declaratory judgment holding that Interior has an enforceable duty to account for the balances in the IIM accounts. Cobell v. Babbitt, 91 F. Supp. 2d 1, 28-31, 56 (D.D.C. 1999). This Court's 2001 decision largely affirmed the declaratory judgment, concluding that the agency had unreasonably delayed performance of accounting activities within the meaning of 5 U.S.C. § 706(1). Cobell v. Norton, 240 F.3d 1081, 1108 (D.C. Cir. 2001).

Although this Court noted that adequate computer systems would be needed to accomplish the required accounting, 240 F.3d at 1106, neither the district court's order nor this Court's decision addressed potential problems that might be generated by computer hackers. To the extent that computer systems were at issue, the concern posed was the need for improved systems to compile and process trust data. See id. at 1092 (noting problems and new computer systems outlined in Interior's 1998 plan of operations). Even in this regard, this Court emphasized the discretion to be afforded the agency in implementing computer systems and other tasks, noting that the "actual legal breach is the failure to provide an accounting, not its failure to take the discrete individual steps that would facilitate an accounting,"

id. at 1106, and admonishing the district court "to be mindful of the limits of its jurisdiction," id. at 1110.

B. This Court's 2003 Contempt Decision.

The remand to the agency envisioned by this Court's decision was short-lived. By the end of 2001, following receipt of reports from Special Master-Monitor Joseph Kieffer, the district court had initiated contempt proceedings charging that Interior had failed to initiate an historical accounting and had included inaccurate statements in its quarterly reports to the court.

The district court ultimately held the Secretary and an Assistant Secretary of the Interior in contempt, declaring that "Secretary Norton and Assistant Secretary McCaleb can now rightfully take their place ... in the pantheon of unfit trustee-delegates." Cobell v. Norton, 226 F. Supp. 2d 1, 161 (D.D.C. 2002). The court announced that, henceforth, it would direct the conduct of the accounting as well as virtually all other trust activities. The court thus ordered the parties to submit accounting plans, as well as plans for achieving compliance with the government's fiduciary obligations to Indians, to be evaluated by the court with a view to issuance of structural relief. Id. at 148-49. In an accompanying ruling, the district court denied the government's motion seeking Mr. Kieffer's removal. Cobell v. Norton, 226 F. Supp. 2d 163 (D.D.C. 2002).

In Cobell v. Norton, 334 F.3d 1128 (D.C. Cir. 2003), this Court vacated the contempt citations because the record demonstrated that "in her first six months in office Secretary

Norton took significant steps toward completing an accounting," id. at 1148, and because the district court's reasoning with respect to the other charges was "mystifying," id. at 1149, and "inconceivable," id. at 1150.

The Court also vacated the appointment of Special Master-Monitor Kieffer, whose reports had prompted the contempt proceedings, id. at 1135, explaining that the district court had improperly "charged [Mr. Kieffer] with an investigative, quasi-inquisitorial, quasi-prosecutorial role that is unknown to our adversarial legal system." Id. at 1142.

C. This Court's 2004 Structural Injunction Decision.

The contempt trial had formed the predicate for the district court's assumption of authority and its justification for issuing structural relief. However, this Court's decision vacating the contempt ruling did not cause the district court to reconsider its action. See Cobell v. Norton, 428 F.3d 1070, 1076-77 (D.C. Cir. 2005) (discussing the district court's failure to reconsider the basis for structural relief).

The structural injunction that issued in September 2003, Cobell v. Norton, 283 F. Supp. 2d 66 (D.D.C. 2003), set aside Interior's plan for an historical accounting and established detailed new requirements that caused "the cost of complying with the injunction to rise by more than an order of magnitude, from \$335 million over five years to more than \$10 billion." 428 F.3d at 1077. In response, Congress, as part of the FY 2004 Interior appropriation, Pub. L. No. 108-108, amended applicable law,

effective until December 31, 2004, to provide that no provision of law required the performance of an historical accounting. See 117 Stat. 1263. This Court vacated the accounting provisions of the structural injunction on the basis of this legislation. Cobell v. Norton, 392 F.3d 461 (D.C. Cir. 2004).

This Court also vacated the provisions of the structural injunction establishing judicial oversight over trust management generally (with the exception of a single reporting requirement). This Court rejected the district court's premise that judicial intervention of this type was permissible because IIM accountholders are trust beneficiaries. This Court made clear that defendants' fiduciary status did not vitiate the normal structure of judicial review of agency action, id. at 471-78, stressing that the APA "'empowers a court only to compel an agency ... to take action upon a matter, without directing how it shall act.'" Id. at 475 (quoting Norton v. Southern Utah Wilderness Alliance, 542 U.S. 55, 64 (2004)).

D. Reissuance of the Structural Injunction.

In February 2005, after the appropriations provision governing historical accounting activities had expired, the district court reissued the accounting portion of the original structural injunction without modification. Cobell v. Norton, 357 F. Supp. 2d 298 (D.D.C. 2005).

This Court stayed the injunction and, in November 2005, vacated the injunction in its entirety, Cobell v. Norton, 428 F.3d 1070 (D.C. Cir. 2005), concluding that "reissuance of the

injunction was not properly grounded in either fact or law." Id. at 1076.

This Court explained that the district court "owed substantial deference to Interior's plan" for historical accounting activities, ibid., and emphasized that "[t]he choices at issue required both subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." Ibid. The district court, however, had improperly "invoked the common law of trusts and quite bluntly treated the character of the accounting as its domain." Ibid. It had "thus erroneously displaced Interior as the actor with primary responsibility for 'work[ing] out compliance with the broad statutory mandate.'" Ibid. (quoting Southern Utah, 542 U.S. at 66-67).

E. Mandamus Petitions Seeking Disqualification Of Special Master Balaran.

This Court has also considered two mandamus petitions regarding Special Master Alan Balaran. In 2004, the Court ordered Mr. Balaran recused from contempt proceedings involving 37 current and former Interior and Justice Department officials. In re Brooks, 383 F.3d 1036, 1044-46 (D.C. Cir. 2004). In 2003, for separate reasons, the government sought Mr. Balaran's recusal from all future proceedings. See No. 03-5288. In April 2004, three days before this Court was scheduled to hear oral argument on the government's mandamus petition, Mr. Balaran submitted his resignation. After further briefing, this Court heard oral argument on October 14, 2005.

F. Pending Appeal From The Order Of July 12, 2005.

On July 12, 2005, the district court issued an order requiring Interior to state in all written communications with class members, without regard to subject matter, that any information regarding trust assets may be unreliable. Cobell v. Norton, 229 F.R.D. 5 (D.D.C. 2005). The July 12 opinion, which had no nexus to any evidentiary proceeding, engaged in an extended diatribe against current Interior officials and employees, decrying the present Interior Department as a "dinosaur - the morally and culturally oblivious hand-me-down of a disgracefully racist and imperialist government that should have been buried a century ago, the last pathetic outpost of the indifference and anglocentrism we thought we had left behind." Id. at 7. It accused the Department of "vindictiveness" and "dishonesty," id. at 9, "Machiavellian guile," id. at 10, and "Byzantine maneuvering," id. at 11, all of which form part of a "degenerate tenure as Trustee-Delegate for the Indian trust," which has featured "scandals, deception, dirty tricks and outright villainy - the end of which is nowhere in sight," id. at 11. This Court stayed the July 12 order, and briefing in that appeal is scheduled to be completed on January 20, 2006. See No. 05-5269. Those briefs also address the government's request that the case be assigned to a different district court judge.

II. Computer Disconnection Orders Prior to 2005.

A. The 2001 Temporary Restraining Order.

In November 2001, at approximately the same time that the contempt proceedings were initiated, Special Master Balaran issued a report identifying flaws in Interior's computer security that the Master believed could detrimentally affect the integrity of Individual Indian Trust Data. See 394 F. Supp. 2d at 166. Although no evidence existed that any person other than the Special Master had ever hacked into Interior's systems, the court entered a temporary restraining order requiring Interior to immediately disconnect from the internet all information systems housing or providing access to IITD. Ibid. Because IITD is present on many computer systems, and because computer systems are interconnected, the order required disconnection of a host of systems, including those of the Bureau of Indian Affairs and the Office of Special Trustee, the two Interior bureaus most significantly involved with administering Indian trust matters.

To regain internet access, Interior agreed to a consent order by which it assented to a procedure for restoring internet connections. Id. at 166-67. The consent order provided that offices would be restored to the internet upon agreement by the Master that the systems were secure or that they neither housed nor provided access to IITD. Id. at 167. Ultimately, most systems taken off-line were restored. Ibid. However, by the time the Special Master regime concluded in 2003, several Interior components, including the Bureau of Indian Affairs and

the Office of Special Trustee, were still barred from internet connection.

B. The 2003 and 2004 Disconnection Orders.

In July 2003, the district court entered a preliminary injunction by which the court, rather than the Special Master, assumed full authority over internet access. Cobell v. Norton, 274 F. Supp. 2d 111 (D.D.C. 2003). The order made no provision for further reconnections as contemplated by the earlier consent agreement and, instead, required Interior to immediately disconnect from the internet the systems already approved by the Special Master. The court stayed the effect of its order with respect to systems that were not already off-line, to allow Interior to submit certifications showing that the systems still connected to the internet were secure from internet access by unauthorized users. Id. at 135-36.

