IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,

Plaintiffs,

v.

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

Defendants.

Case No. 1:96CV01285
(Judge Lamberth)

INTERIOR DEFENDANTS' SUPPLEMENTAL OPPOSITION TO PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION

Interior Defendants respectfully submit this supplemental opposition to Plaintiffs' motion for a preliminary injunction.[1]

INTRODUCTION AND SUMMARY

Plaintiffs have not satisfied their burden of demonstrating that they are entitled to a preliminary injunction in this case. They have offered no evidence of deficiencies in the Department of Interior's information technology ("IT") security that could possibly justify the extraordinary remedy of disconnecting Interior from the Internet. To the contrary, the Special Master appointed by the Court to oversee IT security issues has allowed the vast majority of Interior's systems to reconnect to the Internet. Pursuant to the December 17,2001 Consent Order in this case, the systems could not be reconnected until the Special Master made the necessary inquiries "to determine if it provides adequate

[1] Plaintiffs filed a "Consolidated Motion For A Temporary Restraining Order and Motion For A Preliminary Injunction To Ensure The Protection Of Individual Indian Trust Data" (filed June 26, 2003) and a Notice of Proposed Preliminary Injunction (filed July 9,2003) (collectively "Plaintiffs' TRO/PI Motion").

security for individual Indian trust data." Consent Order Regarding Information Technology Security, at 7 (filed Dec. 17,2001) ("Consent Order"). Special Master Balaran has made no findings that any of the systems he previously approved have now become deficient.

The sole basis proffered by Plaintiffs for the extraordinary relief they seek is the Government's refusal to authorize the Special Master to conduct "penetration testing" of Interior's Information Technology ("IT") systems. But issues relating to IT security generally, and "penetration testing" specifically, are beyond the proper scope of this Court's limited review under the **APA** to determine whether Interior has taken actions "that are so defective that they would necessarily delay rather than accelerate the ultimate provision of an adequate accounting." Cobell v. Norton, 240 F.3d 1081, 1110 **(D.C.** Cir. 2001). In addition, as the court of appeals' recent decision confirms, a Special Master may not play the "investigative, quasi-inquisitorial, quasi-prosecutorial role," assumed by Mr. Balaran. Cobell v. Norton, __ F.3d __, No. 02-5374,2003 WL 21673009 at *11 (D.C. Cir. 2003); see also id. at *12 (holding that this Court's "appointment of the Monitor entailed a license to intrude into the internal affairs of the Department, which simply is not permissible under our adversarial system of justice and our constitutional system of separated powers").[2] It is particularly inappropriate for Special Master Balaran to assume such wide-ranging authority over Interior because, as explained in Interior's pending motion to disqualify, he must be disqualified from acting in any capacity.

[2] Interior Defendants acknowledge the limited role to be played by the Special Master under the Consent Order **in** monitoring reconnection activities following the December 2001 Temporary Restraining Order.

BACKGROUND

A. Pertinent Facts

On November 14,2001, the Special Master issued a Report and Recommendation identifying what he perceived to be deficiencies in the integrity of Interior's IT systems. See Report and Recommendation Regarding the Security of Trust Data at the Department of the Interior, Nov. 14, 2001. Subsequent to the issuance of the report, the Court issued a temporary restraining order requiring Interior to disconnect from the Internet all IT systems housing individual Indian Trust data. Order (filed Dec. 5,2001). Faced with the prospect of a prolonged Internet shutdown, Interior agreed to procedures that would allow it to reconnect its systems to the Internet. Under these procedures, the systems could not be reconnected until the Special Master made the necessary inquiries "to determine if it provides adequate security for individual Indian trust data." Consent Order, at 7. By definition, the systems that are now online have been approved for reconnection by the Special Master. For example, the Special Master has approved reconnection for the Office of Surface Mining ("OSM"). See Memorandum Of Points And Authorities In Opposition To Plaintiffs' Motion For *An* Order To Show Cause Why Interior Defendants Should Not Be Held In Contempt Regarding IT Security Matters (July 7, 2003) ("Brief in Opposition to Contempt Motion"), Exs. 1-2.[3]

Beginning in mid-2002, the Special Master expressed a desire to have his IT expert USinternetworking begin penetration testing to determine the adequacy of Interior's IT Security.

---

[3] Facts relating to the Consent Order and other matters pertinent to this motion are set out in detail in Interior's Brief in Opposition to Contempt Motion, which is fully incorporated herein by reference.

Although such testing was not required under the terms of the Consent Order, Interior began working with the Special Master to establish protocols to govern such testing. Brief in Opposition to Contempt Motion, Exs. **4-6.** Protocols were developed – but never finalized – that identified the parameters of such testing by, inter alia, defining different levels of testing that varied in their intrusiveness and their potential for causing harm to Interior's systems. See id., **Ex.** 6. ***An*** important feature of the protocols – known as "draft rules of engagement" – was the identification of "trusted points of contact" ("TPOC"), who were provided advance notice of planned penetration testing in order to minimize potential damage to IT systems and avoid having the intrusions reported to federal law enforcement authorities **as** unauthorized. Id. Pursuant to the narrow context set out in the draft rules, the Special Master, through contractors, has conducted tests in which he has attempted to access Interior IT systems and the data contained therein.

On April 22,2003, the contractor working with the Special Master informed the TPOCs that it intended to conduct penetration testing with respect to several OSM servers. Id., Ex. 7. The following day, the contractor attempted to conduct the test, but was unsuccessful because, it was later discovered, a cable had become dislodged from the server while it was being moved. Id. Upon discovery of the loose cable, OSM promptly remedied it, and the Special Master's contractor subsequently performed the tests. Id., Ex. 8; Trial Tr., June 5, 2003, p.m., at 9:9-18 (J. Cason testimony that cable problem was rectified and Special Master's contractor was able to complete the tests). Although the interruption did not prevent the Special Master's contractor from ultimately completing its testing of the subject server, the Special Master questioned whether any of the TPOCs had provided OSM employees with advance notice of the test. Despite receiving confirmation that no

TPOC had done so, the Special Master questioned the veracity of those involved, demanded a personal certification by Department of Justice counsel that the reported cable failure was true, and suggested that he intended to commence an investigation by asking for the names of every individual who had access to the OSM server. Brief in Opposition to Contempt Motion at 6-7, **Ex. 7** at 2, **Ex.** 9; Plaintiffs' Motion For ***An*** Order To Show Cause Why Interior Defendants Should Not Be Held In Contempt Regarding IT Security Matters (June 20, 2003) ("Plaintiffs' Contempt Motion"), Exs. 1-5.

