IN THE
UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et. al., on her own behalf and on behalf of all persons similarly situated,	)	
Plaintiffs,	)	
v.	)	**Civil Action Case No. 1:96CV01285 (RCL)**
GALE NORTON, et al.,	)	
Defendants.	)	

PLAINTIFFS' CONSOLIDATED MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

I. INTRODUCTION

Interior information technology systems ("IT Systems") that house or access Individual Indian Trust data ("Trust Data"), by trustee-delegates' own admission, are presently insecure and, therefore, must be disconnected from the Internet **and** shut down to stop the irreparable harm that plaintiffs continue to endure.

On April 8, 2005, the trustee-delegates filed with this Court *Defendants' Notice to the Court Regarding Inspector General's "Notification of Potential Finding and Recommendation" with Respect to Information Technology Systems* ("Defs' Notice"). Defs' Notice selectively restates findings made by the Inspector General[1] that confirm plaintiffs' charges that the trustee-

[1] The trustee-delegates and their counsel, as a matter of practice, withhold incriminating information from this Court and plaintiffs. Such deception through material omission includes without limitation carefully redacted quarterly reports, and edited declarations and certifications that conceal the complete lack of knowledge of the declarants and fail to comply with local and federal rules. Recently, this Court did not permit such arrogation of its authority with respect to a similar attempt to withhold declarations from this Court and plaintiffs, and this Court ordered them to comply with local rules; *See, e.g.*, February 7, 2004 Memorandum Opinion at 2 ("But the defendants have filed with

delegates and their counsel unlawfully have exposed, and continue to expose, critical trust records to loss, destruction, and corruption and that they mislead, and have misled, this Court and the Court of Appeals regarding the security of IT Systems that house or access Individual Indian Trust Data ("Trust Data").[2] The excerpt from the Inspector General findings is damning. It states in pertinent part:

> Given the **poor state of network security** at [REDACTED] and the **weak access controls** we encountered on many systems, it is safe to say that **we could have easily compromised the confidentiality, integrity, and availability of the identified Indian Trust data** residing on such systems.[3]

---

the Court and served upon the plaintiffs only the redacted copies of the declarations of Michael Hackett and Nina Sisquieros, which, as the plaintiffs correctly argue, is inconsistent with LCvR 5.1(j)(1). A party must file an appropriate motion and obtain an order from the Court in order to file documents under seal."). This Court should do so again now where as here the information is unquestionably critical to the trustee-delegates' ongoing malfeasance in their management and administration of the Individual Indian Trust.

[2] *See, e.g.*, Plaintiffs' Exhibit 1, Brief for Appellants, dated April 6, 2004 at 14 ("[S]ystem[s] had been reconnected because the Special Master had agreed that [] [they] were secure or did not house or access IITD."); at 15 ("On August 11, 2003, a variety of Interior officials provided detailed and comprehensive certifications, under penalty of perjury, that specific systems either were secure from internet access by unauthorized users or did not house or provide access to IITD.); at 34 ("Cason emphasized that Interior has now 'driven the vulnerabilities down close to zero for our perimeter security at the Department overall.'"); at 34-35 ("Cason added that the agency has 'taken a lot of measures to basically bulletproof the [network infrastructure] from providing any access to a hacker ...."); at 43 ("A September 12, 2003 GAO Report .... lends no support to the proposition that unauthorized access through the internet presents any imminent danger to the integrity of individual Indian trust data."). *See also* Plaintiffs' Exhibit 2, Reply Brief for Appellants, dated June 21, 2004, at 22 ("Significantly, the record shows that, ... Interior has now 'driven the vulnerabilities down to close to zero for our perimeter security at the Department overall.'").

[3] Defs' Notice at 2 (emphasis added). Notably, the trustee-delegates and their counsel will not even cite to the specific page of the Inspector General's ("IG") excerpted findings and refuse to disclose to this Court and to plaintiffs the IG's report in its entirety, making it impossible for this Court and plaintiffs to assess the nature and scope of the material vulnerabilities found by the Inspector General. Parenthetically, it is clear that this strategy of selective disclosure is designed to deprive this Court of a sufficient record of current insecurity – a record that is required to sustain a preliminary injunction on appeal – to further undermine this Court's ability to protect plaintiffs from the continuing malfeasance of the trustee-delegates and their counsel. But, they are wrong. As discussed more fully below, an evidentiary hearing would allow this Court and plaintiffs to overcome this particular obstruction.

Conspicuously, Defs' Notice does not disclose when the IG conducted its tests and it conceals the date that the IG first disclosed such problems to Norton and her counsel. It states only that "the document is dated April 6, 2005." Defs' Notice at 1-2. Furthermore, the excerpted IG findings do not disclose whether, or the extent to which, the vulnerabilities have been corrected (and, if so, when

Because it is indisputable that the "poor state of network security" creates an imminent risk of irreparable injury[4] – injury that necessarily occurs with the loss, destruction, corruption, and continuing degradation of Trust Data – plaintiffs request that this Court disconnect from the Internet **and** shut down each information technology system which houses or access individual Indian trust data to protect plaintiffs against further injury to their interests, injury that is certain if a temporary restraining order ("TRO") and effective preliminary injunction are not entered.

This Court's authority to enter the proposed TRO and a preliminary injunction to protect plaintiffs from further irreparable injury is without question. The law is settled and is set forth clearly by the Court of Appeals in *Cobell XII*.[5] The *Cobell XII* Court noted with approval this Court's succinct statement of the trustee-delegates' fiduciary duty in *Cobell XI*[6] as well as the irreparable harm a breach of this duty would cause plaintiffs. Further, the *Cobell XII* Court restated this Court's conclusion that "'Interior's present obligation to administer the trust presents sufficient grounds for finding that Plaintiffs will be irreparably injured.'"[7] Dispositively, *Cobell XII* dismissed the trustee-delegates' contention that this Court lacks authority to ensure that Trust Data is preserved and expressly held that **no** jurisdictional constraints exist where, as here, Trust Data is in imminent risk:

> We further hold that the district court's jurisdiction properly extends to security of Interior's information technology systems ("IT") housing or accessing IITD,

---

they were corrected) or if, and when, they will be corrected. Nor does it include any assessment of the impact such vulnerabilities have had, and continue to have, on the ever-degrading integrity of Trust Data.

[4] *See, e.g., Cobell XI,* 310 F.Supp.2d at 96 n.27 ("Interior's present obligation to administer the trust presents sufficient grounds for finding that Plaintiffs will be irreparably injured.").

[5] *Cobell v. Norton,* 391 F.3d 251, *256 (D.C. Cir. 2004) ("*Cobell XII"*) ("[W]e hold that the district court possessed authority on remand from *Cobell VI* to issue a preliminary injunction regarding IT security.").

[6] *Id.* at 310 F.Supp.2d at 96 n. 27.

[7] *Cobell XII,* 391 F.3d at *253.

because the Secretary, as fiduciary, is required to maintain and preserve IITD.[8]

As *Cobell XII* noted when it remanded the IT security matter to this Court for an evidentiary hearing, then, as now, "the **only** issue before the district court [i]s the security of IT systems housing and accessing IITD, ..."[9] Thus, there is no issue with respect to the nature and scope of this Court's authority. None. That means that when this Court finds that IT security is inadequate, it may fashion whatever remedy it deems appropriate, including, without limitation, an order that compels the trustee-delegates to disconnect all such systems from the Internet and to shut down all information technology systems which house or access individual Indian trust data. For purposes of the TRO, the factual issue is resolved without the need for an evidentiary hearing. The admission filed with this Court on April 8 and the recently adduced deposition testimony of Interior's Chief Information Officer are sufficient. For a preliminary injunction, however, an evidentiary hearing is required to demonstrate the current state of gross insecurity.

As this Court is well aware, throughout this litigation, the trustee-delegates and their counsel have misled this Court and plaintiffs in their quarterly reports, declarations, and certifications to coverup the inadequacy of IT security and, by doing so, they consciously have violated Court orders that were entered to ensure the integrity of Trust Data and other trust records, including email. The trustee-delegates' willful failure to obey such orders has ensured the degradation of the integrity of Trust Data to levels that are now unquantifiable, rendering futile the complete and accurate accounting of all funds that has been declared for each trust beneficiary.

In addition, as this Court has acknowledged, for several years in this litigation, plaintiffs were not permitted to take discovery that would have allowed them to prove to the satisfaction of

---

[8] *Id.* at *253-*54. Emphatically, the *Cobell XII* Court rejected Norton's claim that this Court's authority is limited and for Norton's benefit the Court of Appeals clarified the meaning of its decision in *Cobell VI:*

> [T]he court did not limit the district court's authority to exercise its discretion as a court of equity in fashioning a remedy to right a century-old wrong or to enforce a consent decree, *see Frew v. Hawkins,* 540 U.S. 431, 124 S.Ct. 899, 905 (2004).