In March 2004, without considering the government's evidence, the district court issued a preliminary injunction that superseded the 2003 injunction and required Interior immediately to disconnect all information systems from the internet, with limited exceptions. Cobell v. Norton, 310 F. Supp. 2d 98 (D.D.C. 2004).

This Court first stayed and, in December 2004, vacated the injunction. Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004). Noting that "there was no evidence that anyone other than the Special Master's contractor had 'hacked' into any Interior

computer system housing or accessing IITD," id. at 259, this Court remanded for further proceedings, id. at 262.

III. The October 20, 2005 Disconnection Order.

A. Statutory Provisions Governing Information Security.

In 2002, Congress enacted the Federal Information Security Management Act ("FISMA"), which establishes a "comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations." 44 U.S.C. § 3541(1).

1. The FISMA makes the head of each agency responsible for "providing information security protections" that are "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction." 44 U.S.C. § 3544(a)(1)(A). These protections must be "integrated with agency strategic and operational planning processes." Id. § 3544(a)(1)(C). Each agency must "develop, document, and implement an agencywide information security program," which must include policies and procedures aimed at "cost-effectively reduc[ing] information security risks to an acceptable level" on the basis of mandated risk assessments. Id. § 3544(b)(2)(A), (B).

2. The FISMA requires an "independent evaluation of the information security program and practices of that agency," 44 U.S.C. § 3545(a)(1), which is generally performed by the agency's Inspector General ("IG"), id. § 3545(b)(1). The IG's independent evaluation includes a testing of effectiveness, and an assessment

of compliance with statutory requirements and related security policies. Id. § 3545(a)(1).

3. The FISMA vests the Office of Management and Budget ("OMB") with ultimate responsibility to "oversee agency information security policies and practices." 44 U.S.C. § 3543(a). OMB is empowered to "approv[e] or disapprov[e], agency information security programs," id. § 3543(a)(5), and the agencies and Inspector Generals are required to report to OMB at least annually, id. §§ 3544(c)(1), 3545.

B. District Court Proceedings.

1. Testing by the Inspector General.

In 2003, Interior officials contacted Interior's IG, offering to fund independent "penetration testing" of the Department's computer systems. 394 F. Supp. 2d at 202. The testing entailed the IG's retention of a team of expert security consultants to conduct a variety of simulated attacks by "hackers." Id. at 199. The IG testified that this offer allowed him "to jump start that program that I was trying desperately to find funds" to implement. Id. at 202 (quoting Devaney, 5/20/05 AM at 37).

That both Interior and the IG believed that penetration testing would provide a useful diagnostic tool reflected the extent to which progress had already been made. Prior to that time, "Interior's IT security program had simply not advanced far enough for penetration testing to be a useful evaluation tool." Id. at 200.

In April 2005, after the IG's office had started its penetration testing, Interior provided the district court with the IG's "Notice of Potential Findings and Recommendation with Respect to Information Technology Systems," which included the results of a recent penetration test. 394 F. Supp. 2d at 169. Plaintiffs immediately sought a temporary restraining order and preliminary injunction requiring disconnection of Interior's computers. Ibid.

The hearing on this motion grew into a 59-day trial. Among other witnesses, personnel from the IG's office and its contractors testified regarding their concerns with Interior's security as well as the progress that the agency had made.

2. The Order and Injunction.

The district court once more issued an injunction requiring disconnection of a broad array of Interior computers and computer systems from the internet. 394 F. Supp. 2d 164. In contrast to its previous orders, however, this injunction also required that Interior sever internal connections from other Department computers, networks, or electronic devices. Id. at 276-78. Thus, some systems, such as those of the Minerals Management Service, which are currently connected to the internet, would lose both external and internal connections. Other systems, such as those of the Bureau of Indian Affairs and the Office of Special Trustee, which are already denied internet access, would be precluded from reconnection, and would also have to sever

electronic communications internally and to all other Interior components.

a. The court did not find that anyone other than the IG (and, earlier, the Special Master) had ever hacked into any relevant computer system or that any IIM accountholder had ever been injured because of a problem with Interior's computer security. It did not find that computer security at Interior was significantly different than at other government agencies. Nor did it find that Interior had failed to make progress or to commit energy and resources to enhancing computer security. To the contrary, the court observed that "[t]here can be no doubt that Interior has made substantial progress in implementing a comprehensive departmental IT security program in a very short time," 394 F. Supp. 2d at 249, and recognized that "Interior's progress in a period of five years is laudable," *id.* at 272. As the court also noted, Interior had invested over \$100 million in IT security in a three-year period. *Id.* at 267-68.

The court noted continuing problems, however, and stressed in particular that Interior's information safety plan should be structured to give the highest priority to Individual Indian Trust Data. Thus, despite the "substantial progress that has been made," the court concluded that judicial intervention was warranted because "the evidence indicates that Interior has not properly emphasized IITD in its IT security efforts." *Id.* at 272.

b. The injunction requires that Interior "forthwith" disconnect affected computers:

1. from the Internet;
2. from all intranet connections ... or any other connection to any other Interior bureau or office;
3. from all other Information Technology Systems; and
4. from any contractors, Tribes, or other third parties.

Id. at 277-78.

The computers subject to this disconnection are described in a series of sweeping definitions. The order requires disconnection of "all Information Technology Systems that House or provide Access to Individual Indian Trust Data." Id. at 277.

An "Information Technology System" is defined to include "[a]ny computer, server, equipment, device, network, intranet, enclave, or application, or any subsystem thereof" used by Interior in any number of ways, "including without limitation computers, wireless devices (e.g. Blackberrys) and networks," as well as any "ancillary equipment, devices, or similar services or protocols." Id. at 276-77.

"Individual Indian Trust Data" is not limited to records of IIM account balances, withdrawals, and deposits. Instead, it encompasses all "[i]nformation ... that evidences, embodies, refers to, or relates to – directly or indirectly and generally or specifically – a Federal Record that reflects the existence of Individual Indian Trust Assets," provided that this information was used or produced in some way related to the administration of

the trust or in Interior's relationship with individual Indian trust beneficiaries. Id. at 277 (emphasis added).

In turn, "Federal Record" includes all federal documentary materials in any physical form whatsoever that are preserved, or are appropriate for preservation, because of their informational content. Ibid.

"Individual Indian Trust Assets" include all lands, natural resources, monies, and other assets held in trust for individual Indians by the federal government. Ibid.

The district court fully understood the breadth of the resulting injunctive provisions. As it observed, "IITD in one form or another permeates Interior's IT environment fairly completely," id. at 258; see also id. at 271 ("The evidence shows that IITD is suffused in varying forms and amounts throughout Interior's network environment.").

The injunction exempts from its scope only those systems "necessary for protection against fires or other such threats to life, property, or national security." Id. at 278.

The order purports to mitigate its impact by allowing Interior to reconnect computer systems for up to five business days per month "for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." Ibid. Before it may do so, Interior must provide five days advance notice to the court and to the plaintiffs, together with a plan for interim "security controls and measures to cover such reconnection." Id. at 279.

The order will continue indefinitely unless and until Interior persuades the court to authorize connection of one or more systems. Interior may urge such reconnections in proposals that include "a uniform standard to be used to evaluate the security of all Information Technology Systems which House or provide Access to Individual Indian Trust Data[.]" Ibid.

Each proposal will then become the subject of additional adversary litigation. The plaintiffs are authorized to take discovery regarding the proposal, following which the district court "will conduct any necessary evidentiary hearing and decide whether a proposed Information Technology System may be reconnected and order further relief, as appropriate." Ibid.

c. On October 21, 2005, this Court granted the government's motion for an administrative stay. On December 9, 2005, the Court issued a stay pending appeal and granted the government's motion for expedition.

SUMMARY OF ARGUMENT

The district court has required a Cabinet department to disassemble much of its electronic communications network, severing links to the public and other federal agencies, and dismantling bureau-to-bureau and computer-to-computer connections with respect to affected components. Although the purpose of the injunction is different, its effect is the same as an act of computer sabotage designed to bring a government agency to its knees. The 59-day trial established no legal or factual basis

for any order of relief. Separately, the injunction fails both as a matter of law and if judged solely by principles of equity.

I. The Federal Information Security Management Act, enacted in 2002, establishes a comprehensive framework for addressing computer security that directs agency officials to evaluate risks, prioritize their concerns, and develop cost-effective solutions to the most pressing problems. It does not establish substantive standards of security, and does not suggest (much less require) that sweeping computer disconnections may be an appropriate means for achieving security improvements.

A court undertaking review of decisions made under the FISMA scheme should recognize that "[t]he choices at issue required both subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." 428 F.3d at 1076. The need for deference is underscored by a statutory structure that explicitly requires responsible officials to balance costs and risks and develop priorities on an agencywide basis. The comprehensive review mechanisms including independent Inspector General assessments and OMB oversight provide additional reasons to defer to Executive Branch choices. Indeed, a court that addresses an agency security plan reviews no single decision but a program of multiple, interrelated technical strategies that reflect a series of risk and cost assessments.

