

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

DEFENDANTS’ OPPOSITION TO PLAINTIFFS’ CONSOLIDATED
MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

Pursuant to Rule 65 of the Federal Rules of Civil Procedure and Local Civil Rule 65.1, Defendants respectfully submit the following opposition to Plaintiffs’ Consolidated Motion for Temporary Restraining Order and Preliminary Injunction (Dkt. No. 2926) (filed Apr. 11, 2005) (“Plaintiffs’ Motion” or “Pl. Mot.”), which seeks an order requiring that “the Interior Defendants shall immediately disconnect from the Internet and terminate the operation of all information technology systems within the custody and control of the Department of the Interior, its employees, agents, and contractors that house or provide access to Trust Data.” Pl. Mot., Ex. 1 (proposed order).¹

Plaintiffs’ Motion Should Be Denied Because Plaintiffs Cannot Establish
Any of the Elements Required for Issuance of Such an Order.

In their motion, Plaintiffs seek the broadest and most damaging of orders to-date with

¹ Interior can respond more specifically once an appropriate protective order has been entered. Interior filed its motion for a protective order on April 12, 2005. Dkt. No. 2929 (filed Apr. 12, 2005) (motion to expedite consideration of motion for protective order).

respect to Interior's Information Technology ("IT") systems: Plaintiffs seek an order to disconnect such IITD systems from the Internet and to shut down their operations entirely. Pl. Mot. at 6; Ex. 1. In seeking such relief, Plaintiffs devote only a slim portion of their motion to a discussion of the elements that this Court must consider before entering a temporary restraining order or a preliminary injunction. See Pl. Mot. at 29-34.

As this Court is aware, in considering whether to grant an application for a temporary restraining order or a preliminary injunction, this Court must examine (1) whether a substantial likelihood exists that the plaintiff would succeed on the merits, (2) whether the plaintiff would suffer irreparable injury if the injunctive relief is denied, (3) whether the granting of injunctive relief would substantially injure the other party, and (4) whether the public interest would be served by the granting of the injunctive relief. E.g., Davenport v. Int'l Bhd. of Teamsters, AFL-CIO, 166 F.3d 356, 360-61 (D.C. Cir. 1999) (citing Serono Lab., Inc. v. Shalala, 158 F.3d 1313, 1317-18 (D.C. Cir. 1998)); Kudjodi v. Wells Fargo Bank, 181 F. Supp. 2d 1, 2 n. 2 (D.D.C. 2001). Simply put, Plaintiffs have failed to establish any of these elements and, accordingly, no basis exists for a temporary restraining order or a preliminary injunction.

A. Plaintiffs Have Not Established a Substantial Likelihood of Success on the Merits.

Plaintiffs assert that the notice filed by Defendants on April 8, 2005 (the "April Notice")² and the purported "admissions" of Interior's Chief Information Officer, W. Hord Tipton, provide sufficient evidence to find that a substantial likelihood exists that Plaintiffs will succeed on the

² Defendants' Notice to the Court Regarding Inspector General's "Notification of Potential Finding and Recommendation" with Respect to Information Technology System, Dkt. No. 2994.

merits of their claim that individual Indian trust data (“IITD”) on Interior’s IT systems is insecure and that there is an imminent risk of loss, destruction or corruption of IITD. Pl. Mot. at 30. Neither the April Notice nor the unsigned transcript from Mr. Tipton’s yet-to-be-completed deposition meets their burden.

The April Notice refers to a memorandum entitled “IT Security Penetration Testing - Notification of Potential Finding and Recommendation” provided to the Bureau of Land Management (“BLM”) on April 6, 2005 (the “April Report”). As the April Notice explained, the penetration testing³ (conducted by a contractor supervised by the Office of the Inspector General (“OIG”) independently of BLM or the rest of Interior) is part of a larger, comprehensive program which Interior has established to monitor and assess security controls placed on Interior’s IT

³ Penetration testing is a security test in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify methods of gaining access to a system by using tools and techniques that may be employed by attackers. Penetration testing can be an invaluable technique to any organization's information security program. However, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems. Furthermore, the possibility exists that systems may be damaged in the course of penetration testing and may be rendered inoperable, even though the organization benefits in knowing that the system could have been rendered inoperable by an intruder. National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-42, Guideline on Network Security Testing, October 2003, at 3-11 to 3-16; NIST SP 800-12, An Introduction to Computer Security - The NIST Handbook, October 1995, at 100, § 9.4.1.4.

NIST is responsible for developing standards and guidelines, including minimum requirements, and providing adequate information security for all agency operations and assets, (excluding standards and guidelines for national security systems). NIST SP 800-37 is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III, and sets forth a four phase program for Certification and Accreditation (“C&A”): Initiation; Security Certification; Security Accreditation; and Continuous Monitoring.

systems,⁴ in compliance with requirements of the continuous monitoring final phase of the Certification and Accreditation (“C&A”) described in NIST SP 800-37.⁵ The potential for discovery, during the continuous monitoring phase, that security controls are not as effective as intended is specifically contemplated by NIST SP 800-37:

If the results of the security assessment indicate that selected controls are less than effective in their application and are affecting the security of the information system, corrective actions should be initiated and the plan of action and milestones updated.

Id. at 45. As the April Notice reflects, “all vulnerabilities identified by the Inspector General either have been or will be addressed promptly.”⁶ April Notice at 2.

⁴ The monthly scanning of the perimeter of Interior’s IT systems by a different contractor using the SANS (SysAdmin, Audit, Network, Security Institute) Top 20 list is another part of the continuous monitoring of IT systems embodied in the C&A process defined in NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004 (“NIST SP 800-37”). The SANS Top 20 list is an industry-accepted standard for critical vulnerabilities scanning of IT system perimeters. The SANS Top 20 list is relied upon as a widely accepted standard within the government and the private sector. Declaration of Hord Tipton Decl. at 9 (“Tipton Decl.”) (Exhibit 1 to this brief). To the extent that the SANS Top 20 scanning (reported upon in recent quarterly status reports to the Court) failed to reveal potential vulnerabilities like those that formed the basis for the April Report, Interior has initiated plans to modify the monthly scanning to make it even more robust and effective in discovering potential vulnerabilities. Id. at 18.

⁵ The Continuous Monitoring Phase includes assessing “an agreed-upon set of security controls in the information system 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.” NIST SP 800-37, Subtask 9.2, Selected Security Control Assessment, at 45. While this section references NIST SP 800-53A for guidance on techniques or controls to use, NIST has yet to publish SP 800-53A, even in draft.

⁶ As the attached Declaration of Ms. Levine (“Levine Decl.”) (Exhibit 2 to this brief) explains, BLM took prompt action to limit Internet access for those portions of the network that access or house IITD. Complete disconnection was not directed because certain critical functions relating to the protection of life and property depend on Internet connections to function effectively. Levine Decl. at 5 and 6.