Cobell XII at *257.

[9] *Id.* at *258 (emphasis added).

the Court of Appeals the scope of the trustee-delegates' material misrepresentations and failures regarding IT security, making it impossible for plaintiffs to discover and demonstrate the gross insecurity of IT systems that house or access Trust Data. Such constraints – in conjunction with the former special master's decision to permit the trustee-delegates to reconnect to the Internet knowingly insecure systems,[10] relying solely on the hollow promise of Jim Cason that the trustee-delegates eventually would bring their insecure systems into compliance with OMB Circular A-130, Appendix III – provided ample opportunity for these unprincipled trustee-delegates and their counsel to exploit the discovery constraints imposed on plaintiffs and further obscure and obfuscate the on-going imminent risk to the degrading integrity of Trust Data.[11] At the same time, with no concern about the consequences of their misconduct, they misled this Court and the Court

---

[10] Within a year after entry of the December 17, 2001 Order, the former special master allowed Interior to reconnect to the Internet 95% of its IT Systems notwithstanding the fact that such systems that housed and accessed Trust Data continued to be insecure at the time he allowed reconnection. *See, e.g., Cobell IX*, 310 F.Supp.2d at 82. These decisions were made without prior consultation with plaintiffs' counsel and they placed plaintiffs in an untenable situation. Specifically, the admissions made by the trustee-delegates on December 17, 2001 and the prior findings of the master regarding the insecurity of IT Systems became dated once he allowed insecure systems to be reconnected because the master made no new findings and did not restate the nature and scope of the existing vulnerabilities at the time he approved reconnection. Instead, the master trusted Cason et al. to that which they have never done in this litigation: tell the truth and discharge their trust duties.

Because plaintiffs could take no discovery and could not examine the trustee-delegates' certifiers and declarants, plaintiffs had to rely entirely on dated government reports and were denied the ability to proffer current evidence of insecurity to overcome the trustee-delegates' false and materially misleading certifications and declarations to the contrary. Further, because the trustee-delegates thwarted the master's monitoring and oversight – to coverup material vulnerabilities in IT security – they ensured that no current evidence would be available to meet the evidentiary burden that must be met to sustain an injunction on appeal. Simply put, they gamed the master and, thereby, further undermined the integrity of these proceedings. As a result of the trustee-delegates' unethical gamesmanship, plaintiffs have been compelled to suffer relentless irreparable injury and Trust Data has degraded an additional three and one-half years since the December 17, 2001 confession of systemic insecurity.

[11] The trustee-delegates' open disdain for the harm that they and their counsel inflict on individual Indian trust beneficiaries is further evidence of on-going malfeasance that must be stopped. Norton and her counsel ignore the fact that their conduct must be judged not by the marginal standards that they are accustomed to, the standards of lobbyists and influence peddlers, willfully ignorant laymen, dishonest defense counsel, and incompetent trust counsel. Rather, the trustee-delegates are judged by only one standard – "'**the most exacting fiduciary standard**[], ...'" *Cobell XII*, 391 F.3d at *257 (emphasis added) (quoting *Seminole Nation v. United States*, 316 U.S. 286, 297 (1942).

of Appeals in their filing of false and materially misleading declarations and certifications that claimed their IT systems were secure when they were not.

It is no coincidence that the IG findings were briefly mentioned[12] to this Court and plaintiffs only after this Court restored plaintiffs' discovery rights on February 8, 2005. Unfortunately, however, the trustee-delegates and their counsel continue their bad faith defense of this litigation. They continue to coverup the nature and scope of their deception and their conscious violations of Court orders. That is, as discussed more fully below, they continue to withhold incriminating evidence, including the IG report itself and similar such reports. They obstruct the discovery process by instructing witnesses to refuse to answer deposition questions (the answers to which would further demonstrate the insecurity of IT systems that house or access Trust Data) and they refuse to allow witnesses to be deposed on consecutive days, obviously to ensure that they are well-coached to continue the deception they practice on this Court.[13]

Nonetheless, in accordance with the guidance provided by *Cobell XII*, the IG findings alone demonstrate that Trust Data presently are in imminent risk of loss, destruction, and corruption. This admission justifies issuance of a TRO to ensure that the *status quo* is maintained – no matter how bad that is – and to ensure that the irreparable harm the trustee-delegates knowingly inflict on plaintiffs is not compounded, pending a preliminary injunction hearing and the fashioning of more comprehensive relief.

Once the TRO is entered and all insecure computers are shut down – not merely disconnected from the Internet – the trustee-delegates should be compelled to produce Rule

---

[12] In bad faith, the trustee-delegates and their counsel continue to withhold from this Court the IG findings noticed as well as other documents, memoranda, and findings that describe the nature and scope of the inadequate security of all relevant IT Systems. Thus, only one paragraph of the IG findings is disclosed.

[13] By separate motion, plaintiffs will file a motion to compel so that this Court may address the discovery abuse practiced by the trustee-delegates and their counsel.

30(b)(6) witnesses to testify in an evidentiary hearing[14] to enable plaintiffs to demonstrate through cross-examination, that each IT system that houses and accesses Trust Data has been, and continues to be, insecure. Such systems include each such system that is owned, controlled, or operated by Interior and each such system that is owned, controlled, or operated by Interior's agents and contractors. With this current record of inadequate security, deception, and conscious violations of orders, the preliminary injunction can be affirmed on appeal.

II. PROCEDURAL HISTORY

On December 5, 2001, this Court granted plaintiffs' motion for a TRO that required the trustee-delegates "immediately [to] disconnect from the Internet" all IT systems housing or accessing Trust Data.[15] To avoid a preliminary injunction, on December 17, 2001, this Court entered an order proposed by the trustee-delegates and opposed by plaintiffs,[16] admitting to the insecurity of Trust Data, admitting to the urgency that exists to correct the pervasive vulnerabilities in IT security, and conceding that "Interior shall not reconnect any information technology system to the Internet without the concurrence of the Special Master," who "shall verify compliance with

---

[14] Because of the sensitivity of IT security issues and the possibility that whatever inadequate security exists might be compromised if disclosures are made in a public hearing, this Court may prefer to hold a sealed evidentiary hearing to afford the trustee-delegates a brief period of time to prove that any sealed information should remain sealed. The burden of proof is the trustee-delegates' alone.

To enhance the likelihood of candid testimony, it is essential that this Court order the immediate production of **all** relevant reports, risk assessments, memoranda, and other documents (in draft and final form) – whether prepared by Interior officials, other government agencies, or third parties – that shed light on the security (or insecurity) of each IT system that houses or accesses Trust Data. This is particularly important because the trustee-delegates' hand-picked declarants and certifiers make representations to this Court with no knowledge as to whether their representations are true. And, defense counsel conduct no due diligence before filing such misleading declarations and certifications with this Court.

[15] *Cobell v. Norton*, 274 F.Supp. 2d 111, 113 (D.D.C. 2003) ("*Cobell IX*").

[16] Plaintiffs objected because they did not believe that the order would ensure the security and integrity of Trust Data. Unfortunately, plaintiffs' fears were warranted.

this Consent Order ...."[17] Plaintiffs' concerns about the inadequacy of the December 17th Order and the master's reliance on the good faith of Cason proved to be true. In April 2003, the trustee-delegates, Cason, and their counsel consciously violated the December 17th Order and obstructed penetration testing being conducted by the former Special Master's experts to verify the effectiveness of security enhancements.[18]

On June 26, 2003 – more than seven years after this action in equity was filed – plaintiffs again were forced to file a motion for a TRO and preliminary injunction to try to protect whatever remained of the integrity of Trust Data that continued to degrade through the trustee-delegates' conscious violations of the December 17th order. Plaintiffs' motion again requested this Court to disconnect from the Internet all Interior systems and computers that housed or accessed Trust Data until the former master certified that the systems and computers, in fact, were secure. A TRO was entered that was modified to accommodate certain requests made by the trustee-delegates and their counsel, requests that were granted because this Court (again) relied on representations of the trustee-delegates, Cason, and their counsel that they would work out whatever disagreements they had had with the former master. To no surprise, their representations were false. Instead of resolving the issues they had with the master, they asked this Court and the Court of Appeals to disqualify the master from any further role in these proceedings.[19]

It is under these circumstances that this Court held a preliminary injunction hearing on July 28, 2003 at the conclusion of which it entered a preliminary injunction that by its terms stayed the December 17th Order – injunctive relief that the trustee-delegates and their counsel successfully evaded a full year and one-half when they persuaded this Court to rely on their good faith and enter the so-called Consent Order in lieu of an injunction. Thus, from December 17, 2001 to July 28, 2003, an additional year and one-half of irreparable harm and degradation of Trust Data occurred.