The 59-day trial provided no basis for rejecting Executive Branch security decisions in favor of judicial controls.

As the district court acknowledged, Interior has invested over \$100 million in IT security in three years, and has made real and substantial progress in implementing an IT security program. In so doing, Interior has made every effort to implement the FISMA process as Congress intended. The IG's "penetration testing" that formed the focus of the trial was undertaken at Interior's invitation and made possible by its funding.

As might reasonably have been expected, the testing revealed weaknesses as well as strengths. However, the IG's evidence and the record as a whole make clear that the problems faced by Interior are not different in severity or kind than those facing federal agencies in general. More important, the record demonstrates both commitment to information security and significant actual progress, and does not suggest that any judicial action is required to ensure that the Executive Branch mechanisms function as Congress contemplated.

The district court nevertheless frankly declared that it could reorder agency priorities because Interior has a fiduciary relationship with IIM accountholders. That error replicates the mistaken premise of previous structural injunctions, and this Court has explicitly held that the court may not substitute its judgment for that of the agency by invoking the status of accountholders as trust beneficiaries. Moreover, the court's belief that the agency should shift priorities by "segregating" its Indian trust data reflects its pervasive misunderstanding of

complex computer systems and underscores why courts defer to Executive Branch judgments in this area.

The court thus erred in believing that any basis existed for setting aside the agency's information security program or undertaking further judicial intervention. The court did not, however, merely purport to set aside Interior's program. Instead, as in its previous structural injunctions, the district court disregarded this Court's declaration that a court is empowered only to compel an agency "'take action upon a matter, without directing how it shall act,'" 392 F.3d at 475, and that it should not interject itself "into day-to-day agency management," id. at 472. The court thus mandated its own security program, which includes widespread, crippling disconnections that would remain in effect until the government persuaded the court in further adversarial proceedings that the court should, in its discretion, permit reconnections. The record provides no legal or factual basis for any relief, much less the injunction issued by the court.

II. Apart from these errors, however, it would be necessary to vacate the injunction even it were judged solely by standards of equity: the injunction would result in immediate and crushing harm to the public interest and is not required to prevent imminent, irreparable harm to plaintiffs.

The order requires both external and internal computer disconnections. Some major systems, such as those of the Minerals Management Service, must sever their internet

connections. Other components, such as the Bureau of Indian Affairs and the Office of Special trustee, are precluded from reconnecting. All affected components must sever their connections with each other and with the rest of the Department, and must also disassemble their own internal, computer-to-computer communications. The precise impact of the order is discussed below, but the general devastation of government services that would result should not require elaboration. The court's suggestion that the impact of the injunction would be mitigated by allowing reconnections for five days each month betrays a deep misunderstanding of the operation of these systems and is without a foothold in common sense.

That the court would issue such an order is even more extraordinary because plaintiffs have made no showing that the injunction is required to avoid any imminent harm, much less significant or irreparable harm. The record is barren of even a single instance in which an IIM accountholder has been harmed by the activities of an unauthorized hacker. Plaintiffs do not satisfy the threshold requirement for any equitable relief, much less the relief ordered by the court.

STANDARD OF REVIEW

Legal conclusions underlying an injunction are reviewed de novo. Cobell, 428 F.3d at 1074. Although the decision to enter an injunction is reviewed for abuse of discretion, ibid., 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 Improperly Set Aside The Information Safety Plan Developed Under The Comprehensive FISMA Scheme And Wrongly Assumed Authority For Directing Agency Security.

A. The FISMA Establishes A Highly Discretionary Comprehensive Scheme Of Cost-Effective Risk Assessment.

1. The Federal Information Security Management Act establishes a comprehensive scheme for promoting and monitoring computer security throughout the federal government. The statute creates procedures rather than substantive mandates. At every point, it stresses that agencies must evaluate security concerns in an integrated manner, and must weigh costs and risks.

Each agency is thus responsible for providing information security protections "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction." 44 U.S.C.

§ 3544(a)(1)(A). These protections must be implemented through security processes that are "integrated with agency strategic and operational planning processes." Id. § 3544(a)(1)(C). The statute emphasizes that agencies should assess "the risk and magnitude of the harm that could result" from potential security problems, and implement "policies and procedures to cost-effectively reduce risks to an acceptable level[.]" Id. § 3544(a)(2). Similarly, the statute provides that the agency

information security program should include policies and procedures aimed at "cost-effectively reduc[ing] information security risks to an acceptable level" on the basis of the required risk assessments. Id. § 3544(b)(2)(A), (B).

Although the FISMA vests primary responsibility in responsible agency officials, it also requires an "independent evaluation of the information security program and practices of that agency," 44 U.S.C. § 3545(a)(1), and specifies that this annual audit should, when possible, be performed by the agency's Inspector General, id. § 3545(b)(1). Like the agency's own assessments, the IG's evaluations are provided to congressional oversight committees. Id. §§ 3544(c), 3545. These provisions reflect the IG's general statutory function as a largely independent office within an executive agency charged with investigating agency operations in order to assist Congress and the agency by recommending means of improving economy and efficiency. 5 U.S.C. App.3 § 4(a)(1)&(3).

The FISMA provides not only for an independent IG role and congressional oversight, but also for ultimate review authority in the Executive Branch by OMB. Both the agency and the IG must report to OMB at least annually, 44 U.S.C. §§ 3544(c), 3545, and OMB has final authority to "approv[e]" or "disapprov[e]" information security plans, id. § 3543(a)(5).

2. The FISMA procedures incorporate guidance issued by OMB and by the National Institute of Standards and Technology ("NIST"). See 44 U.S.C. § 3544(a)(2)(B). Like provisions of the

statute, this guidance is procedural and does not purport to establish substantive criteria. OMB's security policies are premised on the core concept of "adequate security," which OMB has defined to mean "security commensurate with the risk and magnitude of the [potential] harm." OMB Circular A-130, App. III, § A(2)(a). "This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act[,] "id. § B; see 394 F. Supp. 2d at 171.

NIST standards establish a process by which risks should be assessed and managed, including a "certification," which is defined as "a comprehensive assessment of the management, operational, and technical security controls in an information system[.]" NIST Special Publication 800-37 at 1; see 394 F. Supp. 2d at 172. On the basis of this information, a designated agency official must make a decision whether an information system warrants "accreditation." The purpose of the NIST certification and accreditation process is to assure responsible risk assessment and accountability. Thus, an agency's accreditation decision is "the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls." NIST SP 800-37 at 1.

NIST guidance explains that, for purposes of information security management, an agency's risk assessment should reflect

the nature of the information the agency holds; the harms that could result from possible security breaches; and the likelihood that particular kinds of breaches might occur. "Risk is a function of the likelihood of a given threat-source's exercising a potential vulnerability, and the resulting impact of that adverse event on the organization." NIST Special Publication 800-30 at 8 (discussed at 394 F. Supp. 2d at 179-82).

3. This statutory and regulatory structure reflects the fundamental realities of information security. Because the effectiveness of computers and computer systems depends on their ability to communicate with each other, security concerns must be evaluated and addressed on an agencywide, and ultimately on a governmentwide, basis. See 44 U.S.C. §§ 3543, 3544. Because all security is relative, and because resources are finite, that evaluation depends on a series of risk determinations and judgments as to how best to allocate limited funds. And because the security decisions of each agency are of concern to the government as a whole, agency heads do not have final authority to approve security plans. That responsibility is placed in OMB, which coordinates security efforts governmentwide. See 44 U.S.C. § 3543.

Neither the FISMA, nor any guidance from NIST or OMB, dictates that computers should be disconnected when potential security threats are discovered. Nor do these provisions suggest that wholesale dismantling of computer communications would ever be appropriate. In applying FISMA standards, decisionmakers

would undertake such action only after weighing the costs to the public and the government that would result from such disruption.

Perhaps unsurprisingly, Dr. Ron Ross, a NIST scientist and principal author of relevant NIST standards, testified that, in his seven years at NIST, those standards have never led to the denial of approval to operate a computer system due to security concerns. Dr. Ross was asked, "[n]ow, in your experience there at the FISMA implementation team, generally how often in the federal government is a system denied the authority to operate?" Ross, 7/5/05 AM at 40. When Dr. Ross declared that "I've never seen any in my experience," the district court interjected, "[n]o matter how the risk assessment went, you've never seen anything ever shut off?" Ibid. Dr. Ross informed the court that this was, indeed, correct. Id. at 40-41.

Similarly, OMB guidance addresses the issue of service interruption only as a threat to security. See OMB Circular A-130, App. III, § B(a)(2)(e) ("When automated support is not available, many of the functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service."). OMB guidance specifically stresses that "[m]anual procedures are generally not a viable backup option." Ibid. OMB's concern is reflected in the FISMA itself, which does not require disconnections but rather requires that an agency's information security program include "plans and procedures to ensure

continuity of operations for information systems that support the operations and assets of the agency." 44 U.S.C. § 3544(b)(8).

B. Governmentwide Experience Under The FISMA Underscores The Difficulty And Complexity Of The Security Problems Faced By Agencies And OMB.