The immediate risk to IITD which resulted from the potential security control vulnerability in the BLM network has been mitigated or eliminated in the short-term by the disconnection of the majority of the BLM network from Internet access. As the attached Levine declaration demonstrates, the longer-term solution to protecting IITD is to permit those portions of the network housing or accessing IITD to have Internet access restored only after corrective actions are taken, additional security is in place and a new security control assessment is completed, including further assessment by the OIG. Levine Decl. at 10. Thus, for the BLM IT systems covered by the April Notice, Interior has already taken the steps necessary to protect IITD and is implementing short-term and long-term solutions to resolve the issues identified by the OIG penetration test.⁷

While Plaintiffs' Motion seeks an order to disconnect and terminate the operation of all Interior systems housing or accessing IITD, their motion provides no factual basis for such a sweeping, harsh and draconian order.⁸ The April Report contains no information concerning potential vulnerabilities or weaknesses that threaten any IITD in any non-BLM IT systems housing or accessing IITD. Lacking any direct evidence on the security of the IITD on IT systems other than BLM, Plaintiffs rely on the Office of the Inspector General's Annual

⁷ As the Levine Declaration explains, BLM was notified generally of some potential vulnerabilities on March 22, 2005, and it promptly addressed those issues. Later, on April 6, 2005, the OIG provided the considerably more explicit April Report and other documentation to BLM. Levine Decl. at 2 and 3.

⁸ As explained in Section D, infra, termination of all Interior IT systems housing or accessing IITD would cripple the operation of significant portions of Interior and its ability to serve the public, including IIM administration and trust reform. Further, the sweep of Plaintiffs' Motion would seriously impair the ability of Interior to perform functions necessary to protect lives and property against fires and other threats.

Evaluation of the Information Security Program of the Department of the Interior (the “OIG Annual Evaluation”)⁹ and the deposition testimony of Mr. Tipton. Neither source supports their assertion that an Internet disconnection or a total termination of all Interior IITD IT systems is required to protect IITD.

Despite Plaintiffs’ attempt to characterize the OIG Annual Evaluation in terms of their view of the C&A process,¹⁰ the Inspector General, whose investigators examined the enumerated systems, came to a different conclusion. The Inspector General stated:

We found that DOI has effectively designed its information

⁹ Report No. A-EV-MOA-0006-2004, October 2004. Interior submitted this report to the Court along with the Interior Federal Information Security Management Act Report for 2004 on November 1, 2004. Dkt. No. 2750.

¹⁰ Plaintiffs’ attack on the C&A process as a “sham” (including the evaluations and judgments made therein) is remarkable considering that these sensitive documents have not been made public. The Department of the Interior has taken extraordinary steps to comply with OMB Cir. A-130, Appendix III requirements as well as the FISMA requirements. Interior has made IT security maintenance a high priority for all bureaus and offices and has invested more than \$100 million in its IT security program over the past three years. During this time period, the percentage of certified and accredited systems has dramatically increased from no accredited IT systems in 2002 to approximately 96% accredited in 2005. Tipton Decl at 5. Interior’s publicly stated intention is to “continue to make improvements to further strengthen IT security and ensure consistent implementation by all bureaus and offices.” Department of the Interior FY 2004 Performance and Accountability Report (“PAR”) at 18; <http://www.doi.gov/pfm/par2004/>.

Before fiscal year 2002, Interior’s IT Security Program budget was approximately \$4 million. In fiscal year 2004, the annual IT Security Program budget grew to \$30 million. Interior invested \$12 million in C&A implementation and has established a quality assurance program run by an independent contractor. The Office of the Inspector General concluded that Interior has “significantly improved its information security program” and “generally meets the requirements of FISMA” and that “most of the information systems have levels of security to safeguard Department information and related assets.” Cover letter from Inspector General Earl E. Devaney to Mr. Joshua B. Bolten, Director, OMB, OIG Annual Evaluation of DOI Information Security Program, dated October 12, 2004, Dkt. No. 2750, filed November 1, 2004; see Department of the Interior FY 2004 PAR, at 66-68, 86-88, <http://www.doi.gov/pfm/par2004/>; Tipton Decl. at 5.

security management program to meet the requirements of FISMA and continued to improve security over its information systems. DOI developed its information security program based on OMB policies, NIST standards and guidelines, and DOI policies established through departmental directives.

OIG Annual Report at 3 (citations omitted). Although the OIG noted that problems existed, including the failure of bureaus to uniformly follow DOI guidance in implementing their security policies and the C&A process, the OIG Annual Evaluation rated the Interior C&A process as satisfactory.¹¹ Thus, Interior clearly has made significant improvement in IT security, as evidenced by the independent report from the Inspector General, and the overall situation is markedly different from that which prevailed in 2001. Plaintiffs' reliance upon that outdated historical material should be rejected outright as not being probative of Interior's IT security today.¹²

Plaintiffs either ignore or gratuitously characterize as false, misleading or deceptive¹³ the

¹¹ On February 16, 2005, the Government Reform Committee of the U.S. House of Representatives released its 2004 "Federal Computer Security Report Card" (<http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%2002%20years.pdf>). The Government Reform Committee also released the grading criteria and methodology. (<http://reform.house.gov/UploadedFiles/2004%20FISMA%20Report%20Grading%20Element.pdf> and <http://reform.house.gov/UploadedFiles/FISMA%20How%20Grades%20Were%20Assigned1-10-05v2.pdf>). The overall government score was D+; however, the Department of the Interior grade was C+, putting it in the top third of all government agencies. This is a marked improvement over last year's failing grade.

¹² The OIG Annual Evaluation lists Interior's IT security related improvements over the past year and the list is impressive (Appendix 3 at 26).

¹³ Pl. Mot. at 2 n.2 (alleging that the Appellants' Brief misled the Court of Appeals on IT security); 4, 6, 7 n.14 (alleging misleading declarations and certifications concerning IT security); 5 n.10 (dismissing the Special Master's determinations of adequate security to protect IITD because they were not made with prior consultation with the Plaintiffs, ignoring that the determinations were based upon reports made by IT security consultants and contained detailed information concerning vulnerabilities and risks); 5 n.11 (alleging that Defendants adopt the

considerable weight of the evidence showing that Interior's IT security has improved greatly over the past three-plus years. The extensive testing done by the Special Master's well-qualified IT security consultants prior to the reconnection of many IT systems, reflects the improvement of the security of Interior's IT systems since December 2001. This demonstrated improvement cannot be dismissed through a casual allegation that Interior "gamed" the Special Master or declaration that, almost two years after the last approved reconnection, the Special Master's determinations are suspect.¹⁴ Interior's security posture did not stagnate once approval was obtained to reconnect to the Internet. Interior committed more than \$100 million to improving the security of its IT systems since the December 17, 2001 Consent Order, increased its IT Security Program seven-fold and obligated \$12 million to its C&A program. See infra, p. 6 n.10.

"marginal standards" of lobbyists, influence peddlers, willfully ignorant laymen, dishonest defense counsel and incompetent trust counsel); 10-12 (alleging false and misleading statements in Status Reports to the Court Numbers 16-19); 19 (alleging false statements by Secretary Norton intended to mislead the Director of the OMB); 33 (Secretary Norton deceiving the Court and misled the Court of Appeals).