These incidents made clear that the tentative draft rules of engagement for performing penetration testing were unworkable. In addition, penetration testing conducted by the Special Master had revealed no material security deficiencies with respect to Interior's IT security. **As** a result, the United States informed the Special Master that it was unable to consent to any further penetration testing. Plaintiffs' Contempt Motion, **Ex.** 4.

B. Plaintiffs' Request for TRO and Preliminary Injunction

In their TRO/PI Motion, Plaintiffs allege that individual Indian trust data "is recklessly exposed to unlawful manipulation and deletion that threatens the integrity of the trust data," and that "it is clear that corruption or loss of individual Indian trust data will result in irreparable harm and cannot be cured." Plaintiffs' TRO/PI Motion at 1. Plaintiffs submitted no affidavit or other evidence with their TRO/PI Motion.[4] Rather, the motion rests solely on the Government's refusal to authorize further

[4] Plaintiffs instead "incorporated by reference" briefs they submitted in connection with motions they filed in 2001 for a temporary restraining order, preliminary injunction, and contempt findings, and Plaintiffs' Contempt Motion. The briefs submitted by Plaintiffs over two years ago do not speak to the specific issues they raise in their present motion or to the current state of IT security at Interior and, therefore, provide no support for their present motion. Plaintiffs' Contempt Motion, also submitted without any affidavits or other evidence, merely recites the same unsupported allegations made in Plaintiffs' TRO/PI Motion, and merely attaches as exhibits the correspondence related to the cable failure and penetration testing.

penetration testing by the Special Master. See id. at 2-4. Plaintiffs aver that the inability of the Special Master to conduct penetration testing presents a "clear and present" danger to individual Indian trust data because the Special Master's contractor concluded in a report that one OSM server in Pittsburgh lacked sufficient intrusion detection software and the intrusion detection software on another OSM server in Pittsburgh had not been adequately monitored.[5] Id. at 4. No evidence was submitted that the OSM servers in Pittsburgh even housed or accessed individual Indian trust data, much less that such data was "in imminent jeopardy of loss, corruption or unlawful manipulation," as Plaintiffs generally alleged. Id. at 4. In fact, the OSM servers in Pittsburgh do not house or access any such data.[6]

C. TRO and Proposed Preliminary Injunction

On June 27, 2003, the Court granted Plaintiffs' Motion for a TRO, and ordered "that Interior defendants immediately shall disconnect from the Internet all information technology systems which house or provide access to individual Indian Trust data until such time as the Special Master has determined that all Individual Indian Trust data is properly secured." TRO at 2. The Court also ordered that Interior "immediately shall disconnect from the Lntemet all computers within the custody and control of the Department of the Interior, its employees and contractors, that house or provide access to individual Indian trust data until such time as the Special Master has determined that Individual Indian Trust data is properly secured." TRO at 2. The TRO exempted "[a]ny system essential for protection against fires and other threat to life or property." Id. at 2. The order did not

---

[5] The OSM servers in Pittsburgh are distinct from the OSM server that suffered a cable failure; the latter server is located in Washington D.C.

[6] See Declaration of Glenda H. Lewis, executed Jan. 11,2002, at ¶¶ 3-4. Interior submitted the declaration to Special Master Balaran in connection with the proposed reconnection of OSM to the Internet in 2002. **A** copy of the declaration is attached hereto as Exhibit 1.

identify any of the reasons for its issuance, see id., but during oral argument of the motion, the Court indicated that it was issuing the TRO because it lacked adequate time to fully address the merits of the motion. On July 14,2003, the Court extended the TRO for an additional ten days. Order (filed July 14,2003).

Plaintiffs have now proposed a preliminary injunction that would sweep even more broadly than the Court's TRO. Among other things, plaintiffs' proposal would expand the definition of "Individual Indian Trust Data" as previously defined in the December 17, 2001 Consent Order. It would also confer broad new powers upon the Special Master, including "the authority to do all acts and take all measures necessary or proper for the effective performance of the Special Master's duties conferred upon him by this Order, including without limitation, the retention of experts, " Proposed Preliminary Injunction at ¶ 4, the power to "conduct unannounced site visits, order the production of information, documents, and other records, and conduct investigations," id. at ¶ *5,* and the "power and authority to scan, conduct penetration testing or engage in any other appropriate system security test of Interior's Information Technology Systems or computers that House or Access Individual Indian Trust Data," id. at ¶ **6.** These powers far exceed the role of the Special Master under the December 17, 2001 Consent Order.

D. The Court of Appeals' July 18,2003 Decision

On July 18,2003, the court of appeals issued a decision reversing the September 17,2002 contempt findings against the Interior defendants in their entirety, and vacating the order appointing Joseph S. Kieffer as a Court Monitor and the order elevating him to the position of "Special Master-Monitor." & Cobell v. Norton, No. 02-5374,2003 WL 21673009 (D.C. Cir. July 18,2003). In

that decision, the court of appeals made clear that a Special Master is subject to the same standards of recusal as a judge, id. at *13, that a Special Master may not simultaneously wield both judicial and investigative authority, id. at **13-14, and that the injury suffered by a party required to subject itself to oversight by a judicial officer who should be disqualified is "by its nature irreparable." Id. at *7. Among other things, the court stressed that "it was surely impermissible to invest the Court Monitor with wide-ranging extrajudicial duties over the Government's objection," and that the "appointment of the Monitor entailed a license to intrude into the internal affairs of the Department, which simply is not permissible under our adversarial system of justice and our constitutional system of separated powers." Id. at **11-12.

GOVERNING LEGAL STANDARDS

The Supreme Court has observed that "a preliminary injunction is an extraordinary and drastic remedy, one that should not be granted unless the movant, by a clear showing, carries the burden of persuasion." Mazurek v. Armstrong, 520 U.S. 968, 972 (1997) (citation omitted). In seeking such extraordinary relief, a plaintiff must include with its application "all affidavits on which the plaintiff intends to rely." L. Cv. R. 65.1.

A court may issue a preliminary injunction only when a movant demonstrates: (1) a substantial likelihood of success on the merits; **(2)** that it would suffer irreparable injury **if** the relief is not granted; (3) that an injunction would not injure other interested parties; and (4) that the public interest would be furthered **by** the injunction. Mova Pharm. Corp. v. Shalala, 140 F.3d 1060, 1066 (D.C. Cir. 1998). **If** a court finds, based on the above factors, that relief is warranted, "any injunction that the court issues must be carefully circumscribed and tailored to remedy the harm shown." Lee v. Christian Coalition of

America. 160 F. Supp. 2d 14, 27 (D.D.C. 2001) (citing National Treasury Employees Union v. Yeutter, 918 F.2d 968, 977 (D.C. Cir. 1990)). "Every order granting an injunction and every restraining order shall set forth the reasons for its issuance; shall be specific in terms; [and] shall describe in reasonable detail, and not by reference to the complaint or other document, the act or acts sought to be restrained . . . ." Fed. R. Civ. P. 65(d).