---

17 *Id.* at 114.

18 *Id.* at 114-24.

19 *See, e.g., id.* at 124.

The July 28th injunction again ordered the trustee-delegates to disconnect from the Internet all IT systems that house or access Trust Data with two exceptions: (1) the exception proposed by plaintiffs for systems that are "essential for protection against fires or other threats to life or property" and (2) all other systems that the trustee-delegates certified as secure.[20]

On March 15, 2004, this Court entered yet another preliminary injunction because the trustee-delegates consciously violated this Court's July 28, 2003 IT injunction in their filing of "procedurally and substantively defective" certifications.[21] The incorrigible trustee-delegates appealed this injunction as well and the Court of Appeals consolidated that appeal with their appeal of the July 28, 2003 injunction. The March 15th injunction was stayed pending a decision on the merits and, ultimately, it was vacated because no evidentiary hearing was held prior to its issuance. As a result, the trustee-delegates now, and at all times relevant to this litigation, have done, and continue to do, nothing meaningful to ensure the security of Trust Data housed in or accessed by their IT systems and Third-Party IT Systems. Thus, such systems continue to be untrustworthy and the integrity of the Trust Data housed in or accessed by such systems continues to degrade, vitiating the data's evidentiary value and rendering the declared accounting an exercise in futility.

Individual Indian trust beneficiaries cannot afford more corruption of data, more

---

[20] *Id.* at 135-36.

[21] *Id.* at 100-01. Notably, the injunction, itself, articulated only a Rule 11 standard; it did not require actual knowledge of the declarants and certifiers under 28 USC § 1748 or LCvR 5.1(h)(2). The trustee-delegates fully exploited this loophole (and they continue to do so in their quarterly reports and declarations filed with this Court). That is not to say, however, that the certifications were not knowingly false and materially misleading at the time they were made. They certainly were. However, no evidentiary hearing was held to demonstrate the mendacity of the trustee-delegates and their counsel. The absence of such a hearing – combined with what the Court of Appeals considered to be stale evidence of insecurity – allowed the trustee-delegates to persuade the Court of Appeals to vacate the injunction. *See Cobell XII*, 391 F.3d at *259-*61. Indeed, because this Court would not permit discovery, *Cobell XII* noted that this Court too had found that plaintiffs did "not demonstrate[] to the satisfaction of the Court that the reconnected systems are *not* presently secured from unauthorized access." *Cobell IX*, 274 F.Supp. 2d at 132 (italics in original). This finding that plaintiffs' did not demonstrate the current insecurity of Interior's IT Systems was sufficient to vacate the injunction. *See Cobell XII*, 391 F.3d at *261-*62. It is imperative that this not happen again.

destruction of critical records, more losses of trust funds, more broken promises, more undue delays. Time is of the essence.

III. A BRIEF HISTORY OF INTERIOR'S MISREPRESENTATIONS REGARDING THE SECURITY OF INDIVIDUAL INDIAN TRUST DATA

During and after the second contempt trial, trustee-delegates attempted to curry favor with this Court in order to forestall this Court's contempt decision. This doomed effort led to various admissions that were remarkable only for their truthfulness – however fleeting. To wit, on January 16, 2002, the trustee-delegates admitted that the "security of individual Indian trust data is inadequate. . . . the Department is keenly aware that there are weaknesses and shortcomings."[22] Defendants continued to report significant deficiencies in the security of individual Indian trust data through August 1, 2002.[23]

On September 17, 2002, this Court found that: "The Department of Interior has demonstrated that **neither its officials nor its attorneys can be trusted to provide the Court with accurate information** regarding the agency's efforts to ensure the security of its computer systems."[24] Following this Court's finding that defendants had deliberately misled this Court with respect to the status of information technology security, defendants returned to their practice of filing false and materially misleading information regarding the security of individual Indian trust data. Plaintiffs will not burden this Court with a full recitation of defendants' false certifications and violations of Court orders and instead incorporate by reference, as if restated in its entirety

---

[22] *See* Defendants' *Status Report to the Court Number Eight* (dated January 16, 2002) at 48-49.

[23] *See e.g.* Defendants' *Status Report to the Court Number Nine* (dated May 1, 2002) at 12 ("Recent reviews have documented extensive weaknesses in the security measures associated with the IT systems housing or providing access to individual Indian trust data.") and Defendants' *Status Report to the Court Number Ten* (dated August 1, 2002) at 8 ("Recent reviews have documented extensive weaknesses in the security measures associated with the information technology systems housing or providing access to individual Indian trust data (IITD).").

[24] *Cobell v. Norton*, 226 F.Supp.2d 1, 129-130 (emphasis added).

herein, plaintiffs' January 13, 2004 contempt motion.[25] It is sufficient for purposes here to note that trustee-delegates reverted to their standard practice of displaying a complete lack of candor in representations to this Court following the issuance of the September 17, 2002 decision. As this Court is well aware, on April 24, 2003, the Special Master reported to the Justice Department that a security scanning test on OSM servers at the Interior Department revealed that there existed a vulnerability in the system, allowing individual Indian trust data to be accessible from the Internet. The Special Master submitted a plan for further testing in accordance with protocols to which the Special Master and the Interior Department had previously agreed. However, trustee-delegates and their attorneys refused any further testing and demanded that the Special Master be disqualified. The trustee-delegates adopted the position that, under the December 17, 2001 consent decree, once the systems were reconnected to the Internet, no further testing was required, a position this Court noted was inconsistent with its own understanding of the Consent Order. Nevertheless, since this Court's July 28, 2003, Preliminary Injunction and the trustee-delegates subsequent appeal of that order, the plaintiffs, and this Court, have had to rely entirely on the trustee-delegates' own representations regarding trhe safety of individual Indian trust data located on their trust systems. Such reliance has only further endangered trust assets and beneficiaries.

On February 2, 2004, trustee-delegates reported that 99.3% of all vulnerabilities had been eliminated:

> The scanning involved testing IT equipment at the perimeter of Interior's networks where Internet interface occurs. Interior's scanning efforts are designed to identify potential vulnerabilities that may be exploited in a manner that could result

---

[25] *Plaintiffs' Motion for an Order to Show Cause Why the Department of the Interior, Interior Secretary Gale Norton, and Her Senior Managers and Counsel, Should Not Be Held in Civil and Criminal Contempt for Violating Court Orders, Including the Temporary Restraining Order and Preliminary Injunction Entered to Protect Trust Data and Assets*, filed January 13, 2004. This contempt motion is a veritable compendium of defendants' and their senior managers' and counsel's false representations to this Court regarding the security of individual Indian trust data. And, while this motion was withdrawn at the insistence of defendants who threatened to withdraw from mediation if plaintiffs sought to enforce this Court's orders, it is still relevant in that it further corroborates this Court's finding that "neither [DOI] officials nor [their] attorneys can be trusted to provide the Court with accurate information." *Cobell v. Norton*, 226 F.Supp.2d 129-130. Plaintiffs by separate notice will fully inform this Court of the status of mediation.

> in unauthorized access to other computer equipment on the host network. Other scanning efforts may be employed to identify and evaluate potential vulnerabilities on computers hosted on the internal network of each agency.
>
> The number of computer hosts with potential high risk vulnerabilities continued to be reduced during this reporting period. From an initial baseline of 953 potential Department vulnerabilities (December 2002), the most recent scanning report found 7 potential vulnerabilities after the elimination of false positives, for an overall reduction of 99.3%.[26]

Trustee-delegates' fiction continued in their seventeenth status report to the Court: "Interior continued testing its wide area networks . . . . In the March 2004 report, there were no high-risk SANS/FBI Top 20 vulnerabilities identified in the perimeter telecommunications equipment exposed to the Internet."[27] The seventeenth report continued to state that: "none of the remaining [system vulnerabilities] pertain to the potential for unauthorized access from the Internet to IITD."[28] The eighteenth report (August 2, 2004) and the nineteenth report (November 1, 2004) made similar representations that the systems which house or access individual Indian trust data were secure.[29]

On February 1, 2005, trustee-delegates completed their twentieth report to the Court. Again, according to the allegations of the trustee-delegates: "Interior continued testing Internet-accessible systems . . . [but,] no hosts were found to have vulnerabilities listed."[30] In addition, trustee-delegates reported for the first time that the Office of the Inspector General "began unannounced penetration testing exercises for systems connected to the Internet."[31] The status

---

[26] *See* Defendants' *Status Report to the Court Number Sixteen* (dated February 2, 2004) at 6 (emphasis added).