Since the enactment of FISMA, a subcommittee of the House Committee on Government Reform has given each executive agency an annual computer security grade based on its overall progress regarding the FISMA's security management requirements. In 2003, eight cabinet departments received an "F" on this congressional report card, including the Departments of the Interior, Justice, State, Homeland Security, Energy, Health and Human Services, Housing and Urban Development, and Agriculture. Docket #2418. Five of these eight agencies again received an "F" grade in 2004, with Interior obtaining a C+, Justice a B-, and State a D+. Docket #2933 at 7 n.11; 2004 Subcommittee Scorecard, available at <http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%202%20years.pdf>. (Two additional agencies, Commerce and the Veterans Administration, fell from a "C" to an "F" from 2003 to 2004, see *ibid.*)

In its 2004 scorecard, the Committee on Government Reform thus rated Interior higher than several cabinet agencies, including Homeland Security. As the examples of Commerce and the VA indicate, an agency's "grade" may fall as well as rise. The point is not Interior's relative rating in a given year. Rather, the significance of this scoring process is to highlight the

difficulties faced by agencies government-wide. Indeed, in a July 2005 report issued by the Government Accountability Office ("GAO"), the Comptroller General found that "[p]ervasive weaknesses exist in almost all areas of information security controls at 24 major agencies, threatening the integrity, confidentiality, and availability of information and information systems." PX581 at 2. "As a result," the Comptroller General continued, "federal operations and assets are at increased risk of fraud, misuse, and destruction. In addition, these weaknesses place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption." Ibid.

To take one example, the Department of Defense ("DOD"), which houses systems at least as critical as Interior's, is in no way immune from these government-wide problems. In its July 2005 analysis, the GAO listed DOD, along with 13 other agencies, including Interior, as having weaknesses in each of five basic IT security areas. PX581 at 9. A 2004 report by DOD's Inspector General reflects the same types of concerns voiced by other IG's (including Interior's Inspector General); the report concluded that "[t]he DOD warfighting capability and the security of its information infrastructure are at great risk from attacks by foreign intelligence organizations, cyber terrorists, and the incompetence of some of its own users." Information Technology, DOD FY2004 Implementation of FISMA for IT Training and Awareness

(12/17/04), at 21, available at <http://www.dodig.osd.mil/Audit/reports/FY05/05-025.pdf>.

The private sector, of course, faces the same challenges and has been repeatedly victimized by major hacking incidents. See Smith, 7/13/05 AM at 37. Indeed, even as the 59-day hearing in this case was underway, the national media reported major computer security breaches at financial institutions and universities across the country, including one incident in which a hacker accessed 40 million credit card numbers.¹

None of this criticism suggests that the government is in any respect neglecting IT security, or that it has failed to make substantial progress. To the contrary, as the GAO declared, "[o]verall, the government is making progress in its implementation of the provisions of FISMA." PX581 at 2. The point is simply that computer security poses enormous and novel challenges. OMB, the Inspector Generals, the GAO and congressional oversight committees foster improvements by studying vulnerabilities and evaluating responses on an ongoing

¹ See 40 Million Cards May Be Affected By Breach, Washington Post, 6/19/05, at A21; see also, e.g., Associated Press, Computer Breach at U. of Connecticut, N.Y. Times, 6/25/05, at C13 (computer hacker gained access to the names, birth dates, and SSNs of 72,000 university students and employees); Hacker Accesses USC Files, L.A. Times, 7/9/05, at B3 (hacker accessed personal information regarding 270,000 current and former applicants to University of Southern California). For listings of IT hacking incidents in 2005, see, e.g., Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>; Identity Theft Resource Center, <http://www.idtheftcenter.org/breaches.pdf>.

basis. As a result, GAO observed, “[t]he government is progressing in its implementation of the information security management requirements of FISMA,” but it is equally clear that “challenges remain.” Id. at 14.

C. The Record Provides No Basis For Continuing Judicial Intervention In Computer Security.

1. A Court Should Properly Defer To Decisions Taken As Part Of The FISMA Scheme.

As the previous discussion indicates, in responding to everchanging threats to information security, the Executive Branch must employ both technical expertise and institutional judgment to prioritize risks and utilize limited resources in a cost-effective manner. The FISMA, as well as NIST and OMB guidance, stress these points repeatedly. For good reasons, they do not establish substantive security criteria, instead requiring accountable officials to evaluate and expressly accept risks. Ultimately, moreover, any single agency’s security program reflects not only that agency’s judgment, but the overall FISMA review process, which provides for independent evaluations to be submitted to congressional oversight committees and also to OMB, which is empowered to approve or disapprove agency security programs.

The judicial review principles stressed by this Court in its November 2005 decision vacating the re-issued accounting injunction apply with at least equal force to a review of information security arrangements subject to FISMA. It is incontrovertible that “[t]he choices at issue required both

subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." 428 F.3d at 1076 (citing Heckler v. Chaney, 470 U.S. 821 (1985), and Steel Manufacturers Ass'n v. EPA, 27 F.3d 642 (D.C. Cir. 1994)). The need for deference is underscored by the statutory procedures for ongoing evaluation within the Executive Branch and by the terms of a statute explicitly vesting in Executive officials the responsibility for discretionary decisions based on risk and cost assessments. See In re Barr Laboratories, Inc., 930 F.2d 72, 76 (D.C. Cir. 1991) ("we have no basis for reordering agency priorities. The agency is in a unique - and authoritative - position to view its projects as a whole, estimate the prospects for each, and allocate its resources in the optimal way"); Central & Southern Motor Freight Tariff Ass'n v. United States, 757 F.2d 301, 321-22 (D.C. Cir. 1985) ("[d]eference is particularly appropriate when" agency discretion "necessarily involves the administrative weighing of the costs and benefits").

As this Court has made clear, it is not for a "supervising court, rather than the agency, to work out compliance with the broad statutory mandate," a regime that would improperly "inject[] the judge into day-to-day agency management." 392 F.3d at 472 (quoting Southern Utah, 542 U.S. at 66-67); see also ibid. (warning against "'judicial entanglement in abstract policy disagreements which courts lack both expertise and information to resolve'").

2. **No Basis Exists For Setting Aside Executive Branch Security Decisions And Substituting Judicial Controls.**
 - a. **The Record Demonstrates Unstinting Commitment To The FISMA Process And Substantial Progress In IT Security.**

The record provides no basis for setting aside Executive Branch security decisions and substituting judicial controls.

The record leaves no doubt as to the agency's commitment to improvement or as to its actual progress. As the district court noted, Interior has invested over \$100 million in IT security in a three-year period. 394 F. Supp. 2d at 267-68. The court was obliged to acknowledge that "[t]here can be no doubt that Interior has made substantial progress in implementing a comprehensive departmental IT security program in a very short time," *id.* at 249, and it even observed that "Interior's progress in a period of five years is laudable," *id.* at 272. See also, e.g., *id.* at 274 ("Interior is currently devoting substantial time and resources to IT security").

The district court's praise underscores Interior's recent accomplishments in improving the security of trust-related information. Testimony at trial established, for example, that the IG's hacking contractor was unsuccessful in its attempts to penetrate the computer systems of MMS, which every month receives, processes, and disburses hundreds of millions of dollars in royalty and lease payments. *Id.* at 213-14. Similarly, with respect to the IG's efforts to hack into the BIA's systems from a simulated internet connection, the

contractor's report remarked: "If this environment were accessible from the Internet, it would be an extremely small footprint for such a large organization." Id. at 210. And even in instances where the IG's professionals were able to exploit potential weaknesses in Interior's computer security, they "noted the presence of several kinds of security controls that [were] in keeping with the 'best practices' of the IT security community," id. at 209, and system elements "that were compromised ... exhibited a number of good security practices such as up to date security patches, security monitoring software, and strong password policies that eliminate many common vulnerabilities and reduced the impact of identified vulnerabilities," id. at 213 (quoting contractor report); see also id. at 219 (same).

Interior's progress reflects an unstinting commitment to making the FISMA process effective. The IG's penetration testing that gave rise to plaintiffs' request for an injunction was undertaken at Interior's direct invitation and was made possible by Interior's offer to fund that testing in order to advance its security efforts. As the IG testified, he was contacted in 2003 by James Cason, the Associate Deputy Secretary of the Interior, who "said that he'd like to have some independent [IT security] testing done" sometime in "the late fall of 2003." 394 F. Supp. 2d at 201-02 (quoting Devaney, 5/20/05 AM at 35-36). Mr. Cason explained "that he was at a point where he wanted to begin to see if the systems would withstand penetration, and asked me if I would be willing to be the independent tester if they gave us

some money to do that to hire a contractor." Id. at 202 (quoting Devaney, 5/20/05 AM at 36). Prior to that time, "Interior's IT security program had simply not advanced far enough for penetration testing to be a useful evaluation tool." Id. at 200.

The IG testified that Interior's initiative was vital to his ability to undertake penetration testing. Interior's offer, the IG declared, allowed him "to jump start that program that I was trying desperately to find funds" to implement. Id. at 202 (quoting Devaney, 5/20/05 AM at 37). Interior's offer was memorialized in a Memorandum of Understanding with the IG by which Interior agreed to fund the penetration testing. PX1; see also 394 F. Supp. 2d at 185-86 (noting IG's testimony that Secretary Norton had never exercised her authority to lower the IG budget). As Interior's Chief Information Officer ("CIO") emphasized in his testimony, the essential purpose of the penetration testing, which, as noted, the Department itself initiated, was to expose potential vulnerabilities thereby enabling their remediation. See Tipton, 7/26/05 PM at 76, 87-88.