ARGUMENT

Plaintiffs have not satisfied the stringent criteria for obtaining a preliminary injunction, much less an injunction that would take the extraordinary step of disconnecting an entire Executive Branch Department from the Internet. The systems that Plaintiffs propose to disconnect from the Internet are online precisely because the Special Master previously approved them for reconnection. Plaintiffs have offered no evidence that the security of these systems has somehow become deficient. In any event, even if Plaintiffs had made a colorable evidentiary submission, this Court's review under the APA does not extend to wholesale oversight of IT Security issues. Moreover, as the court of appeals recently explained, a Special Master may not wield intrusive investigative powers. And, it would be particularly inappropriate to invest Mr. Balaran with such powers because he must be disqualified for the reasons stated in our pending disqualification motion.

I. Plaintiffs Have Not Met the Requirements for a TRO or Preliminary Injunction

Plaintiffs have not submitted any affidavit or other evidence that would support the TRO that was issued or the preliminary injunction that is sought. Instead, Plaintiffs rely solely on the assertion that the Government's refusal to permit penetration testing will result in "loss, corruption or unlawful manipulation'' of data, based solely upon statements – unsworn and unverified – made by the Special

Master's IT contractor relating to vulnerabilities at one OSM server location.[7] Plaintiffs' TRO/PI Motion at **4.** These baseless assertions are deficient on their face and cannot support the TRO currently in place or the more radical relief Plaintiffs seek in their proposed injunction. With respect to the four factors that must be considered in this analysis, Plaintiffs do not even approach the requisite showing.

A. No Likelihood of Success on the Merits or Irreparable Harm to Plaintiffs

Plaintiffs have not demonstrated that they can succeed on their claim that individual Indian trust data is in imminent danger of corruption. They have presented no evidence that IT systems housing such data have vulnerabilities that would lead to such a conclusion, or that unauthorized access of those IT systems is occurring. On the contrary, pursuant to the terms of the December 17, 2001 Consent Order, every Interior IT system that houses individual Indian trust data, and that was online prior to the entry of the Court's TRO, had been reconnected to the Internet based on the Special Master's own conclusion that such systems were adequately secure. This fact alone warrants denial of the motion for a preliminary injunction.[8] See WMATA v. Holiday Tours, Inc., 559 F.2d 841, **843** (D.C. Cir. 1977) (absent a "substantial indication" of likely success on the merits, "there would be no justification for the

---

[7] **As** noted above, that server, and OSM IT systems in general, do not house any individual Indian trust data. Thus, Interior has been forced to shut down all IT systems that house individual Indian trust data based not on any established (or even alleged) deficiencies with respect to those systems, but upon an alleged vulnerability in an OSM system that houses no individual Indian trust data.

[8] Even if Plaintiffs had come forward with evidence that a system housing individual Indian trust data was in imminent peril of corruption, the draconian remedy of shutting down all IT systems housing such data would be unsupportable. See Lee, 160 F.Supp. 2d at 27 ("[A]ny injunction that the court issues must be carefully circumscribed and tailored to remedy the harm shown.") (citing National Treasury Employees Union v. Yeutter, 918 F.2d 968, 977).

court's intrusion into the ordinary processes of administration and judicial review.").

That the Government will not now authorize the Special Master to attempt to "penetrate" Interior's IT systems does not alter this result. Attempting to gain unauthorized access to information contained on Government computers is a violation of federal law. See 18 U.S.C. § 1030. Accordingly, the Special Master has no authority to attempt to gain access to Interior's IT systems unless the United States grants him such authority. That the United States does not authorize such testing does not result in the imminent corruption of trust data where there has been no evidence of such corruption.

Although Plaintiffs have not explicitly argued in their brief that Interior has authorized penetration testing through the Consent Order, any suggestion to that effect is unfounded. The Consent Order does not even relate to the matter of penetration testing, much less authorize it. Rather, it establishes a procedure for reconnecting Interior IT systems to the Internet through proposals to the Special Master, and provides the Special Master authority to verify the information set forth in those proposals, There is no provision in the Consent Order that even speaks to penetration testing by the Special Master, much less to such testing **after** such systems have been reconnected. Penetration testing has been conducted solely on a case-by-case basis pursuant to the draft rules of engagement, which have never been formalized. See Meeting Tr., July 15, 2003, at 50:1-52:20 (Special Master discussing the history of penetration testing under the draft rules of engagement, and noting "I think they were de facto rules, and I just assumed that we'd been operating under them long enough that that was sort of the law of the land. If this is something that you want to put in a document that's given to all parties, then we will sign off on it.").

B. Irreparable Injury to Interior and Impact on Public Interest

The magnitude of the injury to Interior being caused by the TRO is indisputable and far-reaching, and will be greatly magnified by the issuance of a preliminary injunction. Declaration of W. Hord Tipton, Chief Information Officer, executed July 25,2003 and submitted herewith ("Tipton Decl."). The proposed preliminary injunction would, among other things, halt improvements of Interior's IT systems, Tipton Dec. at ¶ 7; hinder Interior's ability to conduct security operations with the Department of Homeland Security, id.; affect the ability to perform functions necessary to ensure the continuity of Government operations in the event of an emergency, id. at ¶ 8; affect the Federal Financial System, id. at ¶ 9; negatively impact the preparation of Bureau and Department financial statements, id. at ¶ 11; adversely affect the Interior Department Electronic Acquisition System, which governs Interior's procurement programs, id. at ¶ 12; affect Interior's hiring and employment activities, id. at ¶ 14; adversely affect Interior's FOIA activities, id. at ¶ 15; prevent the Mineral Management Service from carrying out its responsibilities relating to the disbursement of monthly mineral revenues, id. at ¶ **16;** impair the ability of the Office of Historical Trust Accounting to effectively coordinate activities among its staff and contractors, which are geographically disbursed, id. at ¶ 18; prevent the public from accessing the Bureau of Land Management's records systems that relate to the 270 million acres of public domain lands, id. at ¶ 19; adversely impact OSM's ability to carry out functions relating to mining activities, id. at ¶ 21; preclude the public from electronically accessing information relating to national parks, id. at ¶ 22; and prevent the Fish and Wildlife Service from accessing information necessary to complete scientific casework, id. at ¶ 23.