[27] *See* Defendants' *Status Report to the Court Number Seventeen* (dated May 3, 2004) at 5.

[28] *Id.* at 7.

[29] *See e.g.* Defendants' *Status Report to the Court Number Eighteen* (dated August 2, 2004) at 5 ("During this period, no hosts were found to have vulnerabilities") and Defendants' *Status Report to the Court Number Nineteen* (dated May 3, 2004) at 4 ("For the second consecutive reporting period, no hosts were found to have vulnerabilities").

[30] *See* Defendants' *Status Report to the Court Number Twenty* (dated February 1, 2005) at 7.

[31] *Id.* at 4.

report provided no information on the results of the penetration testing and this Court and plaintiffs were left with the impression that "no hosts were found to have vulnerabilities listed."[32] This, of course, is directly contradicted by the trustee-delegates' April 8, 2005 notice which reveals a "poor state of network security . . . and [] weak access controls . . . on many systems."[33] Indeed, such systems are so insecure that the Inspector General "could have **easily compromised** the confidentiality, integrity, and availability of the identified Indian Trust data residing on those systems."[34] It is simply not possible to reconcile their statement that no vulnerabilities remain in their systems with their April 8, 2005 notice. Unfortunately, despite the lapse of four years, the safety of individual Indian trust data on the computer systems is no greater than when Dominic Nessi, then-BIA Chief Information Officer, reported in April 2001, that the network on which individual Indian trust data was located could be "breached by a high school kid."[35]

In short, trustee-delegates and their counsel have a rich history in defrauding this Court with respect to the security of information technology systems which house or access individual Indian trust data. Their continuing representations to the Court that such systems are adequately secured is a complete and utter fabrication to (again) forestall injunctive relief. This Court should consider carefully that the recent April 8, 2005 notice was filed on the eve of plaintiffs' deposition of Mary Kendall-Adler, Deputy Inspector General, and that defendants vigorously objected to Ms. Kendall-Adler's deposition in its entirety.[36] It is beyond peradventure that the deposition of

---

[32] *See* Defendants' *Status Report to the Court Number Twenty* (dated February 1, 2005) at 7.

[33] *See Defendants' Notice to the Court Regarding Inspector General's "Notification of Potential Finding and Recommendation" with Respect to Information Technology Systems* at 2, filed April 8, 2005.

[34] *Id*. (emphasis added).

[35] *See* Katherine McIntire Peters, Trial of Troubles, GOVERNMENT EXECUTIVE, April 1, 2001 at 100.

[36] *See Defendants' Motion for a Protective Order Regarding Plaintiffs' Notices of Deposition of James Cason, Mark Limbaugh, Jeffrey Jarrett, Timothy Vigotsky, Kathryn Clement, Steven Williams, Donald Murphy,* **Mary Kendall Adler**, *William Ragsdale, Francis Cherry, Jr., Robert Doyle, Norma Campbell, Regina Lawrence, Ethel Abeita, Thomas*

Kendall-Adler would have elicited such damning information. Moreover, it is the imminent threat of such heretofore concealed information being revealed during the course of that deposition that provided the impetus to file the April 8 notice, rather than any sense of ethical responsibility on the part of trustee-delegates counsel. It is a despicable and pathetic practice of defendants and their counsel that such critical information is only revealed when a deposition is imminent, rather than when such information is first uncovered.

IV. STATUTORY, REGULATORY GUIDANCE FOR THE SECURITY OF INFORMATION TECHNOLOGY SYSTEMS

Appendix III to OMB Circular A-130 requires that agencies implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in their information technology systems. *See generally* Plaintiffs' Exhibit 3 (OMB Circular, Appendix III). "Adequate Security" is defined therein as:

> security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Id. at A(2)(a). Among other things, OMB Circular A-130, Appendix III assigns responsibility to the National Institute of Standards and Technology to promulgate standards and guidance with respect to security federal information technology systems. *Id.* at A(4)(a). All federal agencies – with certain exceptions, not including the Department of the Interior – are to comply with such guidance. *Id.* at A(3).[37] The core principles and direction contained in OMB Circular A-130 were

---

Kerstetter, and Wendall Galvan, filed January 19, 2005.

[37]

> Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.
> Each agency's program shall implement policies, standards and procedures

reiterated and reconfirmed by the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.[38]

In May 2004, NIST finalized Special Publication 800-37 entitled: "Guide for the Security Certification and Accreditation of Federal Information Systems." *See* Plaintiffs' Exhibit 4. Interior represents its "major goal . . . is to achieve C&A [certification and accreditation process] of its IT systems" in accordance with NIST 800-37 and OMB Circular A-130, Appendix III.[39] Because Interior describes such compliance as the "major goal of Interior's IT security program," plaintiffs will necessarily discuss the certification and accreditation process at some length. NIST 800-37 describes the C&A process as follows:

Security accreditation is the official management decision given by a senior agency

---

> which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives.

Id.

[38] *See* 35 USC 44 § 3543 (charging NIST with developing and promulgating guidance); §3544 requires that heads of agencies "shall" 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.

Id.

[39] *See e.g.* Defendants' *Status Report to the Court Number Twelve* at 13:

> Interior's CIO Security Officer continued work on a Departmental certification and accreditation (C&A) process based upon the new NIST Special Publication 800-37. Two dedicated contractors are supporting this effort. The major goal of Interior's IT security program is to achieve C&A of its IT systems in full compliance with OMB Circular A-130, Appendix III.

See also Defendants' *Status Report to the Court Number Eleven* at 14. This is consistent with NIST 800-37 which instructs that the "guidelines provided in [NIST 800-37] are applicable to all federal information systems other than those systems designed as national security systems as defined in 44 U.S.C., Section 3542." *See* Plaintiffs' Exhibit 4 at 6.

> 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. Required by OMB Circular A-130, Appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. **By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.**
>
> **It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk based decisions on whether to authorize operation of those systems**. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. **The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision**.

See Plaintiffs' Exhibit 4 at 1 (bold emphasis added, underline original). Simply put, certification consists of a comprehensive assessment of the information systems. Such an assessment provides the "factual basis" by which an authorizing official renders an accreditation decision accepting accountability "for any adverse impacts to the agency if a breach of security occurs." *Id*.[40] As stressed in NIST 800-37, "It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk based decisions on whether to authorize operation of those systems." *Id*.

Along those lines, NIST-37 "presume[s] that responsible agency officials understand the

---

[40] *See also id.* at 4 ("Security *accreditation* 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.") (footnotes omitted, emphasis added)).

risks and other factors that could adversely affect their missions." *Id.* at 4. To be sure, the "assessment of risk and the development of system security plans are two important activities . . . that directly support security accreditation and are required by FISMA and OMB Circular A-130, Appendix III." *Id.* at 4.

Ultimately, there are three types of accreditation decisions that can be rendered: (1) authorization to operate; (2) interim authorization to operate; or (3) denial of authorization to operate. *Id.* at 19. In order, an authorization to operate results from an assessment "that the risk to agency operations, agency assets, or individuals is acceptable." *Id.* An interim authority to operate might issue if the authorizing official determines "that the risk to agency operations, agency assets or individuals is unacceptable, but there is an overarching mission necessity to place the information system into operation or continue its operation." *Id.* at 20. Importantly, the duration for an interim authorization to operate should be commensurate with the risk to the agency, assets or individuals, but "mission critical or high-impact systems . . . **should not be operating with significant security vulnerabilities** requiring extended remediation time." *Id.* at 20 n. 32 (emphasis added). In addition, this limited approval requires "specific terms and conditions and acknowledges greater risk to the agency for a specified period of time. The terms and conditions . . . convey limitations on information system operations." *Id.* at 20. Finally, a denial of authorization to operate will result if the "authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable. *Id.* at 21. In the event a denial of authorization to operate is issued, the "information system is not accredited and **should not be placed into operation**. If the information system is currently in operation, all activity should be halted." *Id.* (emphasis added). To be clear, the denial of authorization to operate is not limited to access to the Internet; rather, such a denial requires that the system should be entirely shut down and remain inoperable until the control deficiencies have been remedied.