¹⁴ The Special Master's consultants also conducted penetration testing of various Interior IT systems. Generally, the testing revealed adequate security, although some potential vulnerabilities were discovered in some tests. Dkt. Nos. 2529 and 2535 (redacted versions). Plaintiffs' characterization of the last penetration test on Office of Surface Mining ("OSM") systems, Pl. Mot. at 11, is not in accord with the facts. While the penetration test of one of the OSM IT systems was the last completed test, it was not terminated short of completion as Plaintiffs allege. See SAG Internet Assessment of DOI/OSM Networks, April 29, 2003 ("OSM Assessment"). Plaintiffs also falsely state that the OSM test revealed that a vulnerability in the OSM system which allowed "individual Indian trust data to be accessible from the Internet." Pl. Mot. at 11. Not only does the OSM report contradict this statement ("SAG was not able to gain unauthorized access to ITD data [sic] during the testing...." OSM Assessment at 1), OSM does not have IITD on its IT system. See Declaration of Director Jeffrey Jarrett, OSM, 3, at 1 (Dkt. No. 2175) (filed Aug. 11, 2003); OSM Certification of August 11, 2003, at 16 (Dkt. No. 2175). Furthermore, there is nothing improper in allowing authorized users access to IITD over an Internet connection so long as there is adequate security to protect the data from unauthorized access.

Contractors with specialized skills needed to complete the C&A process were engaged and actively participated in the numerous C&A processes on-going in the many bureaus and offices. Tipton Decl. at 12.

While great emphasis was placed on completing the accreditation of IT systems, Interior also emphasized testing and monitoring of all IT systems. Despite Plaintiffs' unsupported attacks on the results of the SANS Top 20 scanning program, Pl. Mot. at 12, the results of the testing, conducted by a contractor, are real and verifiable.¹⁵ Tipton Decl. at 9. However, it has become apparent that the scope of the scanning should to be expanded beyond the SANS Top 20 to provide Interior bureaus and offices with greater testing depth and the program is being redesigned to test additional items of IT security. Id. at 18. Further, even as the SANS Top 20 scanning was being conducted, Interior took the initiative to expand its security testing program pursuant to an agreement with the OIG to conduct independent penetration testing of Interior IT systems. Id. at 9. The program is funded by Interior but completely managed by the OIG. OIG engaged an IT security firm to conduct the testing. The OIG-administered penetration testing program has been on-going for six months and has provided information useful to Interior in assessing the effectiveness of the security controls on its IT systems. Id. at 12.

The very thorough and intensive OIG penetration tests have worked as designed. By testing the networks in a real world environment and using the expert skills possessed by contractor personnel, the tests have provided valuable data and assisted Interior in further

¹⁵ The Special Master's consultants analyzed some of the results produced from the SANS Top 20 scanning and submitted reports. These reports, SAG SAIC/DOJ January 2003 Scan Data Analysis Report; and SAG SAIC/DOJ March 2003 Scan Data Analysis Report, were filed with the Court. Dkt. No. 2544.

improving its IT security. While some potential vulnerabilities have been revealed, Interior's discovery of these potential vulnerabilities through Interior's own testing program permits the owners of the IT systems to mitigate or remove potential vulnerabilities expeditiously instead of exposing the systems to outside threats. As a result of the SANS Top 20 scanning, the OIG penetration testing and other testing activities, the state of IT security at Interior is better today than it has ever been. Interior is not suggesting, nor does it believe, that further improvements will not be implemented.¹⁶ Further improvements are underway and more are planned, including the consolidation of the thirty-three Interior Internet points of presence ("POPs") into five POPs centrally managed by the Enterprise Service Network, a centralized security control center which can be intensively monitored and protected, and the creation of a Trust DMZ to provide even greater protection for this information. Tipton Decl. at 8. However, there can be no doubt that IITD is at much less risk from unauthorized Internet access today than at any time in the past. Id. at 13.

Plaintiffs' attempt to use the deposition of Mr. Tipton to bolster their argument that IT security is inadequate fares no better than their reliance upon the OIG Annual Evaluation. While

¹⁶ Ensuring adequate security for IT systems is a continuous endeavor. Tipton Decl. at 8. New threats appear almost every day and new exploits are discovered at almost the same rate. See NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995, at 13-14. Complex IT systems are similar in some ways to consumer PCs owned by many Americans. For example, even a minor lapse in vigilance in anti-virus detection and updating of definition files or in patching software applications and operating systems may expose a PC or an IT system to unacceptable risks. Installing a patch to an operating system of a home PC is a relatively simple task; however, on a complex IT system, the patch often must be installed in a test lab and be thoroughly tested before being installed on a system running complex applications used by hundreds of users. Similarly, proposed improvements to network security architecture, hardware or software, must be extensively tested to ensure that operations are unimpeded and that unanticipated vulnerabilities are not created. NIST SP 800-40, *Procedures for Handling Security Patches*, August 2002, Section 5.4, Testing Patches, at 29-31.

Mr. Tipton stated that he was not aware that “irreparable injury to the plaintiffs” was included in the C&A process, Tipton Deposition at 331: 9-14; Pl. Mot. at 26, this statement reflects the poor form of the question rather than a dismissal of the C&A concept of considering the level of harm to individuals or agency operations that might result from a loss of data. Indeed, the confusion demonstrated in Mr. Tipton’s deposition is understandable since “irreparable harm” is a legal term commonly used in the consideration of requests for injunctive relief and not a term used by IT security professionals analyzing risks and implementation of security controls. A question framed in terms of the security categorization of federal information and information systems would be answered in terms that reflect the relevant portion of the process found in FIPS Pub. 199, Standards for Security Categorization of Federal Information and Information Systems (“FIPS 199”), February 2004, and in Chapter 3 of SP 800-37.²² Security categorization requires the system owner to examine, quantify and categorize the information in the IT system based upon the harm that loss or destruction of the information would cause for the organization or individuals. Thus, while Mr. Tipton may not have been familiar with the use of the specific term “irreparable harm” in the C&A process, it is clear that the consideration of the harm that might

²² Security categorization is based upon considerations of the confidentiality, integrity and availability of the information in an information system. Security controls are implemented based upon whether the information on the IT system is categorized as low impact (limited adverse impact on the organizational operations, organizational assets or individuals), medium impact (serious adverse impact) or high impact (serious or catastrophic impact). See FIPS 199 at 2-3; NIST SP 800-37 at 28; NIST SP 800-53 at 13. FIPS 199 defines the category of moderate impact information as that which might result in serious harm to individuals but does not involve loss of life or other serious life threatening injuries if there is a loss of confidentiality, integrity or availability. FIPS 199 at 2. In contrast, high impact information is described in terms of severe or catastrophic harm to individuals involving loss of life or life threatening injuries. Similar descriptions are used regarding damage to organizational assets, organizational functions or financial loss. Finally, this security categorization is done by the system owner, not by the Chief Information Officer one level above the system owner.

result from the loss of data is clearly an integral part of the C&A process.²³

Plaintiffs' assertion that Mr. Tipton's use of the term "residual risk" somehow negates the entire C&A process is even more flawed.²⁴ Management of risk entails the concept of acceptance

²³ The substantive part of the deposition ended for the day just after Plaintiffs' counsel asked the following questions: "[W]hat do you do in performing your job as CIO to insure that you're discharging your fiduciary duties to the trust beneficiaries, particularly with respect to the information that you are insuring? How do you make sure you're doing it properly? ...How do you make sure you're following the law?" Tipton Depo. 339: 2-17, 21-22. Plaintiffs' counsel indicated that he still wanted to question the witness on many subjects including the C&A process and NIST publications. *Id.* at 341:19-22.