As the foregoing illustrates, the preliminary injunction sought by Plaintiffs would have an

enormous adverse impact not only on Interior, but also on other entities and the public. This conclusion is beyond reasonable question; indeed, Plaintiffs do not even address the harm to Interior and the public interest posed by their motion. See Dorfinann v. Boozer, 414 F.2d 1168, 1173 (D.C. Cir. 1969) ("[E]ven where denial of a preliminary injunction will harm the plaintiff, the injunction should not be issued where it would work a great and potentially irreparable harm to the party enjoined . . . unless an overwhelming case in the plaintiffs favor is present on the merits and equities of the controversy.") (citation omitted).

11. The Proposed Preliminary Injunction Would Impermissibly Intrude Into The Affairs Of The Department Of The Interior

A. Review Under the APA Is Limited

In its first decision in this case, the court of appeals made clear this case concerns the Department of the Interior's statutory duty to perform an accounting. The court explained that this Court's review under the APA is limited to determining whether Interior has taken actions "that are so defective that they would necessarily delay rather than accelerate the ultimate provision of an adequate accounting." Cobell v. Norton, 240 F.3d 1081, 1110 (D.C. Cir. 2001). The court of appeals did not sanction a radical departure from settled principles of judicial review, nor did it authorize a judicial takeover of trust management. To the contrary, the appeals court emphasized that the reviewable agency action was the failure to perform an accounting. While failure to take various subsidiary actions might be evidence of the failure to perform this duty, they were not themselves enforceable obligations. Id. at 1105-06 (noting that "defendants should be afforded sufficient discretion in determining the precise route they take").

These admonitions reflect settled law. Although courts have power to review agency action (or

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

Nor may a court insert itself into the agency's decision-making process by imposing additional procedural – much less, substantive – requirements on agencies beyond those mandated by statute. As the Supreme Court stressed in Vermont Yankee Nuclear Power Corp. v. NRDC. Inc., 435 U.S. 519 (1978), the judiciary may not dictate to agencies the methods and procedures of needed inquiries on remand because "[s]uch a procedure clearly runs the risk of 'propel[ling] the court into the domain which Congress has set aside exclusively for the administrative agency.'" Id. at 545 (quoting SEC v. Chenery Corp., 332 U.S. 194, 196 (1947)). These principles apply even where an agency has unquestionably delayed in taking appropriate action. See In re: Barr Laboratories, Inc., 930 F.2d 72, 74 (D.C. Cir. 1991).

Likewise, even in exceptional cases in which an agency has flagrantly disregarded a congressionally-mandated deadline for rulemaking, the appropriate judicial role is to retain jurisdiction over a case and require periodic progress reports until the agency has completed the required action.

See, e.g., In re: United Mine Workers of America International Union, 190 F.3d 545,556 (D.C. Cir. 1999) (retaining jurisdiction and requiring semi-annual progress reports from the Mine Safety and Health Administration until it issued final regulations); see also Global Van Lines, Inc. v. FCC, 804 F.2d 1293, 1305 n.95 (D.C. Cir. 1986) (recognizing agency "discretion to determine in the first instance" how to bring itself into compliance); Telecommunications Research and Action Ctr. v. FCC, 750 F.2d 70, 81 (D.C. Cir. 1984) (retaining jurisdiction pending FCC's resolution of underlying issues). These principles harmonize with the rule that judicial review under the **APA** is limited to the administrative record. See Florida Power & Light Co. v. Lorion, 470 U.S. 729, 743-44 (1985) ("The task of the reviewing court is to apply the appropriate APA standard of review, 5 U.S.C. § 706, to the agency decision based on the record the agency presents to the reviewing court.").

It is the responsibility of the Department of the Interior, not the Judicial Branch, to test and assess the security of Interior IT systems, and the agency is performing that function. Interior's retained experts currently conduct security scans of its IT systems; Interior is developing the means to conduct penetration testing now that it is no longer incurring the expense of the Special Master's penetration testing, and Interior will use other appropriate assessment means as circumstances require. To the extent that Interior's performance of this function, which is neither "agency action" nor "final agency action," is subject to judicial review at all under the **APA,** Interior's approach may be reviewed only to determine whether it "would necessarily delay rather than accelerate the ultimate provision of an adequate accounting." Cobell, 240 F.3d at 1110. The agency's actions are not subject to de novo review in this Court.

B. The Court Has No Power To Confer Wide-Ranging Investigative Authority On A Special Master

As the court of appeals recently made clear, this Court, and its Special Masters or other judicial adjuncts, are limited to resolving disputes brought to it by the parties; they have no general investigative authority. The court observed that this is not an "institutional reform" case and found impermissible the former Court Monitor's wide-ranging charge to monitor all of Interior's trust reform activities, explaining that judicial intrusion into the internal affairs of an Executive Branch Agency runs counter to our judicial system and violates the constitutional mandate of separated powers. Cobell v. Norton, 2003 WL 21673009 at *12. The Court is not empowered to oversee the details of the government's management of the Indian trust fund program, and the extraordinary actions that are contemplated by Plaintiffs' preliminary injunction motion would run afoul of that fundamental principle.

The proposed injunction would give the Special Master virtually unfettered control over any Interior IT system that "evidences, embodies, refers, or relates to -- directly or indirectly and generally or specifically – Individual Indian Trust Assets. Proposed Preliminary Injunction at 4-5. His powers would include "the authority to do all acts and take all measures necessary or proper for the effective performance of the Special Master's duties conferred upon him by this Order, including without limitation, the retention of experts," id. at ¶ 4, the power to "conduct unannounced site visits, order the production of information, documents, and other records, and conduct investigations," id. at ¶ 5, and the "power and authority to scan, conduct penetration testing or engage in any other appropriate system security test of Interior's Information Technology Systems or computers that House or Access Individual Indian Trust Data," id. at ¶ 6. Such wide-ranging, investigative authority is plainly prohibited. Cobell v. Norton, 2003 WL 21673009 at ** 11-12 ("[T]he district court's appointment of the Monitor

entailed a license to intrude into the internal affairs of the Department, which simply is not permissible under our adversarial system of justice and our constitutional system of separated powers.").