FISMA "provide[s] a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and

assets." *See* 35 USC 44 § 3541(1). And, while it left the decision of whether or not to operate information technology systems with agency officials, it did not do so without prescribing extensive risk management analysis and development of system security plans prior to making a decision to operate a particular system. Indeed, FISMA and NIST require that systems not be operated if adequate security controls – commensurate with the risk to assets and individuals – are not in place. In this case, Interior has been operating information technology systems – and, reconnecting such systems to the Internet – by employing a sham certification and accreditation process. Plaintiffs discuss this sham certification and accreditation process below.

V. INTERIOR'S CERTIFICATION AND ACCREDITATION PROCESS

NIST 800-37 was finalized in May 2004, but as early as November 2002 trustee-delegates represented that their "major goal . . . is to achieve C&A [certification and accreditation process] of its IT systems".[41] Remarkably, trustee-delegates reported on February 2, 2004 that 52 of the 62 identified information technology systems which house or access individual Indian trust data had been granted an interim approval to operate.[42] All trust systems had received an interim approval to operate by the next status report.[43] This must be contrasted with GAO's June 2004 report which reported that Interior had only completed their certification and accreditation process for 19% of the information technology systems as of June 30, 2004 – down from 22% in fiscal year 2002.[44]

---

[41] *See e.g.* Defendants' *Status Report to the Court Number Eleven* at 14 (November 1, 2002). Note, draft versions of NIST 800-37 were circulated before it was finalized in May 2004.

[42] *See* Defendants' *Status Report to the Court Number Sixteen* at 11 (February 2, 2004). Defendants reported that 4 systems had completed the certification and accreditation process while 6 systems had only completed an initial assessment. The status report is silent as to whether or not the six systems were operating absent the requisite interim authority to operate. *Id*. The table reporting on the status of the certifications and accreditations for trust systems contained in the sixteenth status report was not included in any subsequent reports.

[43] *See* Defendants' *Status Report to the Court Number Seventeen* at 7 (May 3, 2004).

[44] *See* Plaintiffs' Exhibit 5 at 24. In addition, GAO reported a number of problems with the federal government's implementation of the certification and accreditation process including, but not limited to, problems with the quality of the certification and accreditations and problems with

Magically, Norton reported to Joshua Bolton, Director – Office of Management and Budget, on October 8, 2004 (less than three months later) that 90% of Interior's information technology systems had completed their certification and accreditation process.[45] But, now Norton concedes that her certification and accreditation process is deeply flawed:

> We recognize that the C&A process is not perfect, particularly since most of our systems are legacy in nature and this is the first accreditation they have undergone. **The C&A is primarily a process of risk management, requiring application of considerable subjective judgment**. System owners, project managers, and designated officials have been trained and have a **greater understanding of the risks** associated with the numerous legacy systems in the DOI. . . . As part of our C&A process, we have implemented a rigorous oversight and quality assurance program for all C&A systems.

Id. at 1-2 (emphasis added). This statement is demonstrably false and was filed with this Court to mislead it with respect to the status of the certification and accreditation process. Norton knew this to be false because Interior's Inspector General reported to her otherwise two days before she transmitted her memorandum to Mr. Bolton.

On October 6, 2004, the Inspector General transmitted a memorandum to Norton and reported that his office "continue[s] to identify weaknesses in bureau and office implementation of IT security requirements." *See* Plaintiffs' Exhibit 7. He continued:

> our review of information and actions reported by bureaus indicated that they have not consistently followed DOI guidance in implementing their security programs. In particular, **our tests of 20 systems, 19 of which were certified and accredited by the bureaus, identified weaknesses in the conduct of a majority of the system certifications and accreditations**. In our opinion, this demonstrates a clear need for qualitative examination by the CIO of reported bureau accomplishments.

Id. at 3 (emphasis added).[46] In short, the trustee-delegates have been engaged in a sham

---

accuracy of the system inventories. *Id.* at 26-27. While GAO was reporting these problems with respect to the federal government at large, they are identical to those problems reported by the Interior Inspector General. *Infra.*

[45] *See* Plaintiffs' Exhibit 6 (October 8, 2004 Norton Memo) at 2. This memorandum was attached to defendants' *Notice of Filing* which was filed with this Court on November 1, 2004.

[46] The twenty (20) tested information technology systems are listed on page 27-28 of Plaintiffs' Exhibit 7 (Appendix 4). At least four systems have trust data (BLM Perimeter Security/DMZ, Reston Local Area Network, BIA TrustNet and OSTNet), but that number may be

certification and accreditation process in order to continue operating seriously flawed information technology systems which house or access individual Indian trust data.

Of the nineteen systems reviewed which were certified and accredited, twelve (63 percent) did not have a risk assessment. *Id.* at 4. As reported in NIST 800-37:

> The **assessment of risk** and the development of system security plans are two **important activities in an agency's information security program that directly support security accreditation and are required by FISMA and OMB Circular A-130, Appendix III**. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans.

See Plaintiffs' Exhibit 4 (NIST 800-37) at 4 (emphasis added). How Norton possibly certified and accredited these systems without performing a risk assessment is no doubt the application of her "**considerable subjective judgment**."[47] It is certainly not in compliance with FISMA and OMB Circular A-130 which "require[s]" the preparation of a risk assessment.[48] The Reston Local Area Network, BIA TrustNet and OSTNet are among the systems that have not undergone a risk assessment.[49]

The Inspector General made a number of additional findings which reveal the certification and accreditation process as a sham to mislead this Court. Of the nineteen (19) systems reviewed which were certified and accredited by trustee-delegates:

- Three (3) systems underwent limited security control testing which did not cover all system components or locations. *See* Plaintiffs' Exhibit 7 at 4. Three (3) other systems underwent no testing of security controls at all. *Id*.
- Three (3) systems had no plan for continuity of operations in the event of a disaster. *Id.* at

---

substantially larger. The report does not indicate which systems house or access individual Indian trust data. This Court will note substantial and material weaknesses in each of the four aforementioned trust systems. *Id*.

47 *See* Plaintiffs' Exhibit 6 (October 8, 2004 Norton Memo) at 2

48 *See* Plaintiffs' Exhibit 4 (NIST 800-37) at 4.

49 *See* Plaintiffs' Exhibit 7 (October 6, 2004 IG Memo) at 27-28, Appendix 4.

5. Of the sixteen (16) systems which had continuity of operations plans, twelve (12) had material deficiencies. *Id*.

- Six (6) contingency plans were not tested, including at least three trust systems: BLM's Perimeter/DMZ, BIA's TrustNet[50] and OST's OSTNet. *Id*.
- Seventeen (17) had material deficiencies in their security plans, as a result of which "DOI lacks assurance that it has an adequate overview of each system and the system control environment." *Id.* at 5-6.
- Seven (7) systems did not integrate the security costs into the life cycle of the information technology systems. Consequently, the trustee-delegates "lack assurance that they have the most cost-effective security controls implemented." *Id.* at 6.
- Many did not include identified weaknesses in the remedial plans. *Id.*

The Inspector General made additional findings that bear on the trustee-delegates "considerable subjective judgment." First, trustee-delegates cannot identify all contractors with access to information technology systems which house or access individual Indian trust data. *Id.* at 7. The Inspector General reports that Interior "rarely" ensures that contractor provided services are adequately secured and meet regulatory and statutory requirements. *Id.* at 18 (question A3(a)). Second, trustee-delegates have still not identified individuals with significant information security responsibilities. As a foundational matter, Interior cannot control access to individual Indian trust data if they have not identified all individuals with significant access privileges.

Remarkably, the Inspector General reported the trustee-delegates' certification and accreditation process as "satisfactory." *Id.* at 21. However, this is based on (yet another) plan to make a plan: "Our rating of satisfactory in this area, in part, is based on the implementation of the **new initiative** by DOI, **the effectiveness of which has not yet been evaluated**." *Id*. (emphasis

---

[50] The Inspector General reports that: "Indian Affairs' TrustNet [] contingency plan was limited to only technical procedures and did not identify a team for recovery operations or include the specific steps to recover from a disruption in service. Additionally, the plan did not show the order of priority for recovering critical applications." *Id*.

added). Put another way, Norton browbeat a "satisfactory" certification and accreditation rating out of the Inspector General with the feeble promise to conduct a quality assurance review of all C&A documents.

The certification and accreditation process is the statutory and regulatory framework whereby agencies are permitted to operate their information technology systems. Simply put, it provides government officials the assurance that their information technology systems are properly secured and effectively protect their data. This process gives rise to one of three results: (1) operate; (2) disconnect; or (3) limited interim authority to operate. There is a reason that agencies are instructed to disconnect their systems and not operate them unless they have completed the certification and accreditation process. Without assurance that security controls are operating effectively, government officials do not know the risks to which their information technology systems are subjected and are in no position to take affirmative actions to secure the data housed or accessed by their systems.