**b. The Problems Cited By The District Court
Provide No Basis For Judicial Intervention.**

The evidence at trial thus suggested neither a lack of progress nor a failure to commit to progress. The precise strengths and weaknesses of Interior's evolving security program may be debated, but the trial evidence provided no basis for concluding that judicial action of any kind is necessary to

ensure that the FISMA process operates in the manner that Congress intended.

The IG's penetration testing, undertaken at Interior's behest, forms part of an internal and ongoing Executive Branch process and provides no ground for judicial involvement. The IG noted that Congress had recently given Interior a C+ computer security grade, "I think recognizing the progress that has been made." However, "this penetration testing in my mind has taken that grade back to F." Devaney, 5/20/05 PM at 59. As the IG testified, it is not his role to assign a grade, id. at 60, and he acknowledged that neither he nor his staff was prepared to offer any opinion on the security of Interior's computer networks generally, see Devaney, 5/20/05 AM at 85-89, or of its trust data in particular, see id. at 88. Indeed, the IG specifically cautioned against drawing conclusions about Interior's information security from the penetration testing results. Devaney, 5/20/05 AM at 87; accord Miles, 5/18/05 PM at 100 (testimony of IG's hacking contractor noting that penetration testing did not permit meaningful appraisal of Interior's overall security posture).² In any event, as discussed above, the

² Asked whether he could offer the court any representations concerning the security of trust-related data on Interior's computer networks, Inspector General Devaney testified:

I think the only representation I can make is the snapshots that we took here. We came in at a given time and penetrated the system in a certain way. If we were to come back the day after, or if we had done it
(continued...)

relative grades accorded by congressional oversight committees are significant chiefly because they reveal the magnitude of the problems presented government-wide, and preclude any inference that problems faced at Interior result from a lack of commitment or unique difficulties in developing effective responses.

Indeed, the testimony made clear that vulnerabilities found at Interior were not in any sense unusual among government agencies. To the contrary, Roger Mahach, a member of the IG's staff, testified that "I don't think any government program, whether it's at the Department of Interior, the EPA, or the Food and Drug Administration or Homeland Security can withstand this type of scrutiny." Mahach, 6/10/05 PM at 80.

Similarly, an employee of the firm retained by the IG to hack into Interior's computers testified that it is commonplace for testing of this kind to result in successful penetration. Scott Miles, who personally conducted much of the hacking in question, estimated that the kind of penetration testing conducted by his firm on behalf of government and private clients is generally successful about 75 percent of the time. Miles, 5/18/05 PM at 62; see Brass, 5/09/05 PM at 85 (same).

²(...continued)

the day before, we might not have gotten in. We might have through a more - we might have tried to get in and been rebuffed. The fact that we got into two of these bureaus and were able to do what we did gives me great concern, but I can't say that tomorrow, if penetration testing was done, that we would be successful.

Devaney, 5/20/05 AM at 87.

Although the district court referred broadly to "fundamental systemic problems inherent in the structure of Interior's IT environment," 394 F. Supp. 2d at 271, it did not conclude that the problems faced by Interior were different in kind or scope than those at other agencies. Many of the issues that the court found troubling involved perceived bureaucratic shortcomings of the type endemic to all large organizations. See, e.g., id. at 194 (failure to place copies of risk-assessment documentation in all field offices); id. at 196-97 (inadequate "plan of action and milestone" (POA&M) documentation); id. at 197 (failure to update POA&M documentation in a timely fashion).

More fundamentally, when an agency is fully cooperating in the FISMA scheme and is making substantial progress, no apparent basis exists for a court to intrude into the operations of the statutory scheme. Nor, in these circumstances, is it at all apparent what relief a court could order consistent with the statute's emphasis on cost-effective risk assessment by agency officials, with independent evaluation by the IG, close congressional oversight, and ultimate review authority vested in OMB.

3. No Evidence Exists Of Past Or Imminent Threats To Accountholder Security That Would Warrant Judicial Intervention.

As the previous discussion indicates, protection of IITD cannot be considered in isolation from the agencywide security program. Even if a legal basis existed for questioning the precise protections accorded to IITD within that program (and

even assuming that such an inquiry were feasible), the record provides no basis whatsoever for inferring that IITD is at any imminent risk of corruption. Indeed, no evidence exists of even one instance of unauthorized computer tampering with the IIM account of any member of the plaintiff class.

When IG auditor Diann Sandy (praised by the court for telling the "unvarnished truth," 394 F. Supp. 2d at 186 n.11) was asked whether "in the 20-plus years that you've been an auditor with the IG's office," she had "ever heard of an instan[ce] in which someone manipulated data within Interior's systems and arranged to have an Individual Indian Trust beneficiary's payment sent to someone other than the intended Trust beneficiary," she testified "[n]ot to my knowledge." Sandy, 6/6/05 PM at 83.

Moreover, as the trial testimony underscored, the ability of retained security experts to gain access to a computer system does not indicate that other individuals, lacking similar expertise and immunity from criminal prosecution, see 18 U.S.C. § 1030, would easily enjoy similar success. As noted by Mr. Mahach, an IG employee with substantial involvement in the penetration testing of Interior, "[t]he success of the Office of Inspector General's penetration testing is not ... due to trivial weaknesses that allow for easy, automated exploitation by unskilled hackers. Commonly used and readily available automated tools used by [unskilled hackers] would not find the type of weaknesses we have been able to exploit." PX41. Similarly, authorized hackers can focus their efforts on gaining entry

without investing comparable time and resources to ensuring that their efforts will not be traced. Nor did the evidence explain why unauthorized hackers would be motivated to risk potentially severe criminal sanctions to tamper with IIM accounts, see, e.g., Brass, 5/09/05 AM at 64 (noting that malicious hackers seeking to break into government computer files face "a long stay in Leavenworth").

4. The District Court's Belief That IITD Should Be "Segregated" Reflects a Fundamental Misunderstanding Of Computer Systems And Limitations Of Judicial Expertise.

Although the injunction does not specify how the district court would exercise its ongoing control of Interior's computers, its decision suggests that "the most immediate, commonsense step to securi[ng] electronic trust data" would be the segregation of IITD onto systems isolated from Interior's general network. 394 F. Supp. 2d at 261; see also id. at 258, 271. During the 59-day hearing, the district court repeatedly interrupted the testimony to ask witnesses why, in their view, Interior had failed to undertake the complete segregation of trust data. See, e.g., Tr. 5/12/05 PM at 34-35 (Mahach); Tr. 6/30/05 PM at 70-71 (Brown).³

³ Typical was this interjection during plaintiffs' direct examination of Roger Mahach:

THE COURT: I can't help interrupting. I'm burning with one question that I have never understood.... Why after all the problems in 2001 with the trust records and this Court's concerns, why has the trust record never been separated out from the other systems so we didn't have to put the whole department at risk and we could have just had the trust records on one
(continued...)

And in its opinion accompanying the injunction, the district court expressed disapproval over what it perceived as "Interior's continuing inability to ... segregat[e] IITD on secure servers separate from Interior's accessible IT networks and systems." 394 F. Supp. 2d at 261.

The district court's focus on "segregation" as the appropriate security strategy for IITD is symptomatic of the flaws in its analysis and underscores why judges do not properly assume administrative authority for safeguarding the government's computer networks. The court's evident belief that Interior "could have just had the trust records on one system," Tr. 5/12/05 PM at 34-35, is at odds with the court's own recognition that IITD "permeates Interior's IT environment fairly completely." 394 F. Supp. 2d at 258. Nothing in the record suggests that Interior could identify, aggregate, and organize into a single isolated system all of its electronic information that "evidences, embodies, refers to, or relates to – directly or indirectly and generally or specifically – a Federal Record that reflects the existence of Individual Indian Trust Assets," id. at 277 (injunction's definition of Individual Indian Trust Data).

As one government witness testified, a true "segregation" program would arguably require the wholesale duplication of major

³(...continued)
system? [I]t's been four years. Why hasn't that been done?

Tr. 5/12/05 PM at 34-35.

Interior computer networks, and of the human and capital resources necessary to operate those networks. See Brown, 6/30/05 PM at 70-71, 76-77. Even then, the witness noted, segregation might not appreciably improve the security of trust data, because duplication of existing networks would merely duplicate many existing vulnerabilities. Ibid. Moreover, even if such an undertaking were thought desirable, the costs would be prohibitive. As the district court itself acknowledged, one of the reasons Interior has not pursued a strategy of complete segregation is "because the resources that such an effort would require are simply not available." 394 F. Supp. 2d at 258; see Cason, 7/18/05 PM at 75-77 (noting resource constraints).

The problems inherent in judicial second-guessing of complex security decisions are evident throughout the court's opinion. For example, the court disagreed with the agency's choice of spending priorities, noting that while Interior had sponsored the testing of its network security, it had not given the same weight to security testing of agency employees and third-party contractors, thus wrongly failing to make such testing "a priority within the departmental IT security program." 394 F. Supp. 2d at 256. This is precisely the type of judgment that an agency must be allowed to make, and judicial intervention would be inappropriate even if the record demonstrated actual problems with IITD security due to employees and contractors. In fact, the court cited no such evidence.