III. Mr. Balaran Must Be Disqualified From Acting In Any Capacity In This Case

Even if general oversight of IT security were within the scope **of** this Court's limited review under the APA, and even if a Special Master could, in appropriate circumstances, exercise some investigative authority, Mr. Balaran cannot do so in this case. **As** our pending motion to disqualify Mr. Balaran explains, his conduct in this case demonstrates actual bias and would, at a minimum, cause an objective observer to question his impartiality. See 28 U.S.C. § 455. The court of appeals' ruling conclusively establishes that Special Masters are subject to the same standards of recusal as federal judges. 2003 **WL** 21673009, at *13 (citing Jenkins v. Sterlacci, 849 F.2d 627,630-32 & n.1 (D.C. Cir. 1988)). **As** a result, Interior's failure to comply with Mr. Balaran's demands to accede to "penetration testing" cannot provide a proper basis for issuing a preliminary injunction. To the contrary, allowing a judicial officer who must be disqualified to assume any role in this case would inflict irreparable harm on Interior. See id. at *7 ("When the relief sought is recusal of a disqualified judicial officer, however, the injury suffered by a party required to complete judicial proceedings overseen by that officer is by its nature irreparable.").

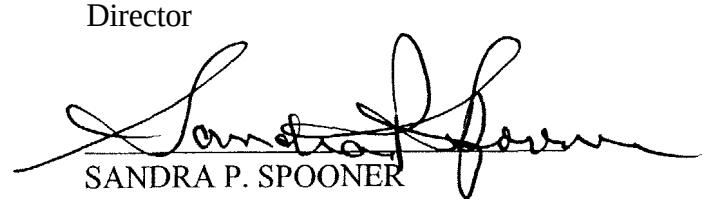
CONCLUSION

For all of the foregoing reasons, Interior Defendants respectfully request that the Court deny Plaintiffs' motion for a preliminary injunction.

Dated: June 25,2003

Respectfully submitted,

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



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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et. al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No, I:96CV0 1285
	)	(Judge Lamberth)
GALE NORTON, Secretary of the Interior, et. al,	)	
	)	
Defendants.	)	

DECLARATION OF GLENDA H. OWENS

1. I am the Acting Director of the Office of Surface Mining (OSM), Department of the Interior (Interior;).

2. As the Acting Director of OSM, my responsibilities include implementation of the Surface Mining 'Control and Reclamation Act of 1977, implementing regulations. policies and procedures and other related laws. These responsibilities include providing leadership for the management of the day-to-day operations of OSM, formulation of OSM policies, and leadership in the administration of all aspects of the programmatic, technical, and administrative support functions, including information technology systems (IT) systems.

3. After careful consideration and review, OSM was able to locate only one IT system, an application system, that contained individual Indian Trust data. That information had been submitted to OSM as part of a coal mining permit application and is public information. The data, related to the McKinley mine, has been downloaded to a CD for greater safekeeping. Therefore, OSM IT systems no longer house any individual Indian trust data.

4. While OSM may possess other individual Indian trust data, none of it is in computerized form and therefore none of it is housed on OSM's IT systems.

5. I declare under penalty of perjury that the foregoing is *true* and correct to the best of my knowledge.

Dated: January 11, 2002

GLENDA H. OWENS

Exhibit 1
Intr. Def's. Suppl Opposition
to Pltfs. Motion for P. I

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

DECLARATION OF W. HORD TIPTON

1. I am the Chief Information Officer ("CIO") for the United States Department of the Interior ("Interior," "DOI" or "Department") in Washington, D.C. In this capacity, my duties and responsibilities include management of the information technology ("IT") systems and implementation of applicable Interior policies and directives. As CIO, I oversee the management of Department-wide systems. I am responsible for issuing department-wide policies and measuring compliance against those policies. Additionally, I coordinate with Bureau/Office CIOs in the development and maintenance of Bureau-specific IT systems. I am also responsible for overseeing the portfolios of **all** IT investments and spending for the Department.

2. This declaration is offered in support of Interior Defendants' Supplemental Opposition to Plaintiffs' Motion for a Preliminary Injunction.

3. I assumed my current position in October 2002. Before that time, I had been Acting CIO since June 10, 2002. Prior to my becoming Acting CIO, I served for approximately two-and-half years as the CIO for the Bureau of Land Management ("BLM") arid five years as

Exhibit 2
Intr. Def's. Suppl. **Oppositio**
to Pltfs **Motion for P.** I

Assistant Director for several programs. I also served as State Director for the Eastern States Office of the BLM. Prior to that, I was Deputy Director of the Office of Surface Mining ("OSM") for four years.

4. Based upon my current and former positions within Interior, I am familiar with the real and potential harms that could result to both Department-wide and bureau specific programs and systems if the Court enters the preliminary injunction proposed by plaintiffs (the "Proposed PI Order").

5. The Proposed PI Order contains extremely broad definitions, most notably the definitions of "Individual Indian Trust Data" ("IITD") and "Individual Indian Trust Assets" ("IITA"). If the Court were to adopt such broad definitions, Interior arguably would be forced to disconnect numerous systems previously connected to the Internet in accordance with the Consent Order entered December 17, 2001. Disconnection of these additional systems would have far-reaching impacts upon Interior's operations, the plaintiffs, and the general public.

6. Because the Proposed PI Order sets forth a limited exemption for IT systems "essential for protection against fires and other threats to life or property," my declaration does not discuss those systems or computers that support wildfire management and suppression efforts. However, it is important to note that Department systems are integrated and in the event of an emergency, it is impossible to forecast which systems will be needed by emergency response teams. For example, the Interior Department Electronic Acquisition System ("IDEAS") and IDEAS-Electronic Commerce ("EC") are critical to provide contracting support for the wildland firefighting efforts. Other agencies providing information critical in emergencies, such as the National Weather Service, rely heavily on data collected and provided from Departmental

systems through the Internet that are not readily ascertainable as "essential for protection against fires and other threats to life or property." Additionally, the Department's law enforcement and security personnel will lose access to critical databases that may not fall within the proposed exemption.

7. The balance of this declaration describes some of the definite and potential impacts that would or could result from the Court's entry of the Proposed PI Order and is not intended to set forth an exhaustive listing. In addition, this declaration briefly describes the Department's scanning efforts, an important part of the Department's security management program.

Description of Impacts Upon Selected Department-Wide Programs and Systems

8. Disconnection would hinder maintenance of Interior's IT systems and would impact Interior's IT security. For example, such an Internet shutdown would result in the inability to electronically obtain security software updates and patches, including antivirus definition files and intrusion detection systems signature files. In addition, Interior will lose the capability to electronically report and coordinate with the Department of Homeland Security ("Homeland Security"), which operates the Federal Computer Incident Reporting Center ("FedCIRC"). This would hinder or eliminate the ability of the Department to coordinate security reporting with Homeland Security and would affect such operations as reporting incidents to the FedCIRC and obtaining patches that allow the Department to secure, update and measure IT system configuration compliance. Further, the Department would not receive the electronically transmitted Daily Open Source Infrastructure Reports from Homeland Security. In addition, Interior's IT security managers and other network operations personnel would not be

able to access an Interior website that provides IT security policy, patch updates, and a library of information relevant to system management, such as DOI guidelines.