In this instance, Norton approved every single trust system to operate without conducting a certification and accreditation process. A materially flawed process is no process at all. And, the exercise of "considerable subjective judgment" is not a license to evade their statutory and regulatory responsibility to disconnect systems that have not been properly secured. As a matter of law, such systems must be shut down. Neither Norton, nor any of her senior managers or counsel have the authority to act *ultra vires* and operate systems that have not undergone a proper and complete certification and accreditation process. Yet, that is precisely what has happened here. The widely reported information technology system vulnerabilities remain uncorrected today. Without ever informing this Court or plaintiffs, Norton directed that systems be brought online and operational and deliberately placed irreplaceable individual Indian trust data in imminent risk of loss, manipulation or destruction. Put another way, Norton and her senior managers and counsel want this Court to believe that they "accepted" the risk to individual Indian trust data and determined that such information technology systems should remain in operation.

Information technology systems which house or access individual Indian trust data certainly remain in operation, but did Norton and her senior managers and counsel even consider the risk to individual Indian trust data in conducting their certifications and accreditations? The Interior Chief Information Officer, Hord Tipton, testified on March 25, 2005 that government officials did **not** consider the potential risk to individual Indian trust data and trust beneficiaries. *Infra*.

VI. HORD TIPTON TESTIFIED THAT GOVERNMENT EMPLOYEES DID NOT CONSIDER THE POTENTIAL RISK TO TRUST DATA AND BENEFICIARIES IN THEIR CERTIFICATIONS AND ACCREDITATIONS

NIST 800-37 states that: "It is **essential** that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order **to make timely, credible, risk based** decisions on whether to authorize operation of those systems."[51] This foundational knowledge is of such importance that NIST 800-37 "presumes that responsible agency officials understand the risks and other factors that could adversely affect their missions." *Id.* at 4. It is for this reason that a NIST companion special publication states that:

> **It is of paramount importance that responsible individuals within the organization understand the risks and other factors** that could adversely affect their operations and assets. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated missions with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

See Plaintiffs' Exhibit 8 (NIST 800-53 entitled: *Recommended Security Controls for Federal Information Systems*) at 2 (emphasis added). It would be difficult to overemphasize the importance of understanding the potential risks to data – it is simply of "paramount importance."

This Court's rulings are dispositive on the question of individual Indian trust data's value.

---

[51] *See* Plaintiffs' Exhibit 4 (NIST 800-37) at 1 (emphasis added).

As early as December 1999, this Court held that "[t]he information contained in and processed by the [trustee-delegates'] computer systems must be monitored and verified." *Cobell v. Babbitt*, 91 F.Supp.2d at 45. Again, on September 17, 2002, this Court made an explicit finding regarding the value of individual Indian trust data: "Specifically, the Court finds that the Department of Interior has the fiduciary obligation to ensure the security of trust information regardless of whether that information is stored on a computer or in a warehouse." *Cobell v. Norton*, 226 F.Supp.2d 1, 129. This Court then stressed the importance of ensuring that such trust data is preserved because of its "fundamental" importance to the Court-ordered accounting:

> To be sure, **there is simply no possible way for the Secretary to provide plaintiffs with, for instance, an accurate accounting if the data upon which she relies to do so is subject to unauthorized manipulation**. The Court's finding today is entirely consistent with and is actually a corollary to this Court's ruling in December 1999. In that opinion, the Court noted, among other things, that "**a fundamental requirement** of defendants' responsibilities in rendering an accurate accounting is retaining the documents necessary to reach that end[.]" The Court similarly finds and declares today that the **defendants' accounting responsibilities also includes the duty to ensure the security of the information upon which that accounting will be based**.

Id. (emphasis added). Multiple subsequent decisions of this Court also reaffirmed the importance of ensuring the integrity of trust data, including this Court's entry of the July 28, 2003 preliminary injunction:

> The Court finds that the continued operation of computer systems connected to the Internet that either house or provide access to individual Indian trust data, and **which have not been demonstrated to be secure** from Internet access by unauthorized persons, constitutes further and continuing an irreparable injury to plaintiffs. Their continued operation provides an opportunity for undetectable unauthorized persons to access, alter, or destroy individual Indian trust data via an Internet connection. The alteration or destruction of any of the trust data would further prevent the beneficiaries of the individual Indian money (IIM) trust from receiving the payments to which they are entitled, in the correct amount. Although money damages might provide adequate compensation for this injury, it manifestly cannot provide adequate compensation if neither the Interior Department nor the beneficiaries are aware that such information has been altered or destroyed. Additionally, the alteration or destruction of any of this information would necessarily further render any accounting of the individual Indian trust inaccurate and imprecise, and therefore inadequate. Again, the risk that such an alteration or destruction might never be discovered renders this harm one for which money damages are manifestly inadequate. **The Court thus concludes that plaintiffs have demonstrated that they would be further irreparably harmed if the Court were to permit the continued operation of the Interior Department's computer**

> **systems that either house or provide access to individual Indian trust data**, and which have not been demonstrated to be secure from Internet access by unauthorized persons.

Cobell v. Norton, 274 F.Supp.2d 111, 129-130 (emphasis added).[52] Finally, the U.S. Court of Appeals echoed this Court in holding that: "As the district court noted, 'Interior's present obligation to administer the trust presents sufficient grounds for finding that Plaintiffs will be irreparably injured.'" *Cobell v. Norton XII*, 391 F.3d at 253.

It is manifestly clear that regulatory and statutory guidance dictates that responsible government officials understand the risks to their information technology systems, going so far as to say that such knowledge is of "paramount importance." Likewise, this Court and the U.S. Court of Appeals have repeatedly held that individual Indian trust data is vital to the prudent management and administration of the trust, including the rendering of the Court-ordered accounting. The compromise of such data irreparably harms plaintiffs: "there is simply no possible way . . . [to render] an accurate accounting if the data . . . is subject to unauthorized manipulation." The logical question follows: did responsible government officials consider the risks to plaintiffs when they were conducting their certifications and accreditations? Hord Tipton testifies that they did not, in any way, consider the risk to the data or plaintiffs as a result of operating insecure systems which house or access individual Indian trust data. *Infra*.

The Chief Information Officer, by statute, is charged with developing and maintaining an information security program, developing policies and procedures and control techniques, "training and overseeing personnel with significant responsibilities for information security . . . and assisting senior agency officials concerning their responsibilities. . . ."[53] On March 25, 2005,

---

[52] This Court again reiterated and reaffirmed its analysis of the irreparable harm to plaintiffs as a consequence of the continued operation of insecure information technology systems on March 15, 2004.

[53] *See* 35 USC 44, § 3544(3). In the context of the certification and accreditation process, NIST 800-37 defines the Chief Information Officer's role as follows:

> The Chief Information Officer is the agency official responsible for: (i) designating a senior agency information security officer; (ii) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; (iii) training and overseeing personnel with significant

plaintiffs deposed Tipton, who repeatedly testified that no Interior employees considered the irreparable harm (the risk) to the trust data or plaintiffs when conducting the certification and accreditation process:

> Q Okay, do you know whether anyone has assessed the nature and scope of the irreparable injury to plaintiffs and whether that was considered in the C&A process?
> A I don't know that that assessment is included in the C&A process.

See Plaintiffs' Exhibit 9 (Tipton Deposition) at 331:9-14.[54] *See also id.* at 321:19-322:3:

> responsibilities for information security; (iv) assisting senior agency officials concerning their security responsibilities; and (v) in coordination with other senior agency officials, reporting annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions. The Chief Information Officer, with the support of the senior agency information security officer, works closely with authorizing officials and their designated representatives to ensure that an agency wide security program is effectively implemented, that the certifications and accreditations required across the agency are accomplished in a timely and cost-effective manner, and that there is centralized reporting of all security-related activities.
> To achieve a high degree of cost effectiveness with regard to security, the Chief Information Officer encourages the maximum reuse and sharing of security-related information including: (i) threat and vulnerability assessments; (ii) risk assessments; (iii) results from common security control assessments; and (iv) any other general information that may be of assistance to information system owners and their supporting security staffs.

See Plaintiffs' Exhibit 4 (NIST 800-37) at 12 (footnote omitted). Tipton corroborated that he is "the official delegated authority from the Secretary to determine whether or not any system in Interior meets the requirements [to operate] . . . . I'm ultimately responsible." *See* Plaintiffs' Exhibit 9 (Tipton Deposition) at 318:7-17.