The security categorization of information is a required predicate to performing a C&A on an IT system. The categorization is used to determine the level and type of security controls required to adequately secure the system and the data contained in the system. *See* NIST SP 800-53 at 4 ("This publication associates recommended minimum security controls with FIPS 199 low-impact, moderate-impact, and high-impact security categories."). It should be noted, however, that SP 800-53 was published in February 2005, after most of Interior's IT systems completed the accreditation phase of the C&A process.

²⁴ Plaintiffs take issue with Mr. Tipton's use of the word "residual risk" as being contrary to NIST guidance and without support in any other authority. Pl. Mot. at 28-29 ("[T]here is no regulation, NIST publication or any other authority supporting Tipton's notion of 'residual risk'"). This assertion is simply wrong.

NIST publishes Information Technology Laboratory ("ITL") Bulletins on subjects of concern to users of information technology. In the ITL Bulletin, February 2002, Joan S. Hash of the Computer Security Division, Information Technology Laboratory, NIST, discussed "Risk Management Guidance for Information Technology Systems:"

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission. ***The risk remaining after the implementation of new or enhanced controls is the residual risk.*** Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero. If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level. Once the management official responsible for the IT infrastructure determines that an acceptable level of risk has been achieved, the official should sign a statement indicating acceptance of the residual risk prior to

of some risk and does not require the elimination of all risk, an impossible task.²⁵ Mr. Tipton's deposition testimony does not support the Plaintiffs' assertions that Interior's IT systems are insecure; it in fact accurately tracks the NIST guidance on the management of risk in federal information systems.

Moreover, in apparently rejecting the process prescribed by FISMA and OMB Circular A-130 – governmental assessment of risks and terminations to accept certain risks – Plaintiffs substitute no standard for this Court to apply. Rather than recognizing that it is the responsibility of informed officials who are responsible for the operation of IT systems, Plaintiffs seek to

authorization or accreditation of the system for full operation.

ITL Bulletin, Feb. 2002, at 5-6; <http://www.itl.nist.gov/lab/bulletns/bltnfeb02.htm> (emphasis in the original).

NIST 800-53, Recommended Security Controls for Federal Information Systems, February 2005, notes that an effective security program should include “policies and procedures that are based on risk assessments, cost-effectively **reduce information security risks to an acceptable level**, and ensure that information security is addressed throughout the life cycle of each organizational information system.” *id.* at 1 (emphasis added). NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001, provides that “Moreover, these officials [responsible agency officials] must understand the current status of security programs and controls in order to make informed judgments and investments that **appropriately mitigate risks to an acceptable level.**” *id.* at 1. NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002, describes part of this process: “Because the **elimination of all risk is usually impractical or close to impossible**, it is the responsibility of senior management and functional and business managers to use the *least-cost approach* and implement the *most appropriate controls* to decrease mission risk to an acceptable level, with *minimal adverse impact* on the organization's resources and mission.” NIST SP 800-30 at 27 (emphasis added).

²⁵ Management of risk decisions on “Legacy systems” may include the acceptance of greater risk than on more modern systems because the cost of removing the remaining risk may be unacceptably high. The management decision to operate the “Legacy systems” with some significant risks is not contrary to the risk management policy that undergirds the NIST guidance in the information security arena. See generally NIST SP 800-30.

substitute their own judgment that any perceived risk to IITD – even risks not shown to have resulted in any loss of data – is sufficient to order the severe impact of disconnection of IT systems from the Internet and even the shutting down of such systems completely.

Not only have Plaintiffs failed to show a substantial likelihood of success on their allegation that Interior IT systems housing or accessing IITD are not adequately secure from Internet access by unauthorized users, but also the facts discussed in their motion actually support the conclusion that Interior’s IT security program is making great progress toward full compliance with the federal standards contained OMB Cir. A-130, Appendix III.²⁶ Plaintiffs have not met their burden of showing a substantial likelihood of success on the issue of whether IITD on the BLM systems is at risk from Internet access by authorized access, much less on the other IT systems within Interior which contain IITD.

B. Plaintiffs Have Not Established the Potential for “Irreparable Harm.”

Plaintiffs’ Motion provides no specific support for a finding of irreparable harm if a temporary restraining order is not granted. Plaintiffs simply assert that “degradation of the integrity of Trust Data is *per se* a breach of trust and constitutes irreparable harm on its face.” Pl. Mot. at 32. No evidence, however, supports their assertion that any IITD on any IT system is being degraded, destroyed, corrupted or lost. Indeed, much of the IITD housed or accessed on Interior IT systems is not accessible from the Internet and has not been since December 5, 2001.²⁷

²⁶ The federal guidelines emphasize a “risk-based policy for cost-effective security established by the Computer Security Act.” OMB Cir. A-130, Appendix III at ¶ B. Absolute security is not the standard; the federal standard is “adequate security.”

²⁷ The IT systems under the control of the Office of the Special Trustee, the Bureau of Indian Affairs (except for 100 firefighter PCs and 100 administrative PCs), the Office of the Solicitor and the Office of Hearing and Appeals were disconnected from the Internet in

Moreover, the April Notice refers only to the BLM IT systems, and as noted, even that bureau has taken prompt actions to address potential vulnerabilities identified by the Inspector General and to protect IITD. Levine Decl. at 2, 4-6, 8.

Further, Plaintiffs establish no irreparable harm as a result of the operation of Interior IT systems that house or access IITD and have Internet connections.²⁸ Plaintiffs have not even attempted to provide evidence to suggest that the IITD housed or accessed on Interior IT systems without Internet connectivity is being degraded, lost, destroyed or corrupted. Without such a showing, no basis exists for directing that these systems terminate their operation. Simply stated, Plaintiffs have failed to present any evidence that any IITD on Interior IT systems is currently being lost, damaged, degraded or corrupted so as to constitute “irreparable harm.”²⁹

C. The Granting of Plaintiffs’ Motion Would Substantially Harm Interior and Is Not in the Public Interest.

Plaintiffs’ Motion completely disregards the harm to Interior and the public that would result from the granting of a motion to disconnect from the Internet and shut down all IT systems “within the custody and control of the Department of the Interior, its employees, agents, and contractors that house or provide access to [IITD].” It is beyond comprehension that Plaintiffs

accordance with the TRO issued on December 5, 2001, and have not been authorized to reconnect.

²⁸ With regard to the OIG’s findings regarding BLM’s IT systems, Interior’s senior management took prompt action to address potential vulnerabilities noted by the OIG, thereby reducing the risk to any IITD on BLM’s IT systems. Levine Decl. at 5-6, 8.

²⁹ Plaintiffs’ suggestion that, because there has allegedly been unspecified loss, damage or destruction of trust records or IITD in the past, it must still be happening today does not meet their burden of proof. The independent judgment of the Inspector General is that information security has improved at Interior and continues to improve. In the face of such evidence, the Plaintiffs rely solely on speculation.

could seek such unprecedented and patently destructive relief and, at the same time, deny that such an order would harm Interior or the public. Pl. Mot. at 32-33.