9. Disconnection will affect the ability to perform emergency Continuity of Operations ("COO") and Continuity of Government ("COG") functions. COO/COG is a national-level program involving the White House and other departments. Loss of Internet access will impact on the United States' ability to assume the continuity of government operations in the event that the United States is subject to a terrorist attack. COO/COG functions are severely limited without access to all communication tools available to the Department. The more serious the emergency scenario, the more dependent COO/COG communications would be on all available forms of communication.

10. Disconnection will affect the Federal Financial System ("FFS"), which provides financial accounting, funds control, management accounting, and financial reporting processes for Interior bureaus and offices, as well as approximately twenty (20) non-Interior agencies. Not being able to process payments for government services would be a violation of the Anti-Deficiency Act. FFS is used by major Department bureaus to manage and control financial activity related to Federal appropriated funds, including funds management, receipt management of Federal funds, payments to vendors, reimbursement of charge card transactions, travel reimbursements and other financial transactions. If the Department is required to disconnect from the Internet, some of the smaller FFS clients will lose the secure network connectivity provided via Internet Virtual Private Network ("VPN") connections. These VPN connections allow smaller clients a more economical connection alternative to expensive dedicated lines. Installation of dedicated lines for these clients will take a minimum of four (4) months to procure

and will require them to incur significant additional costs. Until such time as new communications lines can be procured for these clients, there will be a significant impact on these clients' ability to make vendor and travel payments. Further, the inability to access FFS may result in a violation of the Prompt Payment Act, 31 U.S.C. § 3909.

11. Interior operates the Federal Personnel Payroll System ("FPPS"), and this system would be affected negatively by disconnection. Without FPPS access, personnel actions cannot be processed in **FPPS.** This includes appointment of new hires, promotions, awards, reassignments, retirements, transfers to other government agencies, and changes in enrollment resulting from open season for Federal employees for Thrift Savings Plan. FPPS customers would lose secure network connectivity to the VPN to input time and attendance data for payroll processing. In addition, the FPPS system has been chosen as one (1) of four **(4)** electronic payroll service providers to provide payroll services for all federal government organizations and will be providing services to many more government agencies in the near future. The Department is currently working on the conversion of four **(4)** non-Interior agency clients and is using secure Internet connections during the early conversion stages of the projects until such time as permanent non-Internet network connections are established. Disconnecting Internet services at this time would impact conversion schedules.

12. Interior'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 Interior bureaus and offices and to non-DOI 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

Interior's Inspector General. If the Department is required to disconnect the CFS System from the Internet, Interior and its clients will not meet quarterly and year-end financial statement deadlines and it would be unlikely that Interior or its clients could complete its annual financial statement audit, in violation of the Government Management Reform Act and OMB Circular 01-09. Further, delays in the completion of bureau financial statements will substantially increase the audit costs and jeopardize the data submission to Treasury for the consolidated financial statements of the Federal Government.

13. Disconnection will affect IDEAS, which is used by all bureaus as well as some non-Interior clients. Non-Interior clients include defense and other national security agencies, which could impact national defense and homeland security. IDEAS is utilized to comply with the Federal Acquisition Regulation ("FAR'), which require that procurement actions be electronically posted on single point-of-entry for the Federal government through the FedBizOpps web site operated by the General Services Administration ("GSA"). Part 5 of FAR requires that Federal notices of opportunities for contracting be announced to the public and contract solicitations and be made publicly available to vendors interested in selling to the Federal government. IDEAS encompasses requests for quotes, requests for proposals, and vendor contract award information. If vendors are unable to submit electronic proposals for procurement requirements, bid protest actions may be brought against the Federal government, with significant dollar impacts on Interior. In addition, IDEAS users will not be able to obtain procurement data necessary to perform their duties because they will be unable to initiate or complete any contract actions in the system. Further, IDEAS is utilized for electronic contract administration, e.g., obtaining contract actions, such as delivery orders, modifications, change

orders to contracts, or provide proposals to active procurement actions. Finally, procurement notices for time-sensitive, critical wildland fire program, and construction and repair contracts will not be posted timely. Delays will affect Interior's ability to award contracts early enough to ensure completion of critical maintenance tasks during this year's construction season and reduce the pool of available competitors for Interior contracts. Because of the timing of the proposed PI, contract actions scheduled for award in the last quarter of the fiscal year are in jeopardy, as annual appropriations cannot be spent in subsequent fiscal years. Typically, Interior averages more than fifty (50) announcements per business day on requirements that exceed $2 billion dollars in obligations annually.

14. Disconnection will affect the electronic commerce payments. IDEAS-EC is a web application that allows registered trading partner vendors to submit invoices electronically to the government for payment via electronic data interchange. The absence of this system will increase the government cost for services due to penalties for late payments.

15. Disconnection will affect the hiring and employment activities for the Department and its bureaus. The Department utilizes Internet access to the Office of Personnel Management's ("OPM") web site to post vacancies, and all bureaus announce employment vacancies using OPM's USAJOBS web site. OPM requires that all vacancies open to the general public be posted on the USAJOBS site. In addition, most bureaus have web-based hiring systems that accept, rate, rank, and refer candidates.

Description of Selected TRO Impacts That Will Continue Under the Proposed PI Order

16. Prior to the June 27, 2003 Temporary Restraining Order ("TRO"), Interior had Electronic Freedom of Information Act ("E-FOIA") capabilities required by 5 U.S.C. §

552(a)(2)(E) utilizing a server previously deemed to have adequate security, pursuant to the December 17, 2001 Consent Order. E-FOIA requires Interior to make electronically available FOIA records. The relevant server **was** disconnected as a result of the TRO, and the Proposed PI Order would continue this disconnection. The total number of FOIA requests will increase as a result of disconnection because the public information currently available on the Interior's websites will no longer be available on-line. The time required to process the average FOIA request will increase because the FOIA guidance currently available on the Interior's website will no longer be available to the public. The Interior's websites have become a key communication vehicle for the program, directing requestors to the appropriate FOIA office, informing requestors of current regulations and fee schedules. The agency's website is a key research and communication tool for FOIA staff. Customer satisfaction with the program will decrease because the cost to the customers for access to agency information would increase (due to the imposition of statutory FOIA fees), and the timeliness of obtaining agency information will decrease.