[54] *See also id.* at 336:5-11:

> Q Okay, does anyone -- have you ever been informed that in the C&A process you consider the irreparable harm that has already been done to the trust beneficiaries in making the decision to continue operating the system? Has anyone asked you to do that?
> A No, not explicitly.

And, *id.* at 326:4-18 (emphasis added):

> Q Okay, did you do an assessment or did anyone do an assessment of the risk to the trust beneficiaries as a result of the deficiencies that you were aware of?
> A The assessments were made on the systems, per se. **I cannot answer whether or not they were assessed for impact on any particular class of people**.
> Q Well, was there -- specifically then, you don't know if there was any assessment with respect to the impact of those deficiencies that the government admitted to on December 17th. These would be trust beneficiaries, correct? You don't know.
> A **I don't know that they were made for the specific purpose of assessing impact on trust beneficiaries**.

Q Did you state what the consequences were [of operating insecure systems]?
A The consequences were decertification of the systems.
Q No, the consequences to the data.
A To the data? I don't know that there were any consequences to the data.
Q Did you assess that issue?
A No.

Id. In addition, Tipton testified that he was unaware that the U.S. Court of Appeals had also held there was irreparable injury to plaintiffs as a result of the operation of insecure information technology systems. *Id.* at 331:15-332:20.[55] In short, Tipton directed that government officials undertake a certification and accreditation process without ensuring that they consider the risk to trust data and the individual Indian trust beneficiaries.

Such a paradigm necessarily dislodges the NIST 800-37 balancing of factors in favor of operating any system – especially since there is **no** consideration of the risk to operating such systems, however insecure they might be or what vulnerabilities may render them ineffective to secure trust data. But, it is much worse. For the first time in this litigation, Tipton disclosed that certain vulnerabilities on trust systems cannot be mitigated because such systems are so deficient. He now testified that the risk of operating such systems with vulnerabilities that cannot be remedied are treated differently – this novel approach is referred to as "residual risk."

Q Okay. And security is -- at least based on regulations, is designed to insure integrity of data. Do you accept that?
A Yes.
Q Are you stating that today the integrity of the data in the legacy systems is insured?
A I'm stating that the data in all of the systems we've discussed has been evaluated as to the impact, the sensitivity classification that goes onto that system, the controls on those systems have been tested, application of controls, to the extent that they can be applied, has been evaluated, **risk that result from inability to put controls on those systems** have been transcribed to vulnerabilities. That information and those risks have been listed in a corrective action plan that we call our POAM, so **we have two types of risk**. We have **residual risk** and risk to be mitigated. **On these older systems there are more things in there that can't be mitigated that result in risk** and by the definition, anywhere you want to look on

[55]Plaintiffs then inquired as to whether or not any government attorney had advised Tipton that plaintiffs suffered irreparable injury as a result of the operation of insecure systems. Tipton was advised by Department of Justice attorney, John Warshawsky, to not answer that question even though plaintiffs counsel made it abundantly clear that they were only asking with respect to the management and administration of the trust. *Id.* at 332:21-334:22.

> IT security, simply requires that you evaluate that risk. You do the testing on your systems to confirm those risks and then you certify around what controls you deem that are appropriate. You discuss those with your system owner. **The system owner knows the risk by not having a control as you just prescribed to that system, and it is up to them to accept or to reject that risk**. If they reject that risk then they do not operate the system. But it is a judgment based upon as good as you can secure the system in the state that it's in and knowing exactly what risks are out there.

Id. at 262:21-264:8 (emphasis added).[56] Preliminarily, there is no regulation, NIST publication or any other authority supporting Tipton's notion of "residual risk." But, it is dispositive for purposes of this motion to note that every single responsible government official made a decision to operate their trust systems despite the existence of significant deficiencies **that cannot be remedied**. To be clear, this Court was never told that certain trust systems are so defective that they cannot be secured. Moreover, this Court was never told that such irremediable vulnerabilities are significant: "We have systems that have **some significant risk**, these old legacy systems, that **we had chosen to accept those risks, to go ahead and certify the systems and to operate**." *Id.* at 288:20-289:1 (emphasis added).[57] Plaintiffs counsel was careful to clarify the nature and scope of this admission:

> Q Is it fair to say that it's -- what you've been testifying to means that system

[56] Tipton testified repeatedly that he considered a system to have "adequate security" once the risks to the system were accepted: "Adequate security is defined as assessing each of your systems having appropriate documentation, assessing your risk, balancing available resources to mitigate those risks, **and then accepting those risks**. . . ." *Id.* at 11:20-12:1 (emphasis added). To be sure, Tipton testified that once a risk has been identified, a system may be brought operational by "accepting those risks" – he continued: "it's acceptance of the risk that has been identified within that system by an official that's responsible for the system." *Id.* at 16:7-9. Without respect to whether or not responsible government officials understand the risks to their trust systems – and, he has testified that they do not understand those risks – Tipton testified that the critical feature of the certification and accreditation process is the **acceptance** of risk rather than the **remediation** of risk.

[57] As candidly admitted by Tipton, these systems are not perfect and the integrity of these systems has not been able to be documented:

> A **We're not testifying today that those systems are perfect, not by any means**.
> Q I didn't ask you that question. I'm asking you questions as to whether the systems are secure and whether the data has integrity and whether you've been able to document the integrity. **Have you been able to document the integrity to the best of your knowledge**?
> A **Not based on my knowledge**.

Id. at 275:11-18 (emphasis added).

> owner makes the decision to continue to operate a system even if there are risks that are identified to the data housed in the system? Is that true, not you but the system owner makes that decision.
> A That's true . . . .

Id. at 292:6-12.

This is a flagrant violation of this Court's order and a material breach of trust. Interior has been certifying information technology systems which house or access individual Indian trust data to operate knowing that they were insecure and that certain vulnerabilities could not be remedied. At the same time they ignore the resulting irreparable harm to plaintiffs consequent to operating such systems. This is a clear and unambiguous breach of trust which is compounded by trustee-delegates' efforts to deceive this Court and conceal such material information. After nine years in this litigation, it should come as no surprise that this information was withheld by Hord Tipton, the certifier for the information technology security sections of the eighteenth, nineteenth and twentieth status reports to the Court.[58] Unfortunately, the risk to Trust Data is real and imminent. Unless and until these information technology systems which house or access individual Indian trust data are rendered inoperable, irreparable harm will continue to be inflected on over 500,000 individual Indian trust beneficiaries.

VII. PLAINTIFFS HAVE MET THE STANDARDS FOR THIS COURT TO ENTER A TEMPORARY RESTRAINING ORDER AND A PRELIMINARY INJUNCTION

The District of Columbia Circuit applies a traditional four-part test for determining a request for a temporary restraining order, under which a moving party must establish: (1) substantial likelihood of success on the merits; (2) irreparable harm for which there is no adequate legal remedy in the absence of the injunction; (3) that the injunction will not substantially harm

[58]It is revealing that Tipton knew that this was material information that should have been disclosed to the Court but decided to not disclose this information because it "is of a sensitive nature." *Id.* at 295:9-297:8

other parties; and (4) that the injunction will not significantly harm the public interest.[59] A deficiency in one or more of the four factors may be balanced against a particularly strong showing in one or more of the others.[60]

A. Plaintiffs Have a Substantial Likelihood of Success on the Merits

As discussed more fully above, this Court and the Court of Appeals repeatedly have held that an imminent risk to the integrity of Trust Data constitutes irreparable harms and that this Court is vested with the authority to issue a preliminary injunction to ensure that Trust Data is protected and preserved. Moreover, on this very issue, the Court of Appeals in *Cobell XII* has determined that if this Court at the conclusion of an evidentiary hearing finds that IT Systems currently are insecure, it is empowered to shut down insecure computers to ensure the preservation of Trust Data.

The admission contained in trustee-delegates' April 8, 2005 Notice, itself, and the admissions of Tipton that the trustee-delegates cannot ensure the integrity of Trust Data[61] is powerful evidence that plaintiffs will prevail on the merits for the TRO. To the extent there is any reasonable doubt about the imminent risk to Trust Data – and there should be none – based on the record of these proceedings, applicable law and the facts stated herein, plaintiffs will demonstrate in an evidentiary hearing that the trustee-delegates' are consciously deceiving this Court and plaintiffs and knowingly operating insecure information technology systems that house or access Trust Data which exposes Trust Data to an imminent risk of further loss, destruction, corruption and further irreparable degradation.