Similarly, the court criticized Interior at length because it believed that the language of contracts with third-party contractors did not mandate adequate testing of the contractors' systems. See id. at 256-57. In this manner, the court not only undertook to second-guess security judgments as to what testing might be required, but also assumed authority to judge the level of explicit detail to be included in Interior's contractual arrangements. The impropriety of such judicial micromanagement is further underscored by the absence of citation to evidence that any contractor system has, in fact, placed any data - much less IITD - at an unacceptable risk of corruption or loss.

In short, the court's analysis highlights its failure to appreciate that Interior's discretion in implementing the FISMA process requires "both subject-matter expertise and judgment about the allocation of scarce resources." 428 F.3d at 1076.

D. In Assuming Control Of Interior Computer Systems, The District Court Replicated The Errors Underlying Its Previous Structural Injunctions.

As we have shown, neither the governing statutory and regulatory scheme nor the record at trial provides any basis for setting aside any aspect of Interior's information security program. Accordingly, the matter of information security is properly remanded to the Executive Branch to be addressed by Interior, its Inspector General's Office, and OMB, which are responsible to Congress for the effective operation of the FISMA scheme.

The court would thus have erred even if it had simply remanded with instructions to alter one or more security priorities. The full extent of the court's improper arrogation of Executive Branch responsibilities is thrown into relief by its decision to appoint itself the arbiter of future compliance with unidentified standards, and, for an indefinite period, to require massive disconnections as an alternative agency security program. In so doing, the court not only departed from this Court's directive to accord substantial deference to complex agency judgments, but also departed from other crucial strictures emphasized by this Court in reversing previous structural injunctions.

1. The district court wrongly believed that it was licensed to undertake control of information security programs because of the fiduciary relationship between Interior and IIM accountholders. The court emphasized that judicial intervention was appropriate notwithstanding "the substantial progress that has been made," because, in the court's view, "Interior has not properly emphasized IITD in its IT security efforts." 394 F. Supp. 2d at 272. The court explained that because IIM accountholders are trust beneficiaries, the FISMA scheme could not be considered controlling. The court declared that "[t]o be sure, certification and accreditation is the standard with which Interior must comply to adhere to OMB's guidance for complying with FISMA." Id. at 264. But "the Court cannot accept certification and accreditation alone as sufficient to show that

Interior's IT systems are presently adequately secure to comply with Interior's fiduciary obligations as Trustee-delegate for the IIM trust." Ibid. On this basis, the court explained that it was appropriate to order a restructuring of security efforts even though "[p]riorities will likely have to be shuffled, resources will likely have to be redirected[.]" Id. at 275.

As this Court made clear in vacating the first structural injunction, the trust relationship between the government and IIM accountholders does not vitiate normal limits on judicial review. This Court explained that a judicial takeover of agency responsibilities is not only inconsistent with general principles of judicial review, 392 F.3d at 471-78, but is without foundation in general principles of fiduciary law. This Court noted that "private trustees, even though held to high fiduciary standards, are generally free of direct judicial control over their methods of implementing these duties, and trustee choices of methods are reviewable only 'to prevent an abuse by the trustee of his discretion.'" 392 F.3d at 473 (citing Restatement (Second) of Trusts §§ 186-87).⁴ Moreover, as this Court observed, in private trusts, the costs of trust administration are met from the trust itself, 392 F.3d at 473, and decisions necessarily incorporate a cost-benefit analysis.

⁴ Thus, as Professor Langbein explained earlier in this litigation, under common law principles, a court would be reluctant to interfere with the manner in which a trustee seeks to implement its duties, particularly when the trustee must determine how best to use limited funds. See Langbein, 6/3/03 PM at 74-76, 78-79; Langbein, 6/3/03 AM at 33-34, 39, 67-68.

Thus, in vacating the re-issued accounting injunction, this Court explicitly held that the district court had erred when it "invoked the common law of trusts and quite bluntly treated the character of the accounting as its domain." 428 F.3d at 1076. In so doing, the court had "erroneously displaced Interior as the actor with primary responsibility for 'work[ing] out compliance with the broad statutory mandate.'" Ibid. (quoting Southern Utah, 542 U.S. at 66-67).

2. As in its previous structural injunctions, the district court disregarded this Court's admonition that a court is empowered only to compel an agency "'take action upon a matter, without directing how it shall act,'" 392 F.3d at 475 (citation omitted), and improperly established an ongoing regime that will "inject[] the judge into day-to-day agency management," id. at 472. The court in effect installed its own version of an information security program, one that requires wholesale computer disconnections. Future changes to that program will be made at the court's sole discretion following extended adversary proceedings in which Interior will carry the burden of persuasion. 394 F. Supp. 2d at 279. The injunction is flatly at odds with this Court's warning against "'judicial entanglement in abstract policy disagreements which courts lack both expertise and information to resolve,'" and against "'pervasive oversight by federal courts over the manner and pace of agency compliance with [broad] congressional directives,'" 392 F.3d at 472 (quoting Southern Utah, 542 U.S. at 64).

Of course, the district court's order did not rest on a purported failure to comply with any particular congressional directive. To the contrary, it is the court's alternative security regime that cannot be reconciled with the statute. As discussed above, the FISMA itself neither mandates agency computer disconnections nor suggests any circumstance in which sweeping disconnections are appropriate. Evidence at trial indicated that no federal agency had ever been denied authority to operate a computer system under the FISMA and NIST standards. Ross, 7/5/05 AM at 40. If the Executive Branch, in the course of fulfilling its FISMA responsibilities, were to contemplate the option of wholesale computer disconnections, it would be required to weigh the magnitude and likelihood of the harm to be avoided against the costs in terms of money and degradation of its ability to serve the public. It is difficult to posit what extraordinary circumstance might cause the Executive Branch to engage in widespread, indefinite, external and internal computer disconnections. Nothing in the FISMA could plausibly be construed to mandate such disconnections here.

More fundamentally, a statute that requires responsible Executive Branch officials to evaluate and accept risks is incompatible with judicial revision of security priorities. The extended trial provided no basis for such intervention, and the provisions of the injunction further depart from principles repeatedly emphasized by this Court.

II. The Injunction Cannot Be Reconciled With Basic Principles of Equity.

As we have shown, the injunction is based on fundamental error and cannot be sustained. However, even if the order were reviewed solely in terms of guiding principles of equity, reversal would be required.

The district court has required a Cabinet department to disassemble much of its electronic communications network, both with respect to the public and other federal agencies, and with respect to its own, internal communications. The extraordinary history of this litigation perhaps obscures the utterly remarkable nature of such a ruling. If a court required the Social Security Administration to sever its internet links with the public, the outcry would be immediate. Likewise, it is scarcely conceivable that a court would preclude the Secretary of State or the Secretary of Homeland Security from communicating electronically within large segments of their own agencies. An order inflicting this type of damage on the Department of the Interior is no more supportable.

A. The Injunction Is In No Meaningful Way "Preliminary."

As an initial matter, although the district court styled its order a "preliminary" injunction, the appellation is plainly a misnomer. The injunction is not "preliminary" to any pending "merits" dispute. The injunction establishes an alternative information security plan that will remain in effect until Interior carries a burden of persuading the court, in further

adversary proceedings, that individual computer systems should be reconnected. An injunction that remains in effect indefinitely and shifts the burden of persuasion to the nonmoving party does not remotely resemble a true preliminary injunction, the purpose of which is "merely to preserve the relative positions of the parties until a trial on the merits can be held." University of Texas v. Camenisch, 451 U.S. 390, 395 (1981); see Washington Metropolitan Area Transit Comm'n v. Holiday Tours, Inc., 559 F.2d 841, 844 (D.C. Cir. 1977).

B. An Injunction Must Take Into Account The Public Interest And Be Tailored To Limit Its Adverse Impact On The Defendant.

Apart from the absence of legal authority, a fundamental reason that courts do not cripple the communications of Executive Branch agencies is the bedrock principle that a court must consider the public interest in fashioning equitable relief. As this Court has long made clear, injunctive relief must "eventuate from a careful consideration of all important factors of relevance, not the least of which is the public interest." Udall v. D.C. Transit System, Inc., 404 F.2d 1358, 1360 (D.C. Cir. 1968) (per curiam); see Weinberger v. Romero-Barcelo, 456 U.S. 305, 312-13 (1982).

It is difficult to posit any circumstance in which the public interest could be harmonized with an order destroying significant parts of a cabinet agency's internal communications structure as well as its ability to communicate with the public that it serves. The district court made no serious attempt to

explain how the harms resulting from its order are compatible with the public interest.

To list the specific harms flowing from the injunction is to understate its impact. The Court can readily apprehend the effect of an order requiring the federal judiciary to dismantle its internet connections and to disconnect individual computers from other computers. The impact of such an order on a massive executive agency is no less significant. The injunction would have a devastating effect on even the most routine communications within and among the Interior bureaus, components, and field offices that handle trust-related information.