Contrary to Plaintiffs' unsupported assertions, the experience since the initial disconnection order in early December 2001 confirms that the disconnection of Interior's IT systems has been costly and disruptive. See, e.g., Notice of Filing Interior's Twentieth Status Report at 9 (Dkt. No. 2827) (filed Feb. 1, 2005); Notice of Filing Interior's Nineteenth Status Report at 9 (Dkt. No. 2748) (filed Nov. 1, 2004); Notice of Filing Interior's Eighteenth Status Report at 8 (Dkt. No. 2622) (filed Aug. 2, 2004). As the Court is aware, where systems have remained disconnected from the Internet, Interior has been forced to rely upon costly and, at times, inefficient "workarounds" to continue to seek to perform its many diverse and critical duties. See, e.g., Notice of Filing Interior's Sixteenth Status Report at 43 (Dkt. No. 2455) (filed Feb. 2, 2004). Now, Plaintiffs seek to go even further and deny Interior the use of its own computers, and in seeking such relief, Plaintiffs baldly assert, in this electronic information age, that "The Secretary cannot argue in good faith that the injunctive relief plaintiffs' [sic] request would harm Interior." Pl. Mot. at 32.

Plaintiffs' argument on this point essentially is based upon a flawed premise: that their version of the so-called "maintenance of the status quo" is the sole interest of Interior and that issuance of the Temporary Restraining Order will further that goal. Pl. Mot. at 32. As previously explained, in making this assertion, Plaintiffs ignore the fact that they have not and cannot point to a single example in which IITD has, in fact, been degraded. Indeed, the OIG's April Report – the only new factual basis relied upon for Plaintiffs' latest motion – confirmed that "No information was collected, no data was manipulated, and no system was actually

compromised.” April Notice (Dkt. No. 2994) (filed Apr. 8, 2005).

While Interior recognizes its duties to preserve IITD and has devoted substantial financial and human resources to that end, Interior has a vast array of critical duties, mandated by statute, including but not limited to matters affecting Native American health, education, and housing; the maintenance and protection of natural resources, including fire-fighting systems; and matters affecting national security and the nation's critical infrastructure. See, e.g., National Park Service Organic Act, 16 U.S.C. § 1 et seq.; Indian Law Enforcement Reform Act, 25 U.S.C. 2801 et seq.; Surface Mining Control and Reclamation Act of 1977, 30 U.S.C. § 1201 et seq.; Federal Oil and Gas Royalty Management Act, 30 U.S.C. § 1732; Reclamation Act, 43 U.S.C. § 411; Outer Continental Shelf Lands Act, 43 U.S.C. §§ 1331 et seq.; Federal Land Policy and Management Act, 43 U.S.C. § 1701 et seq. Even assuming for the sake of argument that Interior could continue to perform these varied and important functions without the benefit of IT systems, it is beyond dispute that it could only do so at an extraordinary cost and with substantial disruption to its operations.

In the same fashion as their argument regarding the harm to Interior’s operations, Plaintiffs’ Motion asserts that the granting of the injunctive relief sought in their motion “cannot harm the public interest.” Pl. Mot. at 33. In making this argument, Plaintiffs focus solely on the preservation of IITD – again without any showing of destruction or alteration of IITD – and make no attempt to justify the impact upon the public from the disconnection and shut down which they seek.

Plaintiffs’ focus upon an undefined and theoretical risk to IITD – again, with no showing of actual harm to any IITD housed or accessed by Interior’s systems – completely ignores the real

harm which would flow from the relief they request. Because many of Interior's trust systems have been disconnected from the Internet for over three years, Interior's ability to communicate with beneficiaries and process transactions for beneficiaries has been hampered and made more costly. Now, Plaintiffs seek both an order of disconnection and an unprecedented "shut down" for systems that house or access IITD. In seeking such relief, Plaintiffs even seek to terminate the operation of systems that are currently disconnected from the Internet.

If the Court were to grant Plaintiffs' request for an order disconnecting systems housing or accessing IITD from the Internet, the impacts upon Interior and the public would be substantial. As the Court is aware from prior disconnection orders, the Internet connection is critical for MMS's processing of royalties and related payments. See Tipton Decl. at 17(c). The processing of royalties in excess of \$500 million per month would be severely hampered by another order to disconnect systems housing or accessing IITD from the Internet. Id.

In addition, the public impacts would include areas as diverse as procurement, access to broad and diverse forms of data, and FOIA requests. Tipton Decl. at 17(a), 17(b) and 17(e). Moreover, the issuance of a disconnection order would prevent any affected bureau or office from electronically obtaining security software updates and patches, including anti-virus definition files and intrusion detection system signature files. Id. at 17(d). While such harms to Interior and the public have been documented in connection with prior disconnection orders, e.g., Defendants' Emergency Motion to Stay Preliminary Injunction Pending Appeal and for Expedited Consideration at 12-15 (Dkt. No. 2549) (filed Mar. 22, 2004), Plaintiffs wholly ignore them in their latest request for a Temporary Restraining Order.

Now, Plaintiffs seek even more than disconnection from the Internet; they seek to shut

down computer systems entirely. In spite of this, Plaintiffs' justification for their request devotes slightly less than one page to their discussion of the public harm and wholly ignores previously documented public harm resulting from disconnection orders. Plaintiffs instead rely upon another attack upon the Secretary of the Interior, rather than a serious discussion of the public harm that would result from their request. Pl. Mot. at 33-34.

It should be beyond any serious dispute that an order to shut down computer systems – whether currently connected to the Internet or disconnected – would have severely disruptive impacts upon Interior and would harm the public. While it is impossible to list every adverse impact from such an order, a few examples illustrate the imprudence of such an order. An order to shut down IITD systems would impede or prevent the Interior's (including the Bureau of Indian Affairs, the Office of the Special Trustee and the Minerals Management Service among others) processing activities in a variety of areas affecting beneficiaries, including the electronic processing of payments or the providing of statements to beneficiaries, and would stop the majority of trust reform initiatives among all of the trust bureaus. Tipton Decl. at 18(a), 18(b) and 18(c). Further, such an order would effectively halt Office of Historical Trust Accounting activities, including ongoing accounting activities. Id. at 18(d). A shutdown order would stop MMS's operations with respect to collecting, accounting for, verifying and distributing revenues derived from Indian, federal and state oil, gas, and mineral leases totaling in the billions of dollars each year. Id. at 18(e). BLM would also be severely impacted by a shutdown order in that oil, gas, and minerals permitting actions, which are necessary for leasing and production, would cease on all on-shore public lands. Id. at 18(f).

In summary, Plaintiffs' Motion wholly ignores the impacts upon the operations of Interior

and the public, including members of the Plaintiff class. Plaintiffs elevate the protection of IITD against theoretical harms to a level that supercedes all real impacts upon governmental operations and the general public. No circumstances justify the relief requested by Plaintiffs in the face of its impacts upon both Interior and the public.

Conclusion

Plaintiffs' Motion fails to establish any of the four elements necessary for the granting of a temporary restraining order or a preliminary injunction. It should be denied.

