IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 1:96CV01285
	)	(Judge Robertson)
DIRK KEMPTHORNE, Secretary of the Interior, et al.,	)	
	)	
Defendants.	)	
	)	

DEFENDANTS' MOTION TO VACATE CONSENT ORDER REGARDING INFORMATION TECHNOLOGY SECURITY

Pursuant to Rule 7(b) of the Federal Rules of Civil Procedure and Local Civil Rule 7, Defendants respectfully move this Court for an Order vacating the Consent Order Regarding Information Technology Security (Dec. 17, 2001) (Dkt. No. 1063) ("Consent Order") upon the grounds that substantial changes in the law and the undisputed facts since entry of the Consent Order render it no longer appropriate or justified, as a matter of law. In accordance with Local Civil Rule 7(m), Defendants' counsel conferred with Plaintiffs' counsel on March 19, 2007, and Plaintiffs' counsel stated that this motion would be opposed.

I. Introduction

More than five years after the Consent Order was entered; following three subsequent Information Technology ("IT") security orders entered by this Court in 2003, 2004, and 2005, which plainly were designed to supercede the Consent Order; and in the wake of two separate opinions of the D.C. Circuit which directly addressed and vacated this Court's subsequent IT security orders; the Consent Order nominally remains in force, despite being stripped of virtually all of its legal and factual underpinnings. The vestige of this order continues to prevent the Department of the Interior ("Interior") from considering whether to reconnect important IT

systems – particularly those of the Bureau of Indian Affairs, the Office of the Special Trustee, the Office of Hearings and Appeals, and the Solicitor's Office – to the Internet or to any internal Interior network providing connectivity to the IT systems of other "reconnected" Interior bureaus and offices. The anachronistic nature of the Consent Order is all the more apparent in light of the evolution of federal law regarding IT security, the undeniable investment of massive resources into the improvement of Interior's IT security, and the equally clear fact that, despite bald assertions to the contrary, Plaintiffs have never demonstrated any real basis for injunctive relief, a conclusion confirmed by the latest appellate court decision addressing IT security.

The time is ripe for this Court to allow Interior to move forward, properly utilizing its IT systems to fulfill its statutory duties. For the reasons set forth in the following brief, Defendants respectfully request that this Court enter its Order vacating the Consent Order.

II. Factual Overview

A. December 5, 2001 Temporary Restraining Order

On November 14, 2001, the Special Master then-assigned to this case, Alan L. Balaran,[1] issued a document identifying IT security deficiencies that the Special Master believed could detrimentally affect the integrity of individual Indian trust data ("IITD"). Report and Recommendation Regarding the Security of Trust Data at the Department of the Interior (Dkt. No. 932). Three weeks later, this Court entered a TRO which, among other things, ordered

> that Interior defendants shall immediately disconnect from the Internet all information technology systems that house or provide access to individual Indian trust data; and . . .

[1] Mr. Balaran submitted his resignation as Special Master to the Court on April 5, 2004, and his resignation was accepted by the Court's Order entered April 6, 2004. Order (Apr. 6, 2004) (Dkt. No. 2557).

> that Interior defendants shall immediately disconnect from the Internet all computers within the custody and control of the Department of the Interior, its employees and contractors, that have access to individual Indian trust data.

Temporary Restraining Order (Dec. 5, 2001) (Dkt. No. 1036), as amended by Order (Dec. 6, 2001) (Dkt. No. 1038).

B. The Consent Order

On December 17, 2001, this Court entered the Consent Order, agreed to by Interior but not Plaintiffs, which established a process to allow Interior to reconnect to the Internet IT systems that had been disconnected as a result of the December 5, 2001 TRO. See Consent Order at 5-8. Pursuant to the Consent Order, the Special Master was to review, among other things, (1) submissions identifying IT systems which did not house or provide access to IITD[2] and (2) plans for securing IT systems that housed or provided access to IITD, accompanied by documentation that demonstrated "adequate security" existed to protect IITD on such systems. Consent Order at 5-6, 7.