The Department of the Interior is a cabinet agency with an annual budget of \$11 billion and approximately 70,000 employees. Declaration of W. Hord Tipton (3/22/04) at 1. The Department manages 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 a portfolio of approximately \$1 billion of information technology, including approximately 100,000 computers. Ibid. Even if the court had required severance only of internet connections and had

not addressed internal connections, the injunction would undermine the agency's mission and its ability to serve individual Indians and Tribes, other federal agencies, and the public in general. As Secretary Norton explained in her declaration filed in connection with the district court's March 2004 disconnection order, "Internet communication is not merely a useful tool - it is essential to much of what we do."

Declaration of Gale A. Norton (3/22/04) at 1.

The internet disconnection component of the injunction would frustrate the ability of the Minerals Management Service to receive, process, and disburse over \$500 million in mineral revenues on Federal and Indian leased lands paid by about 2,000 companies each month. MMS accomplishes this mission through delivery of reporting, accounting, and financial services. Tipton Decl. 7. As explained by Interior's CIO, "[a]ll such functions are heavily reliant on automated systems and access to the internet." Ibid.; see Cason, 7/18/05 AM at 38 ("the Minerals Management Service relies upon the Internet heavily to collect the information necessary to process rents, royalties, and bonuses owed to the federal government, including those for Indians").

Minerals revenues are a major source of income for forty-one Indian Tribes; approximately 20,000 individual Indian minerals owners; the federal government; and thirty-eight states. The court's internet disconnection mandate would thus prevent or hinder MMS from being able to make timely monthly disbursements

of over \$500 million in mineral revenues to States, Indians, and Treasury accounts. Tipton Decl. 7. As MMS's Deputy CIO testified, "if we have to shut down from the Internet, the oil and gas companies cannot put their production data into the system, and, therefore, we can't collect the royalties and put that money into the Treasury and, therefore, royalty checks are not paid out to all the allottees." Ekholm, 7/8/05 AM at 12; see Smith, 7/12/05 PM at 56-57 (same).

Other core aspects of Interior's operations that would be affected by an internet shutdown include the Department's personnel, procurement and financial management functions. See Tipton Decl. 3-7. As the record shows, Interior's National Business Center ("NBC") hosts major computer systems that "pay[] approximately 250,000 federal employees [across the government], as well as providing financial management [services] for approximately 30 or 40 different federal organizations, including the Department of Interior." McWhinney, 7/21/05 PM at 4; see Haycock, 7/14/05 PM at 73 ("we have 37 federal clients that we process their personnel actions and pay them.... All of that is computer based."). Impairing the networking capability of these systems "would [thus] have a severe impact on financial management for large portions of the federal government." McWhinney, 7/21/05 PM at 4.

This injunction does not only require new internet disconnections and preclude restoration of connections previously severed. The injunction also requires an internal, intranet

disconnection, 394 F. Supp. 2d at 277-78. Components such as MMS would have to sever their internet connections and also sever their connections to all other offices and bureaus within the Department. Components such as the Bureau of Indian Affairs and the Office of Special Trustee, which had not yet regained internet access, would not be permitted to reconnect and would lose their ability to communicate with other components. To make the calamity complete, affected systems must also dismantle internally within each office and bureau. Thus, every BIA computer must be disconnected from every other BIA computer, every OST computer must be disconnected from every other OST computer, and so on. Ibid. In effect, each affected computer would be transformed into a stand-alone unit isolated from every other computer and computer device in the Interior Department. Ibid.; Declaration of James E. Cason (10/27/05) at 4. As a result, users of the disconnected computers would be deprived of even the most rudimentary e-mail capacity. Implementing the court's order would also result in the loss of basic telephone service for Interior employees who depend on "Voice Over Internet Protocol" (VOIP) telephone systems. Ekholm, 7/8/05 AM at 14 ("we would have to turn off those phone systems"). VOIP is expressly included in the order's definition of "Information Technology System" to which the court's injunction applies (as are hand-held wireless "Blackberry" devices, which provide both telephone and e-mail services). 394 F. Supp. 2d at 276-77.

The court's order would have a particularly harsh impact on services to Indians. Among its many responsibilities, BIA distributes social services payments for individual Indians. To perform that function, it relies upon the automated Social Services Assistance System ("SSAS"). The SSAS system, used by BIA and Tribes, contains financial data used to generate public assistance checks and maintain individuals' files. As the record makes clear, "[i]f that system is shut down, those welfare payments will stop." McWhinney, 7/21/05 PM at 5.

These and other consequences of the injunction are in no way alleviated by its provision, proposed by plaintiffs, that Interior may, after providing written notice to the court and plaintiffs' counsel, "reconnect, for specified periods not to exceed five (5) business days per month, any Information Technology System that Houses or provides Access to Individual Indian Trust Data, for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." 394 F. Supp. 2d at 278.

The apparent premise of this provision is that complex, interconnected computer systems can repeatedly be turned on and off without impact on their functions. It is wholly unclear why the district court would embrace such a mistaken assumption. Like other aspects of its order, this provision highlights the limits of judicial competence to superintend complex information technologies. As is the case with analogous systems in the government and private sector, the computer systems at issue

depend on an ongoing input and exchange of massive amounts of information that cannot be arbitrarily compressed into brief, intermittent periods in which they may receive, process and forward critical data. See Cason Decl. 3, 12-14.

Moreover, this provision is hardly calculated to deal with the asserted threats to IITD. If that data were (contrary to fact) facing imminent, irreparable compromise, it is unclear why hackers could not inflict that harm during the five available days of operations. Indeed, because Interior would have no ability to download "patches" from the internet to guard against new security hazards, the systems would be even more vulnerable when returned to operation. See Tipton Decl. 8; Ekholm, 7/8/05 AM at 11 ("that makes you more vulnerable in many ways because you cannot patch your systems in a timely fashion").

More generally, the negative impact of repeated dismantlings of computer operations should be self-evident. As OMB guidance points out, to guard against the effect of service interruptions, "[a]gency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally not a viable back-up option. When automated support is not available, many of the functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service." OMB Circular A-130, App. III, § B(a)(2)(e). That a court would deliberately inflict this type of damage on an agency beggars belief.

The court opined that "BIA and OST have been disconnected from the Internet for years, yet still manage to carry out their Indian-related missions. Solutions implemented to allow these bureaus to function without access to the Internet should be fairly easily adapted and exported to other bureaus and offices." 394 F. Supp. 2d at 275. This statement is wrong in every respect. First, Interior's quarterly reports repeatedly note that existing internet disconnections do indeed impair Interior's ability to carry out its missions, see, e.g., Report No. 21 at 9-10. Second, BIA, OST, and other components have relied in important respects on MMS's ability to gather production and royalty data through its internet connection, which would be severed by the order at issue, see McWhinney, 7/21/05 PM at 5; Cason Decl. 6-7. Finally, these components have at least been able to communicate internally and with other components. The present injunction, unlike the court's previous orders, would sever bureau-to-bureau and even computer-to-computer communications. 394 F. Supp. 2d at 277-78.

The district court was aware of "the ways in which the department's operations were disrupted by this Court's last disconnection order," and noted in passing "the effects that a loss of Internet connectivity would have on the department's ability to service its customers, many of whom are other governmental agencies." 394 F. Supp. 2d at 274. The court concluded, in effect, that the perceived interest in protecting IITD data constituted an overriding public interest that rendered

the impact of its ruling immaterial. No basis exists for singling out one public interest to the exclusion of all others and rendering all other public interests irrelevant.

C. Plaintiffs Have Failed To Demonstrate That An Injunction Is Needed To Avoid Likely Irreparable Harm.

The court's willingness to undermine a cabinet agency's communications is all the more remarkable because plaintiffs have failed to make a threshold showing of irreparable injury that would entitle them to any equitable relief at all (even setting aside the fatal problems with their position discussed at Point I and the impact on the public interest discussed at Point II.B).

No injunction may issue unless the movant demonstrates that "irreparable injury is 'likely' to occur." Wisconsin Gas Co. v. FERC, 758 F.2d 669, 674 (D.C. Cir. 1985). "Bare allegations of what is likely to occur are of no value since the court must decide whether the harm will in fact occur. The movant must provide proof that the harm has occurred in the past and is likely to occur again, or proof indicating that the harm is certain to occur in the near future." Ibid. (citation omitted, emphasis in original). This, plaintiffs failed to do.

As discussed, plaintiffs provided no evidence that even one class member has ever been harmed by unauthorized computer tampering. Moreover, an IG auditor testified that she had never, in more than 20 years, heard of an instance in which someone had manipulated data within Interior's systems and arranged to have a beneficiary's payment sent to someone else. Sandy, 6/6/05 PM at

83. Likewise, as shown, the fact that the Special Master and the IG, armed with resources, expertise, and immunity from prosecution, were able to penetrate some of Interior's systems does not demonstrate that other persons will have the motivation or means of doing so, let alone that irreparable harm to trust data would necessarily result, see Tipton, 7/26/05 PM at 70, 75. The evidence does not indicate that Interior systems are, on the whole, more vulnerable than those of other cabinet departments, and, indeed, the 2004 "scorecard" issued by the House Committee on Government Reform rated Interior higher than several other agencies. See Docket #2933 at 7 n.11.