17. Prior to the June 27, 2003 TRO, the Mineral Management Service ("MMS") was deemed to have adequate security, pursuant to the December 17, 2001 Consent Order. Some of MMS's systems were disconnected as a result of the TRO, and the Proposed PI Order would continue the following negative impacts:

A. MMS is not receiving international reports on offshore accidents, domestic and international safety alerts from agencies and industry associations, and oil-spill reports via the U.S. Coast Guard's automated system. In addition, MMS is not receiving important safety research data (drilling, production, facilities, pipelines)

in a timely manner or the latest manufacturer updates on new technology and safety improvements. All of this information is analyzed and then used to communicate safety alerts to domestic offshore operators in an attempt to prevent similar operational accidents that may lead to injury or loss of life or environmental pollution. **MMS** is unable to receive and report weather conditions which could lead to loss of life or interruption of energy supplies to the country.

B. Lump- sum distributions of royalties paid during the shut down will confuse owners as they will question whether they have received all they are due. During the last shut down this resulted in a substantial increase in individual Indian mineral owner inquiries, requests for lease reviews, and audits. Individual Indian mineral owners questioned whether the large distribution they received when the systems were reconnected is representative of future amounts to be paid.

C. Discontinuation of on-line royalty and production reporting by solid mineral companies would continue.

D. When MMS's systems ultimately are reconnected to the Internet, the resulting influx of royalty and production data will require MMS to incur additional costs and time to process the backlog, make disbursements to account holders, and remain current on royalty processing.

18. Prior to the June 27,2003 TRO, the BLM was deemed to have adequate security, pursuant to the December 17,2001 Consent Order. Although some of BLM's systems were not disconnected because the TRO exempted "any system essential for protection against fires and other threats to life or property," the Proposed PI Order would continue the disconnection of the

Automated Fluid Minerals Support System ("AFMSS"). AFMSS supports the fluid mineral operational approval process and the inspection and enforcement process for Federal and Indian Trust Oil, Gas, and Geothermal Operations. Furthermore, AFMSS supports the Bureau's mission-critical Fluid Minerals Inspection and Enforcement Program, environmental inspections, and tracking of operational approvals such as Application for Permit to Drill, Well Completion Reports, and Sundry Notices on both Federal and Indian Trust lands and leases. AFMSS also supports an electronic interface between the BLM and the MMS to support exchange of well data to MMS and monthly well production data to BLM. These interfaces occur weekly between BLM and MMS for the thirty-one (31) field offices entering data into AFMSS. BLM Internal Users are in excess of five hundred. MMS has an additional 100 users that access AFMSS for Monthly Production Report verification purposes.

19. Prior to the June 27, 2003 TRO, the Office of Historical Trust Accounting ("OHTA") was deemed to have adequate security, pursuant to the December 17,2001 Consent Order. OHTA's systems were disconnected as a result of the TRO, and the Proposed PI Order would continue the following negative impacts:

A. OHTA staffs are based in Washington, D.C.; Albuquerque, New Mexico; and Portland, Oregon. OHTA employs contractors in Alaska, California, New Mexico, Montana, Virginia, and Washington, D.C., that are actively engaged in efforts necessary to reconcile Individual Indian Money ("IIM") and Judgment and Per Capita accounts, close Retrospective Special Deposit Accounts, and assist the Department of Justice and the Office of the Solicitor in tribal litigation. To ensure effective coordination among all parties, OHTA needs the ability to quickly and

efficiently communicate documents to all parties. Alternative document distribution methods, such as Federal Express and the Postal Service, are available and being employed, but these methods have proven to be considerably more expensive in terms of both cost and time lost compared to e-mail.

B. Available document distribution alternatives present more security risks (e.g., documents that are lost or misdelivered) to OHTA because those systems are independent of OHTA and cannot be controlled or monitored as effectively by OHTA.

C. OHTA is currently engaged in an extensive search for potential sources of third-party information. A large component of this effort involves searching the Internet for preliminary contacts. This work cannot be accomplished from OHTA offices due to the lack of Internet access. Such contacts include trade associations in oil and gas, farming and grazing, coal mining, timber and services industries, as well as museums and historical societies, state and local governments, other Federal agencies, and colleges and universities.

Description of Impacts Upon Selected Bureau Programs and Systems

20. Due to the breadth of the Proposed PI Order, additional BLM systems that were not impacted as a result of the TRO may be affected. Disconnection will adversely impact BLM's role as the lead agency for Federal Land Ownership Status and Public Land Conveyance Records. BLM relies on its land and records management systems to maintain case status for all public domain lands, which consist of approximately 270 million acres and an additional 500 million acres of subsurface minerals. These land and records management systems are used to

maintain information regarding ownership status, teasing rights, encumbrances, and other land use authorizations. These systems are web-based and are utilized both by Interior employees and the public. The public accesses approximately 5,100 reports from these systems per month and provides data to numerous private vendors who use the data in their applications. If these systems are no longer accessible via the Internet, the public would be required to visit individual BLM offices to obtain this data from the case files.

21. Due to the breadth of the Proposed PI Order, MMS systems that were not impacted as a result of the TRO may be affected. Disconnection will adversely impact MMS' ability to accomplish its mission of receiving, processing, and disbursing over $500 million in mineral revenues each month. MMS will be unable to efficiently, effectively and accurately collect, account for, verify or disburse to appropriate royalty recipients in a timely manner. MMS is responsible for the receipt, processing, and disbursement of mineral revenues on Federal and Indian leased lands. MMS accomplishes its assigned mission through delivery of reporting, accounting, and financial services. About 2,000 companies report and pay royalties to MMS each month. All such mission-critical functions are heavily reliant on the automated systems and access to the Internet. Minerals revenues are a major source of income for: (a) forty-one (41) Indian Tribes; (b) Some 20,000 individual Indian minerals owners; (c) the Federal government, and (d) thirty-eight (38) states. Disconnection will prevent MMS from being able to accomplish monthly disbursements of over $500 million in mineral revenues to States, Indians, and Treasury accounts.

22. The Proposed PI Order would adversely impact the National Business Center ("NBC") systems and programs that provide service support to numerous Department bureaus

and offices, in addition to non-Interior clients.

23. The Proposed PI Order would adversely impact the OSM. Because of the breadth of the definitions in the Proposed PI Order, the following OSM systems may be adversely affected:

A. More than 700 Technical Innovation and Professional Services ("TIPS") program users in twenty-six State Regulatory Authorities would be denied access to more than twenty state-of-the-art software applications currently being used on a daily basis (TIPS software is accessed 135 times each day, on average). Potential impacts include: (1) delayed mine permitting decisions resulting in reduced coal production and mine layoffs; **(2)** technical evaluations, designs and decisions would be less accurate and reliable; (3) mine slope failures from insufficient technical design review could result in mudslides, property loss, blocked highways, and possible fatalities; (4) impoundment failures from insufficient technical design review could result in flooding, property loss, blocked highways, or possible fatalities; and *(5)* rushed or insufficient analysis of subsidence data could result in a catastrophic mine subsidence causing structural damage, property loss, blocked highways or possible fatalities.