Respectfully submitted,

ROBERT McCALLUM, JR.
Associate Attorney General

PETER D. KEISLER
Assistant Attorney General

STUART E. SCHIFFER
Deputy Assistant Attorney General

/s/ John Warshawsky

J. CHRISTOPHER KOHN
Director (D.C. Bar No. 261495)
JOHN T. STEMPLEWICZ
Senior Trial Attorney
JOHN WARSHAWSKY (D.C. Bar No. 417170)
Trial Attorney
GLENN D. GILLET
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 307-0010
Facsimile: (202) 514-9163

April 18, 2005

CERTIFICATE OF SERVICE

I hereby certify that, on April 18, 2005 the foregoing *Defendants' Opposition to Plaintiffs' Consolidated Motion for Temporary Restraining Order and Preliminary Injunction* was served by Electronic Case Filing, and on the following who is not registered for Electronic Case Filing, by facsimile:

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

/s/ Kevin P. Kingston
Kevin P. Kingston

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

DECLARATION OF W. HORD TIPTON IN SUPPORT OF
DEFENDANTS' OPPOSITION TO PLAINTIFFS' CONSOLIDATED MOTION
FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

1. I, W. Hord Tipton, am the Chief Information Officer ("CIO") for the United States Department of the Interior. In this capacity, I oversee management of the information technology ("IT") systems and implementation of applicable Interior policies and directives. I also coordinate with bureau/office CIOs in the development and maintenance of bureau-specific IT systems and am responsible for overseeing the portfolios of all IT investments and spending for Interior. In performing my duties, I rely upon information from Interior management and staff to make program management decisions and to prepare communications with the Court, as is the case with this declaration. I am a Certified Information System Security Professional (CISSP #57493) and also am an Information System Security Engineering Professional (ISSEP).

2. The Interior Department is a cabinet level agency with an annual budget of almost \$16 billion and approximately 77,000 employees. It is responsible for managing one out of every five acres of land in the United States; provides the resources for nearly one-third of the nation's

energy; provides water to 31 million people through 900 dams and reservoirs; receives over 450 million visits each year to the parks and public lands it manages; and implements hundreds of statutorily-mandated programs. In addition, the Department provides a variety of critical services on which other federal agencies rely.

3. To meet its responsibilities, the Department manages an IT portfolio of approximately \$1 billion annually, including approximately 110,000 computers. Surveys by the Department have shown that approximately 6,600 of those computers, i.e., approximately 6 percent, house or access Individual Indian Trust Data ("IITD").

4. I have read Plaintiffs' Consolidated Motion for Temporary Restraining Order and Preliminary Injunction ("Plaintiffs' Motion") and am aware that Plaintiffs have asked this Court to order Interior's IT systems housing or accessing IITD to be disconnected from the Internet and shut down. Plaintiffs' Motion contains erroneous assertions regarding IT security procedures and standards and the state of IT security within the Interior Department. This declaration corrects some of Plaintiffs' erroneous assertions and, further, describes some of the enormous harm to the Interior Department and the public that would result from the disconnection from the Internet and shutting down of Interior's IT systems housing or accessing IITD.

5. IT security is not designed with a goal of ensuring "absolute" security because there are always risks associated with the operation of any IT system. Rather, IT security measures are intended to provide sufficient security to ensure that risks to data are kept at acceptable levels, given the criticality and sensitivity of the data to be processed electronically. Since December 2001, Interior has devoted substantial resources to IT security. These resources

include the investment of more than \$100 million in its IT security program, as well as the dedication of an enhanced IT security personnel presence within the Department. The state of IT security as of December 2001 is not comparable to what exists today, which is dramatically improved. For example, in 2002, none of Interior's IT systems were certified and accredited under the then-existing guidelines promulgated by the National Institute of Standards and Technology ("NIST"). By comparison, approximately 96 percent of Interior's IT systems currently have been certified and accredited in accordance with NIST standards. Moreover, while Interior had three CISSPs in our security program in 2001, Interior currently has sixty-three CISSPs employed in our security program.

6. As is further explained below, the April 8, 2005 disclosure by the Government to this Court reflects an aggressive, ongoing program of self-testing by the Department, utilizing independent Office of the Inspector General scrutiny. We expect this program of self-testing to expose potential vulnerabilities; indeed, that is a central purpose of this program. By subjecting Interior to robust internal testing of our own IT systems, we aim to be in a position to improve our IT security profile on a constant basis. This is especially important as systems are modernized and "legacy" IT systems are replaced, modified, and improved, resulting in the reconfiguration of IT systems. The dynamic nature of maintaining current technologies often creates inadvertent vulnerabilities that are only detected through a prudent monitoring program.

7. The April 8, 2005 disclosure to the Court reveals a serious problem with BLM's Internet perimeter security regarding web services on publicly accessible servers, i.e., servers that are intended for public access. Interior has taken this information seriously, and it is being addressed by BLM. Moreover, given prior findings reported to me by the Inspector General with

respect to non-trust bureaus, Interior may have a systemic problem regarding Internet perimeter security for web services on publicly accessible servers. To address this possibility, my office has distributed “lessons learned” information to bureaus and offices and has reinforced this at an Interior-wide meeting/teleconference with bureau and office CIOs. Further, my office is in the process of officially issuing a directive to all CIOs and system owners outlining the nature of the Inspector General’s findings and directing corrective action.

8. Although I consider this vulnerability to be serious, and Interior is acting rapidly to remediate it, I do not consider this to reflect overall systemic problems with IT security at the Department of the Interior as a whole. To the contrary, the test results provided by the Inspector General demonstrate the effectiveness of the Department’s testing program in providing valuable information to further increase the security of Interior’s IT systems. It is important in this regard to reiterate that IT security takes place in a dynamic, not static, setting. Changes affecting IT security are always in progress, and the Department is constantly engaged in self-monitoring and self-improvement. For example, Interior is now in the process of consolidating its thirty-three Internet Points of Presence (“POPs”) – the connection point between Interior and the Internet – into five POPs centrally managed by the Enterprise Service Network, a centralized security control center. This will improve the efficiency of overall security management, including prevention and detection abilities throughout the Department, but will nevertheless require our continued vigilance to assure inadvertent vulnerabilities are remedied while changes are implemented. In addition, the Enterprise Service Network will include a separate “Trust DMZ” for trust entities, i.e., trust bureaus and segments of bureaus with trust data, to provide greater

protection for trust data.

IT Security Procedures and Standards/State of IT Security Within Interior Department

9. Since late 2002, Interior has conducted monthly scanning of the perimeter of Interior's IT networks, using an independent contractor who benchmarks Interior against the SANS "Top 20" list. The SANS Top 20 list is an industry-accepted standard for critical vulnerabilities scanning of IT system perimeters. The SANS Top 20 list is relied upon as a widely accepted standard within the government and the private sector. See www.sans.org/top20/ ("The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus"). The monthly reports generated from these scanning activities have been provided to each of Interior's Assistant Secretaries, bureaus and offices, and are part of the continuous monitoring phase of the Certification and Accreditation ("C&A") process defined in NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004 ("NIST SP 800-37"). Interior's independent contractor has reported no SANS Top 20 vulnerabilities discovered over the past fifteen months of scanning.

10. The April 8, 2005 disclosure to the Court stemmed from penetration testing beyond the SANS Top 20 vulnerabilities by the Office of the Inspector General, which utilizes the services of an IT security firm. The Inspector General's penetration testing program began in October 2004, as part of a larger comprehensive program to monitor and assess security controls placed on Interior's IT systems, in compliance with requirements of the continuous monitoring final phase of the C&A process described in NIST SP 800-37. This testing is in addition to the normal oversight function of the Office of the Inspector General and is funded by the Department of the Interior. The Memorandum of Understanding ("MOU") between the Office of the

Secretary and Interior's Inspector General includes a section establishing the framework for "Network Security Monitoring" ("NSM"). That section provides, in part, that the NSM framework is designed to serve the goal and objective of "establishing a baseline/benchmark for DOI perimeter security using the SANS Top 20, to improve the level of perimeter security."