The Consent Order gave the Special Master far-reaching discretion to make determinations regarding Interior's IT security. For example, the Consent Order provided that the Special Master could "object[] to the plan because it does not provide adequate security for individual Indian trust data," and Interior "shall not reconnect until such objections have been resolved to the satisfaction of the Special Master." In addition, the Special Master was authorized to "verify compliance" and to "conduct interviews with Interior personnel or contractors or conduct site visits wherever information technology systems or individual Indian

[2] Because such systems did not house or provide access to IITD, they were expressly exempt from the TRO's disconnection requirements.

trust data is housed or accessed."[3] In total, nine of the twelve provisions within the Consent Order addressed the duties assigned to the Special Master.

Following entry of the Consent Order, Interior devoted substantial resources to remedying IT security deficiencies and submitted numerous reconnection proposals to the Special Master. As a result of these efforts, within a year following entry of the Consent Order, approximately 95 percent of Interior's IT systems had been reconnected to the Internet. Cobell v. Kempthorne, 455 F.3d 301, 303 (D.C. Cir. 2006), petition for cert. filed, 75 U.S.L.W. 3333 (U.S. Dec 19, 2006) (No. 06-867).

C. FISMA

Slightly less than one year following entry of the Consent Order, Congress passed and the President signed into law the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat 2899. Statement by the President, 2002 WL 31826815 (Dec. 17, 2002). Title III of this law is the Federal Information Security Management Act of 2002 ("FISMA"). See Pub. L. No. 107-347, Title III, §§ 301-305. By enacting FISMA, Congress accomplished the following:

> • Permanently authorize[d] the government-wide risk-based approach to information security by striking the [then-] current 44 U.S.C. 3536, thus eliminating [the Government Information Security Reform Act's (GISRA)] two-year sunset;
>
> • Strengthen[ed] Federal information security by requiring compliance with minimum mandatory management

---

[3] Whether this provision allowed monitoring of IT systems following reconnection of previously disconnected systems ultimately became an issue in June 2003. See Cobell v. Norton, 274 F. Supp. 2d 111, 125 (D.D.C. 2003), vacated, 391 F.3d 251 (D.C. Cir. 2004). Interior viewed these provisions as only authorizing activities to assess proposals to reconnect IT systems to the Internet. The Court, however, construed the Consent Order as authorizing continuing post-reconnection testing and oversight of Interior's IT systems. 274 F. Supp. 2d at 125.

controls for securing information and information systems to manage risks as determined by agencies;

- Improve[d] accountability and congressional oversight by clarifying agency reporting requirements and ensuring access to information security evaluation results by the GAO;

- Improve[d] compliance by streamlining a number of GISRA requirements and clarifying inconsistent and unclear terms and provisions;

- Clarifie[d] provisions regarding responsibilities for national security systems;

- Improve[d] Federal information security by strengthening the role of [the National Institute of Standards and Technology ("NIST")]; [and]

- Streamlin[ed] statutory requirements by repealing duplicative provisions in the Computer Security Act and the Paperwork Reduction Act.

H.R. Rep. No. 107-787 (Part 1), at 58 (2002), reprinted in 2002 U.S.C.C.A.N. 1880, 1893.

D. The Court's IT Injunctions

As noted above, following entry of the Consent Order, Interior undertook a committed effort to address security deficiencies in its IT systems. Beginning in the summer of 2002 and continuing in 2003, Interior undertook an effort with the Special Master whereby his technical representatives performed remote network scanning and penetration testing of Interior's IT systems.[4] See 12th Status Report of Interior at 10 (Feb. 3, 2003) (Dkt. No. 1764).

---

[4] Remote network scanning is one technique for determining potential IT security vulnerabilities. One district court has described such testing as follows:

> A port scan is a method of checking a computer to see what ports are open by trying to establish a connection to each and every port on the target computer. If used by a network administrator on his own network, the scan is a method of

By late spring of 2003, however, the working relationship between the Special Master and the Government had deteriorated. Cobell v. Norton, 391 F.3d 251, 255 (D.C. Cir. 2004). Among other things, the relationship between the Special Master and the Government was undermined by disagreements that arose in the context of network scanning and penetration testing of Interior's IT systems. See, e.g., Cobell v. Norton, 274 F. Supp. 2d 111, 114-19 (D.D.C. 2003), vacated, 391 F.3d 251 (D.C. Cir. 2004).