Furthermore, plaintiffs have prevailed on the merits in each phase of this litigation. In that regard, it is essential that the TRO be entered to ensure that electronic trust records are protected

---

[59]*See Cobell v. Norton*, 274 F. Supp.2d 111, 126 (D.D.C. 2003). *See also Al-Fayed v. CIA*, 254 F. 3d 300, 303 (D.C. Cir. 2001); *George Washington Univ. v. District of Columbia*, 148 F. Supp.2d 15, 17 (D.D.C. 2001).

[60]*See CityFed Financial Corp. v. Office of Thrift Supervision*, 58 F. 3d 738, 747 (D.C. Cir. 1995).

[61]*Supra*.

and preserved in accordance with the fiduciary duties conferred on the trustee-delegates by Congress, in accordance with common law, and as set forth in orders of this Court. To the extent that the trustee-delegates insist that their spoliation has not rendered impossible the accounting of all funds for each trust beneficiary since the inception of the trust, it is imperative that the declared duty to account is not impaired further as a result of the continuing loss, destruction, and degradation of Trust Data. This Court pointedly found that "[t]he relationship between the number of accounts and the number of individual Indian beneficiaries of the trust fund is difficult to unravel."[62] To the extent that the trustee-delegates insist that the declared complete and accurate accounting will be rendered, the remaining trust records and their integrity become even more vital since they are the only source of trust information.

The United States Court of Appeals for the District of Columbia Circuit has held that the Secretary is entitled to **no** deference in the management and administration of the Individual Indian Trust. She is entitled to none here. Moreover, because trust law governs this action in equity and Norton has committed, and continues to commit, malfeasance in the management of the Individual Indian Trust, injunctive relief is required because it is black-letter trust law that on-going malfeasance constitutes a continuing breach of trust and that a breach of trust, itself, constitutes irreparable harm. *Cobell XII* reaffirmed these principles:

> Contrary to the Secretary's view, ''[w]hile the government's obligations are rooted in and outlined by the relevant statutes and treaties, they are largely defined in traditional equitable terms,'' *Cobell VI*, 240 F.3d at 1099, and the narrower judicial powers appropriate under the APA do not apply. . . . The district court, then, retains substantial latitude, much more so than in the typical agency case, to fashion an equitable remedy because the underlying lawsuit is both an Indian case and a trust case in which the trustees have egregiously breached their fiduciary duties. *Id.* at 1099, 1109.[63]

In addition, this Court has ruled repeatedly in favor of plaintiffs on matters related to the

---

[62]*Cobell v. Norton*, 283 F. Supp. 2d 66, 149 (D.D.C. 2003) (*"Cobell X")*.

[63]*Cobell XII*, 391 F.3d *257.

protection and preservation of trust records.[64] The trustee-delegates' admitted imminent risk to the integrity of Trust Data presents this Court with the same issue and, as such, plaintiffs have a substantial likelihood of success on the merits on this issue.

B. Plaintiffs' Injury is Irreparable Unless a TRO and Preliminary Injunction is Entered

The degradation of the integrity of Trust Data is *per se* a breach of trust and constitutes irreparable harm on its face. There is nothing plainer than that. This is particularly compelling here because systemic spoliation has occurred throughout the sordid history of the Individual Indian Trust – as well as throughout the notorious trusteeship of Norton. There is no doubt that further loss, destruction, corruption and degradation of Trust Data will continue absent issuance of the proposed TRO and preliminary injunction. And, there is no doubt that Trust records have been, and will continue to be, in imminent jeopardy of massive loss, destruction and corruption unless this Court intervenes to protect the Trust beneficiaries. In accordance with trust law, there can be no dispute that the harm caused by such malfeasance and breaches of trust is irreparable. As such, it is certain that plaintiffs will be further harmed irreparably if the requested relief is not granted.

C. Entry of a TRO and a Preliminary Injunction Cannot Harm the Secretary Since the Secretary Will Be Restrained From Conduct That Undermines the Integrity of These Proceedings

The Secretary cannot argue in good faith that the injunctive relief plaintiffs' request would harm Interior. First, all that plaintiffs seek is maintenance of the *status quo* until this Court is assured that whatever remains of the integrity of Trust Data is not further degraded. The trustee-delegates have no **legitimate** interest in permitting the further degradation of Trust Data. None. Second, the relief plaintiffs seek is restraint and protection; that trustee-delegates and their counsel have deceived this Court and the Court of Appeals in this regard in willful disregard of the irreparable harm they have done to plaintiffs undermines the integrity of these proceedings. It is

[64]*See e.g.*, December 5, 2001 Temporary Restraining Order, April 18, 2002 Temporary Restraining Order, and September 9, 2004 Memorandum and Order.

unfathomable that fiduciaries cry foul and undue hardship (as opposed to irreparable harm) after their deception is revealed.

What plaintiffs seek herein is appropriate and long over due: that Norton stop deceiving this Court, the Court of Appeals and plaintiffs; stop violating the law; stop degrading the integrity of Trust Data; and stop breaching the trust duties that she as a trustee-delegate owes to the *Cobell* plaintiffs; fiduciary duties that Norton must discharge in accordance with the most strict fiduciary standards and solely in the best interest of individual Indian trust beneficiaries. It is unfortunate that the Secretary chooses to repudiate her trust duties and continues to mislead this Court and the Court of Appeals. It is also unfortunate that plaintiffs must take this action again to seek the protection of this Court from an unscrupulous trustee-delegate and her counsel. Accordingly, the Secretary cannot argue in good faith that an order that restrains such conduct and that stops her from continuing to harm 500,000 individual Indian trust beneficiaries irreparably in anyway harms the Interior Department.

D. Injunction Cannot Harm The Public Interest

The conduct plaintiffs seek to restrain is inimical to the public interest – government officials are not above the law. Trustee-litigants are not permitted to allow the Trust *corpus*, and the electronic records related thereto, to further degrade and fall into ruin. It is surely in the public interest to enjoin the conduct of a trustee-delegate that undermines the integrity of these proceedings. Trustee-delegates are not permitted to destroy, lose, or corrupt Trust Data. Trustee-delegates are not entitled to put beneficiaries' Trust assets, including the Trust *corpus* and Trust Data in imminent risk of further loss, destruction, corruption and further degradation.[65] The proposed temporary restraining order and preliminary injunction are simply designed to preserve the remaining integrity of Trust Data, if any. Nothing more.

One would hope that entry of the requested TRO might help this trustee-delegate begin to

[65]Trust records are the property of the Trust and, as such, they are vested property rights of the Trust beneficiaries akin to the *corpus* itself. *See, e.g.*, *Wood v. Honeyman*, 178 Or. 484, 169 P.2d 131 (1946.).

comprehend the importance of her trust obligations and encourage her to begin to discharge the trust duties owed by the United States to individual Indians in accordance with the highest fiduciary standards. But, it is clear that this is hopeless. It is certainly in the trust beneficiaries' interest that this Court prevent further losses of the Trust *corpus* and the further degradation of Trust Data.[66] It is certainly in the nation's interest to restrain Secretary Norton from continuing to violate the law and willfully breach her trust duties. And, it is in the taxpayer's interest to prevent additional loss, destruction, and corruption of Trust assets – including Trust Data – so this case, ultimately, can be resolved equitably and fairly.

VIII. CONCLUSION

There is an urgent need to protect ever-degrading trust records and trust funds that can only begin to be met if this Court grants plaintiffs' motion for a temporary restraining order, schedules an evidentiary hearing, compels the testimony of Rule 30(b)(6) witnesses, compels production of all documents related thereto, and enters the preliminary injunction proposed by plaintiffs.[67]

---

[66]*Cf. Sac & Fox Nation of Missouri v. LaFaver*, 905 F. Supp. 904, 907-08 (D. Kan. 1995).

[67]In accordance with local rules, plaintiffs' counsel left voice mail messages and attempted to meet and confer with defense counsel. Plaintiffs presume that the trustee-delegates oppose this motion.

Respectfully submitted,

/s/ Dennis Gingold

DENNIS M. GINGOLD
D.C. Bar No. 417748
P.O. Box 14464
Washington, D.C. 20044-4464
202 824-1448

Of Counsel:

JOHN ECHOHAWK
Native American Rights Fund
1506 Broadway
Boulder, Colorado 80302
303-447-8760

/s/ Keith Harper

KEITH HARPER
D.C. Bar No. 451956
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
202 785-4166

Attorneys for Plaintiffs

April 11, 2005

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing PLAINTIFFS' CONSOLIDATED MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION was served on the following via facsimile, pursuant to agreement, on this day, April 11, 2005.

Earl Old Person (*Pro se*)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
406.338.7530 (fax)

/s/ Geoffrey Rempel
_____
Geoffrey M. Rempel