11. The potential discovery that security controls are not as effective as anticipated is specifically contemplated by NIST SP 800-37:

If the results of the security assessment indicate that selected controls are less than effective in their application and are affecting the security of the information system, corrective actions should be initiated and the plan of action and milestones updated.

NIST SP 800-37, Subtask 9.2, Selected Security Control Assessment, at 45.

12. Furthermore, the Plaintiffs' Motion provides an inaccurate portrayal of the Inspector General's findings. For example, on page 20 of the Plaintiffs' Motion, the Plaintiffs asserted, "Of the nineteen systems reviewed which were certified and accredited, twelve (63 percent) did not have a risk assessment." In fact, the Inspector General affirmed a "satisfactory" certification & accreditation (C&A) process, with 19 of 19 systems reviewed (100%) having risk assessments. Only the completeness of compliance with NIST SP 800-30 was questioned by the Inspector General as of August 2004, and Interior addressed this as a component of independent package reviews subsequently performed for trust systems in October 2004. During this time, Interior engaged numerous contractors with specialized skills to complete the C&A process, and their active participation was utilized by the bureaus and offices in this on-going process.

13. The Inspector General's penetration testing has progressed with frequent and interactive sessions for six months. In these sessions, vulnerabilities discovered have been

discussed with the relevant bureaus, and remediation actions scheduled commensurate with the risk to Interior's missions. When the Inspector General identified an elevated risk with specific reference to IITD in the case of BLM, Interior notified the Court and responded aggressively to ensure the protection of all mission data, with special actions related to IITD. The BLM exposure identified by the Inspector General created potential risk to employee working files that support IITD-related activities, and decisive remediation actions have been directed by the highest levels of BLM management, who have maintained multiple daily conferences to assess risk and plan remediation.

14. Based on my day-to-day involvement with this process and in light of improvements Interior has made and continues to make, I believe that IITD is at much less risk from unauthorized Internet access today than at any time in the past. This judgment on my part takes into account the nature and degree of sensitivity of the information involved, the risk of harm if unauthorized access to the information were to occur, and the protections in place to guard against such unauthorized access.

Harm to Interior Department and the Public

15. The Internet is a crucial, and often the primary, way by which the Department communicates with the world. For example, by means of the Internet, the Department maintains numerous databases regularly used by governmental organizations and private persons. As mandated by law and government-wide regulations, the Internet is the primary means by which the Department receives most proposals for Department contracts. It is a crucial means by which the Department distributes certain royalty payments. Further, the Internet serves as a principal source of support for the Department's ongoing efforts to provide and improve IT security.

16. As a result of the Department's statutory duties, Interior provides services critical for protection against fires and other threats to life and property. The disconnection of systems critical to these services – to say nothing about the shutting down of such systems sought in Plaintiffs' Motion – would have obvious catastrophic impacts upon the operations of the Interior Department and would expose the public to serious harm.

17. Even if the relief sought by the Plaintiffs provided an exception for systems necessary to protect against fires and other threats to life or property, the operations of the Interior Department and the public would be seriously harmed. While it is impossible to catalog all the forms of harm to Interior and the public from the requested order, the following provides illustrative examples of harms that would result from a disconnection order.

(a) Procurement: MMS/Gov Works, through its Franchise Fund operation, provides acquisition services to virtually every federal agency involved in national security operations either domestically or in other countries, including the Executive Office of the President, the Department of Homeland Security, the United States Secret Service, and the Department of the Treasury. Because of their diverse locations, the Internet is the primary line of communication with these agencies and the contractors who support them. The Internet is used to receive requirements, conduct necessary acquisition actions, provide contract administration, and process timely payments to contractors. Disconnection will jeopardize the delivery of critical services.

(b) Financial Management: MMS's Public Information Data System ("PIDS") is a huge electronic repository of publicly available document images, consisting of documents such as geophysical and geological permits, plans of exploration and development, and drilling permits. This system contains over one million documents and thousands of documents on average are added weekly. The absence of PIDS will require customers to visit the Public Information Office to retrieve copies of electronic documents. However, many of the paper copies of documents contained within PIDS are no longer immediately accessible at the MMS office, as they have been archived at Federal Records Centers.

(c) MMS Royalties: Disconnection will adversely affect the ability of MMS to receive, process, and disburse over \$500 million in oil, gas, and mineral revenues on federal and Indian leased lands each month. MMS accomplishes its assigned mission

through delivery of reporting, accounting, and financial services. Thousands of companies report and pay royalties to MMS each month. All such functions are heavily reliant on the automated systems and access to the Internet. Minerals revenues are a major source of income for Tribes, individual Indians, the federal government, and states.

(d) IT Security: Disconnection will undermine and impede the progress the Department has already made with regard to IT security. For example, disconnection will prevent any affected bureau or office from electronically obtaining security software updates and patches, including anti-virus definition files and intrusion detection system signature files. Further, disconnection will impact policy and training requirements imposed by the Federal Information Security Management Act ("FISMA") as security practitioners.

(e) E-FOIA: The Department has Electronic Freedom of Information Act ("E-FOIA") capabilities required by 5 U.S.C. § 552(a)(2)(E). E-FOIA requires the Department to make records subject to FOIA electronically available. The total number of FOIA requests will increase, and the FOIA program will be impaired, as a result of disconnection because the public information currently available will no longer be available on-line.

18. In addition to seeking disconnection of systems housing or accessing IITD from the Internet, Plaintiffs have requested an order seeking the complete shutdown of all systems housing or accessing IITD. In addition to the impacts described above for disconnection, a "shutdown" order would also impact the bureaus and offices that have never been reconnected to the Internet since December 2001, i.e., the Bureau of Indian Affairs ("BIA"), the Office of the Special Trustee ("OST"), the Solicitor's Office, and the Office of Hearings and Appeals. Moreover, it would require the shutting down of all systems at the Office of Historical Trust Accounting. A shutdown order of the kind requested would go beyond those bureaus and offices currently connected to the Internet; it would prevent all bureaus and offices with systems housing or accessing IITD from conducting internal computer operations, regardless of whether they had any connection to the Internet. Such an order would cripple the Department and its ability to serve the public. Again, while it is impossible to catalog all the forms of harm to Interior and the

public from this aspect of the requested order, the following provides illustrative examples of harms that would result from an order to shutdown systems housing or accessing IITD:

(a) BIA's processing of probates, title tracking, lease management, ownership changes, and related payments are dependent upon computer systems, and such processing would be severely impeded.

(b) OST would not be able to electronically process payments for royalties or provide statements to beneficiaries.

(c) The majority of trust reform initiatives among all of the trust bureaus would cease.

(d) OHTA's activities, including ongoing accounting activities, would effectively cease.

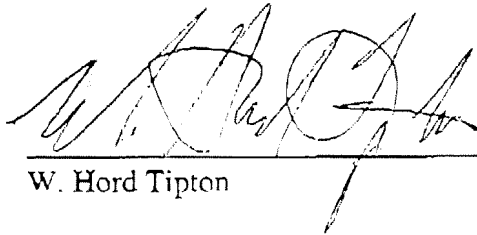
(e) As explained above, MMS is responsible for, among other things, collecting, accounting for, verifying and distributing revenues derived from Indian and federal oil, gas, and mineral leases totaling in the billions of dollars each year. In conjunction with the harms previously described for MMS resulting from Internet disconnection, MMS's operations are dependent upon computer systems, and such operations would cease.