Although the injunction will not avoid imminent irreparable harm to any class member, it will almost certainly operate to the detriment of many members of the plaintiff class who rely on Interior's services to at least the same extent as the public generally. Nor can class members take solace in the belief that the injunction, whatever hardships it may impose, at least advances their interest in obtaining timely and accurate account statements. As this Court has observed, although the failure to provide computer systems is not a breach of a legal duty, effective computer systems are essential to the agency's accounting processes. See 240 F.3d at 1106. Indeed, accounting activities, like much of Interior's work, are dependent on computer systems and electronic communications. See 391 F.3d at 257 ("maintaining adequate computer systems ... is critical to the completion of an adequate accounting"); see Haycock, 7/14/05

PM at 73 (“[w]e rely on computers to do almost everything we do”); Ekholm, 7/8/05 AM at 13-14 (“Pretty much all - nearly all of our operational functions are done in an automated fashion these days.”). Thus, the effect of disabling computers and internal and external communications is to undermine those functions, including the performance of accounting activities that this lawsuit ostensibly seeks to accelerate.

With considerable understatement, the court acknowledged that compliance with its order would be “difficult,” and that “[p]riorities will likely have to be shuffled, resources will likely have to be redirected[.]” 394 F. Supp. 2d at 275. The court’s response was to declare that “[t]he relief granted today is not likely to prove popular in governmental circles. The Court is not, however, in the business of doing the popular thing, or the politically savvy thing. The Court must evaluate the evidence presented, and take the action that is warranted by that evidence.” Id. at 274.

The court is quite right that its role is not to do the “popular” or “politically savvy thing.” If it issues an injunction, however, it is obliged to operate within the traditional constraints on equitable authority. A court must consider the impact of its order on the public and on public services, and it may not redefine the public interest to include only one aspect of the interests of the plaintiff class. Similarly, an injunction can issue only if plaintiffs have carried their burden of demonstrating imminent irreparable harm,

and the court may not redefine irreparable harm to encompass harm that has never occurred in the past and is wholly conjectural in the future. These fatal failings would require reversal even apart from the equally fatal legal errors discussed in the first part of our argument.

CONCLUSION

This Court should vacate the October 20, 2005 injunction, which requires components of the Department of the Interior to disconnect their computers from internet and intragency access and also precludes some of those components from reestablishing internet access.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
ISAAC J. LIDSKY

(202) 514-5089

Attorneys, Appellate Staff
Civil Division, Room 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530-0001

Thomas M. Bondy
Alisa B. Klein
Mark R. Freeman
I. Glenn Cohen
Isaac J. Lidsky

JANUARY 2006

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 13,989 words, according to the count of Corel WordPerfect 12.


THOMAS M. BONDY

CERTIFICATE OF SERVICE

I hereby certify that on this 11th day of January, 2006, I caused copies of the foregoing brief to be sent to the Court and to the following 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
Mark I. Levy
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
607 14th Street, N.W.
Washington, D.C. 20005

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


THOMAS M. BONDY

STATUTORY ADDENDUM

ADDENDUM CONTENTS

Federal Information Security Management Act of 2002
(FISMA), 44 U.S.C. § 3541 et seq. 1a

UNITED STATES CODE ANNOTATED
United States Code Annotated **Currentness**
TITLE 44. PUBLIC PRINTING AND DOCUMENTS
Title 44. Public Printing and Documents **(Refs & Annos)**
CHAPTER 35--COORDINATION OF FEDERAL INFORMATION POLICY
Chapter 35. Coordination of Federal Information Policy **(Refs & Annos)**
SUBCHAPTER III--INFORMATION SECURITY
Subchapter III. Information Security **(Refs & Annos)**

→§ 3541. Purposes

The purposes of this subchapter are to--

- (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
- (2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
- (3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;
- (4) provide a mechanism for improved oversight of Federal agency information security programs;
- (5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and
- (6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2946.)

→§ 3542. Definitions

(a) **In general.**--Except as provided under subsection (b), the definitions under **section 3502** shall apply to this subchapter.

(b) **Additional definitions.**--As used in this subchapter:

(1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide--

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(2)(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency--

(i) the function, operation, or use of which--

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(3) The term "information technology" has the meaning given that term in section 11101 of title 40.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2947.)

⇒§ 3543. Authority and functions of the Director

(a) In general.--The Director shall oversee agency information security policies and practices, including--

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of--

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544(b);

(6) coordinating information security policies and procedures with related information resources management policies and procedures;

(7) overseeing the operation of the Federal information security incident center required under section 3546; and

(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including--

(A) a summary of the findings of evaluations required by section 3545;

(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

(C) significant deficiencies in agency information security practices;

(D) planned remedial action to address such deficiencies; and

(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

(b) National security systems.--Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

(c) Department of defense and central intelligence agency systems.--(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2947.)

⇒§ 3544. Federal agency responsibilities

(a) In general.--The head of each agency shall--

(1) be responsible for--

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of--

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including--

(i) information security standards promulgated under section 11331 of title 40; and

(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through--

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including--

(A) designating a senior agency information security officer who shall--

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

(B) developing and maintaining an agencywide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3543 of this title, and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

(b) Agency program.--Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes--

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

(2) policies and procedures that--

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with--

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

(iii) minimally acceptable system configuration requirements, as determined by the agency; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of--

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing--

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

(B) may include testing relied on in a evaluation [FN1] under section 3545;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including--

(A) mitigating risks associated with such incidents before substantial damage is done;

(B) notifying and consulting with the Federal information security incident center referred to in section 3546; and

(C) notifying and consulting with, as appropriate--

(i) law enforcement agencies and relevant Offices of Inspector General;

(ii) an office designated by the President for any incident involving a national security system; and

(iii) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) Agency reporting.--Each agency shall--

(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to--

(A) annual agency budgets;

(B) information resources management under subchapter 1 [FN2] of this chapter;

(C) information technology management under subtitle III of title 40;

(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101-576) (and the amendments made by that Act);

(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

(G) internal accounting and administrative controls under section 3512 of title 31, [FN3] (known as the "Federal Managers Financial Integrity Act"); and

(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)--

(A) as a material weakness in reporting under section 3512 of title 31; and

(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

(d) Performance plan.--(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of--

(A) the time periods, and

(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

(e) Public notice and comment.--Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2949.)

[FN1] So in original. Probably should be "an".

[FN2] So in original. Probably should be "subchapter I".

[FN3] So in original. The comma probably should not appear.

→§ 3545. Annual independent evaluation

(a) In general.--(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(2) Each evaluation under this section shall include--

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

(B) an assessment (made on the basis of the results of the testing) of compliance with--

(i) the requirements of this subchapter; and

(ii) related information security policies, procedures, standards, and guidelines; and

(C) separate presentations, as appropriate, regarding information security relating to national security systems.

(b) Independent auditor.--Subject to subsection (c)--

(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

(c) National security systems.--For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed--

(1) only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(d) Existing evaluations.--The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) Agency reporting.--(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

(f) Protection of information.--Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

(g) OMB reports to Congress.--(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3543(a)(8).

(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

(h) Comptroller general.--The Comptroller General shall periodically evaluate and report to Congress on--

(1) the adequacy and effectiveness of agency information security policies and practices; and

(2) implementation of the requirements of this subchapter.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2952, and amended Pub.L. 108-177, Title III, § 377(e), Dec. 13, 2003, 117 Stat. 2631.)

➔§ 3546. Federal information security incident center

(a) **In general.**--The Director shall ensure the operation of a central Federal information security incident center to--

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security;

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) **National security systems.**--Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954.)

➔§ 3547. National security systems

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency--

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

(3) complies with the requirements of this subchapter.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954.)

⇒§ 3548. Authorization of appropriations

There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954.)

⇒§ 3549. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g-3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2955.)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

| | |
|--|----------------------|
| _____) | |
| ELOUISE PEPION COBELL, <u>et al.</u> ,) | |
|) | |
| Plaintiffs,) | |
|) | |
| v.) | Case No. 1:96cv01285 |
|) | (Judge Lamberth) |
| DIRK KEMPTHORNE,) | |
| Secretary of the Interior, <u>et al.</u> ,) | |
|) | |
| Defendants.) | |
| _____) | |

ORDER

This matter comes before the Court on Plaintiffs' *Motion for Order to Show Cause Why Interior Secretary Dirk Kempthorne and [Associate Deputy Secretary] James Cason Should Not Be Held in Contempt in Their Official Capacity for Violating the October 20, 2005 Preliminary Injunction and Request for Coercive and Compensatory Sanctions* (filed June 9, 2006) (Dkt. # 3248). Upon consideration of the Plaintiffs' Motion, Defendants' Opposition, any Reply thereto, and the entire record of this case, it is hereby

ORDERED that the Motion for an Order to Show Cause is DENIED.

Hon. Royce C. Lamberth
UNITED STATES DISTRICT JUDGE
United States District Court for the
District of Columbia

Date: _____

cc:

Dodge Wells
Tracy L. Hilmer
Robert E. Kirschman, Jr.
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875

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

Keith Harper, Esq.
Richard A. Guest, Esq.
Native American Rights Fund
1712 N Street, NW
Washington, D.C. 20036-2976
Fax (202) 822-0068

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

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