B. OSM maintains an Applicant/Violator System ("AVS") Office. Losing Internet access would result in the inability to provide Federal and State regulatory authorities with accurate, complete, and current information in response to permit eligibility inquiries required under section 510(c) of Surface Mining Control and Reclamation Act. OSM responds to approximately 3,000 requests annually for

AVS data evaluation checks for permit eligibility and Abandoned Mine Land program reclamation contracts. We have approximately 100 users with update capability that are responsible for AVS data entry on a daily basis via the Internet. The result of the loss of Internet connectivity would be delays in permitting approvals.

24. The Proposed PI Order would adversely impact the National Parks Service ("NPS"). Because of the breadth of the definitions in the Proposed PI Order, the following NPS systems may be adversely affected:

A. **A** shutdown of the NPS's "Parknet" website would preclude the public from accessing information about parks electronically. Parknet normally receives over one million hits per day. This would be a crucial blow to the parks at the height of the visitor season and would result in loss revenues to the National Park system and cause inconvenience to hundreds of thousands of visitors nationwide. It also includes critical information needed for visitor safety.

B. The Natural Resource Stewardship and Science directorate maintains fourteen web-enabled applications, serving both the public and NPS staff. Five *(5)* of these applications receive very high usage by Natural Resource staff and the public. Approximately 1,000 *NPS* staff use the services of these applications alone. Over 12,000 public users accessed the on-line research permitting system. To date in calendar year 2003, more than 3,000 permits have been issued and 2,360 research accomplishment reports processed using these web services. In addition, 1,560 pesticide use proposals supporting integrated pest management have been

processed through the IPM on-line system.

C. Since January of 2003, a weekly average of 26,100 public users accessed the NatureNet website.

D. The transmission of Geographic Information System data for parks adjacent to Indian reservations could be impacted.

E. Disruption of Internet connections impedes NPS's ability to communicate with the public and respond to inquiries.

F. Disruption of Internet access could shut down the NPS reservation system as well as the research permit system.

G. Disruption of Internet connections impedes NPS's ability to fully utilize its Park Maintenance Information System used in formulating budgets for and tracking maintenance, construction, and recreation fee projects.

25. The Proposed PI Order would adversely impact the Fish and Wildlife Service ("FWS"). Because of the breadth of the definitions in the Proposed PI Order, the following FWS systems may be adversely affected:

A. Scientists at the National Fish and Wildlife Forensics Laboratory could not complete casework because certain sources of information used in analyzing evidence are only available via the Internet.

B. Throughout the year, Division of Migratory Bird Management biologists fly surveys through the breeding ground areas of the United States and adjacent countries. These surveys are critical to the effective management of migratory bird species. More important, is the safety of the people flying the surveys. The

pilots rely on access to the Internet for up to the minute weather information covering their flight survey areas. In addition, they use the Internet to obtain customs information when flying between countries. These surveys also require them to fly around major cities, airports, and other critical sites that are often restricted when national security threats are elevated. Flight restrictions can change with short notice. Our pilots use the Internet to check for flight restrictions **prior** to flying a survey.

C. The National Wildlife Refuge System Visitation may be affected. Many of the Refuge System's forty (40) million visitors per year rely on web pages (both national and regional level **as** well as individual sites hosted by individual field stations) to get driving directions, learn about activities and special events offered, and understand site-specific regulations before making a visit.

D. The National Wildlife Refuge System Volunteers system may be affected. Nearly 35,000 people (ten times the number of agency employees in the Refuge System) assist with a wide diversity of activities, contributing about twenty (20) percent of the total hours of work that occur on our field stations. The Internet provides a primary recruitment tool for volunteers and email is a major communication tool for keeping volunteers informed of activities and needs.

26. Disconnection would adversely impact the U.S. Geological Survey ("USGS"). Because of the breadth of the definitions in the Proposed PI Order, many USGS systems may be adversely affected, including the National Spatial Data Infrastructure and the National Biological Information Infrastructure, which are widely used and relied on to provide geospatial and

biological information to other government agencies, external scientists, and the public. Without internet access, there will be no real-time dissemination of information about floods, droughts, streamflow, and water quality collected through the approximately 8,000 USGS gauging stations and monitoring wells nationwide. Data will be unavailable, or severely hampered, for first responders, cooperators and the public. This includes data used by the National Weather Service for prediction of large floods and local flash floods and data used by other public agencies on a daily basis to provide drinking water, operate hydroelectric dams, irrigate farms, manage transportation networks and protect public health and safety.

Departmental Scans

27. Beginning in December 2002, the OCIO commenced utilizing an Interior Department contractor to scan Interior Department's systems for the vulnerabilities identified on a list commonly known as the "SANS/FBI Top 20 List." These are widely recognized in the IT security world as the twenty (20) most critical Internet security vulnerabilities. Current information about the SANS/FBI Top 20 List appears at ww.sans.org/top20. The OCIO has continued the SANS/FBI Top 20 List scanning on a monthly basis and has provided copies of reports, raw data, and relevant e-mails to Government counsel. I understand these materials have been provided to the Special Master by Government counsel.

I declare under penalty of perjury that on this date the foregoing is true and correct to the best of my knowledge.

W. Hord Tipton
Chief Information Officer

Dated: July 25 2003
4:33 pm

CERTIFICATE OF SERVICE

I declare under penalty of perjury that, on July 25,2003 **I** served the foregoing *Interior Defendants 'Motionfor Leave to File Supplemental Opposition to Plaintiffs' Motionfor a Preliminary Injunction* and *Interior Defendants' Supplemental Opposition to Plaintiffs' Motion for a Preliminary Injunction* **by** facsimile in accordance with their written request of October 31, 2001 upon:

Keith Harper, Esq.
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
(202) 822-0068

Dennis M Gingold, Esq.
Mark Kester Brown, **Esq.**
607 - 14th Street, NW
Box **6**
Washington, D.C. 20005
(202) 318-2372

Per the Court's Order **of** April 17,2003, by facsimile and by U.S. Mail upon:

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

By U.S. Mail upon:

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

By facsimile and U.S. Mail:

Alan L. Balaran, Esq.
Special Master
1717 Pennsylvania Avenue, N.W.
13th Floor
Washington, D.C. 20006
(202) 986-8477

K. P. Kingston

Kevin P. Kingston