(f) Electronic oil, gas, and minerals permitting actions, which are necessary for leasing and production verification, would cease on all on-shore public lands if BLM's Automated Fluid Minerals System were shut down.

19. In summary, it is my opinion that although ongoing testing on Interior systems has demonstrated that vulnerabilities relating to web services have been detected in the systems tested to date for four bureaus, Interior's overall IT security is acceptable. Interior and the Inspector General have added an extended layer of vulnerability scanning and other techniques that exceed recommendations in the SANS Top 20 list. This is improving our overall security posture as newly identified vulnerabilities are assessed and either mitigated or accepted. Furthermore, it is my opinion that the harm to the Department of the Interior and the general

public that would be caused by the relief sought in Plaintiffs' Motion is not justified by the vulnerabilities discovered by the Inspector General.

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

 4-18-2005

W. Hord Tipton

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

DECLARATION OF RONNIE LEVINE IN SUPPORT OF DEFENDANTS’
OPPOSITION TO PLAINTIFFS CONSOLIDATED MOTION FOR
TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

1. I, Ronnie Levine, am the Chief Information Officer for the Bureau of Land Management, United States Department of the Interior (“BLM”). In this capacity, I oversee management of the information technology (“IT”) systems under the control and custody of BLM in accordance with applicable Department of the Interior policies and directives. I also coordinate with the Denver National Information Resource Center (“NIRMC”) concerning the Internet points of presence, IT security and other matters concerning BLM IT resources. In performing my duties, I rely upon information from BLM management and staff to make management decisions and to prepare communications with the Court, as is the case with this declaration.

2. On March 22, 2005, in Washington, D.C., I was notified that an unannounced penetration test on BLM’s IT systems under a program managed by the Office of the Inspector General (“OIG”) was complete. Preliminary and partial information regarding the results of the penetration test were provided on that day; however, the preliminary information provided did

not indicate that individual Indian trust data (“IITD”) could have been accessed during the testing. Upon receipt of the information from OIG, a copy of the preliminary report was faxed to NIRMC personnel in Denver and the BLM Deputy CIO who was onsite at NIRMC on March 22, 2005. The Deputy CIO met with NIRMC staff on March 22, 2005, to review the preliminary findings. Following this review, the NIRMC staff was directed to take prompt action to address the OIG preliminary findings. These actions were completed within one day and included: independently confirming the results of the tests; shutting down an Internet accessible database; and password protecting security reports that were accessible from the Internet. Additional technical solutions including configuration changes to the proxy device were completed by March 25, 2005. However, some issues identified in the preliminary report could not be addressed without specific technical details contained in the full report which had not yet been provided to BLM.

3. On the evening of April 6, 2005, BLM received the formal OIG Findings and Recommendations (the “OIG Report”) and a supporting technical report. BLM management immediately reviewed these documents and learned for the first time that IITD on the BLM IT systems was potentially at risk.

4. Upon learning that IITD on the BLM IT systems was potentially at risk, BLM management took prompt action to address the additional issues contained in the formal OIG Report and supporting technical report. The BLM Director convened several meetings throughout the day on April 8, 2005, to address and analyze the findings in the OIG Report and direct appropriate staff to take prompt action to address the findings in the OIG Report. The April 8, 2005 meetings included a meeting with a panel of IT personnel from BLM and the

Office of the Chief Information Officer (“OCIO”) (including personnel from the Cyber Security Division, OCIO) to further assess the findings, evaluate remedial actions already taken and evaluate future remedial actions. The Director of BLM, with her panel of IT personnel, held additional meetings throughout the day with individuals from the OIG, the Department of Justice, the Office of the Solicitor and the Office of the Secretary.

5. On April 8, 2005, following consultation with the Department, at the direction of the BLM Director, the BLM CIO eliminated all external Internet access to BLM web servers with the exception of mail servers and those web servers necessary to support the preservation of life and safety, especially fire fighting mission activities. This action was completed in the evening of April 8, 2005.

6. On April 8, 2005, BLM identified file servers housing or accessing IITD and disconnected those servers from the rest of the BLM network (the “Trust Servers” or “Trust Systems”). BLM also identified individual users on the BLM network who had previously certified that their desktops or laptops contained IITD and completed the disconnection of those computers from the BLM Network on April 13, 2005. E-mail user passwords were reset and the system was configured to require more complex password generation and account expiration every ninety days.

7. On April 12, 2005, the BLM Director established a BLM IT Incident Command Center (the “IT ICC”) to serve as the central point of coordination for addressing issues identified in the OIG Report. The primary goal of the IT ICC is to assure the prompt, efficient, and effective completion of appropriate solutions to the IT security issues raised by the OIG Report.

8. BLM State and Center CIOs have been required to certify that all desktop computers

containing IITD that will be attached to the BLM network are properly configured to store all data only on network storage devices so as to prevent the storage of IITD on desktops computers. BLM end users will re-certify that they are in compliance with directives prohibiting the storage of IITD or tribal Indian trust data on local workstations.

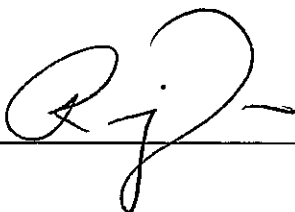
9. In addition to the completed actions described above, BLM initiated a program to further harden its security infrastructure. This includes strengthening the network perimeter and placing all Internet accessible web servers in a hardened Demilitarized Zone (“DMZ”). A DMZ is a computer or small sub-network that sits between a trusted internal network, such as the BLM internal network, and an untrusted external network, such as the public Internet. The DMZ contains devices accessible to Internet traffic, such as web servers, e-mail servers, and domain name servers. Once the new DMZ configuration is established, the web servers related to preservation of life and safety, especially fire fighting, will be moved into the DMZ. Those systems will be tested for potential vulnerabilities once they are located in the hardened DMZ. The blm.gov web server, also to be located in the hardened DMZ, will be tested by an external vendor to assure that the hardened DMZ adequately addresses all Web findings noted in the OIG Report as well as others identified by BLM and the Department. The results of that test will be validated by the DOI OCIO Cyber Security Office with concurrence by the IT ICC prior to permitting public access to the blm.M.gov web server. Only after these steps are completed successfully will other web servers be allowed to operate behind the DMZ. Each server and system will require independent assessment to verify adequate security prior to reconnection to the Internet.

10. The Trust Servers will not be allowed to reconnect to the BLM internal network until the

new DMZ has been successfully established, tested, the OIG determines that potential vulnerabilities have been adequately addressed.. .

11. Through the steps taken promptly after the OIG Report was given to BLM, BLM has ensured that all IITD housed in the Trust Servers and Trust Systems within the BLM IT network is adequately secure. BLM will continue to investigate risk mitigation strategies to further protect IITD and Trust systems. Further, BLM has taken prompt steps to reduce risks to acceptable levels on the rest of its network by not allowing external access to web servers (except for mail servers and those servers necessary to support the preservation of life and safety, especially fire fighting) until the effectiveness of the BLM DMZ is reconfirmed through independent testing.

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



cc:

J. Christopher Kohn, Esq
John T. Stemplewicz, Esq
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Fax (202) 514-9163

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

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

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

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