The broken relationship with the Special Master rendered the Consent Order unworkable. Thus, this Court initially entered a TRO generally ordering Interior to disconnect its IT systems, again, in late June 2003. TRO (June 27, 2003) (Dkt. No. 2118). Following briefing and argument, this Court stayed the Consent Order on July 28, 2003, and entered a preliminary injunction in its place. Preliminary Injunction (July 28, 2003) (Dkt. No. 2159).

Pursuant to the July 2003 preliminary injunction, Interior submitted materials directly to this Court, and on March 15, 2004, this Court entered another preliminary injunction which superceded and replaced the July 28, 2003 preliminary injunction. Preliminary Injunction (Mar. 15, 2004) (Dkt. No. 2531). Like the TRO and preliminary injunction entered in mid-2003, the 2004 preliminary injunction broadly directed Interior not to reconnect any then-disconnected IT

> determining any possible security weaknesses. If used by an outsider, the scan indicates whether a particular port is used and can be probed for weakness.

Moulton v. VC3, 2000 WL 33310901 *1 (N.D. Ga. Nov. 7, 2000). The testing undertaken by the Special Master's experts was "remote" because it was being conducted "outside" the IT systems being scanned. "Penetration testing" followed remote scanning and referred to attempts by the Special Master's experts to gain unauthorized access to Interior's IT systems through vulnerabilities identified during the scanning efforts. See Cobell v. Norton, 394 F. Supp. 2d 164, 167 (D.D.C. 2005), vacated, 455 F.3d 301 (D.C. Cir. 2006), petition for cert. filed, 75 U.S.L.W. 3333 (U.S. Dec 19, 2006) (No. 06-867).

systems and further directed Interior to disconnect systems of the Office of the Inspector General, Minerals Management Service, the Bureau of Reclamation, the Fish and Wildlife Service, the Office of Surface Mining, and Interior's National Business Center from the Internet. Id. ¶¶ B.1 and B.3. Moreover, it continued in place the stay of the Consent Order. Id. ¶ B.9.

The United States Court of Appeals for the D.C. Circuit consolidated appeals of the 2003 and 2004 preliminary injunctions, 391 F.3d at 256, and issued its opinion on December 3, 2004, vacating the 2004 preliminary injunction (which, as previously noted, had superceded and replaced the 2003 preliminary injunction). Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004). In doing so, the Court of Appeals concluded that this Court had committed "error to shift the burden of persuasion to the Secretary [of Interior] to show why disconnecting most of Interior's IT systems was unnecessary to ensure the security of IITD." Id. at 259 (citations omitted). The Court of Appeals further concluded that this Court abused its discretion when it issued the preliminary injunction without first holding an evidentiary hearing to ascertain the then-current state of Interior's IT systems security. Id. at 261-62.

E. 2005 to Present

1. This Court's Evidentiary Hearing and Resultant Order

On April 8, 2005, Defendants informed this Court that Interior's Inspector General had issued a report dated April 6, 2005, with respect to penetration testing results and potential findings and recommendations.[5] Defendants' Notice to the Court Regarding Inspector General's

[5] Following the enactment of FISMA, Interior's Inspector General took on a significantly enhanced role with regard to assessing IT security. See generally 394 F. Supp. 2d at 184-247. By 2005, the Inspector General's role had expanded to include conducting external penetration testing, utilizing the services of a private contractor. See id. at 201-23.

"Notification of Potential Finding and Recommendation" With Respect to Information Technology Systems (Apr. 8, 2005) (Dkt. No. 2924) ("Notice"). In the Notice, Defendants advised the Court that the Inspector General's report included the potential finding that the Inspector General's contractors could have compromised the confidentiality, integrity, and availability of IITD identified on certain IT systems. Notice at 2. The Notice further stated that the Inspector General's Notice had received and continued to receive the attention of senior management within the Office of the Secretary, the Office of the Chief Information Officer, and the bureau/office involved,[6] and that Interior would "take all steps necessary to ensure that any Indian trust data referenced in the Inspector General's Notification of Potential Finding and Recommendation [was] protected . . . ." Id.

On the next business day, Plaintiffs filed their motion for another TRO and preliminary injunction with regard to IT systems security. Plaintiffs' Consolidated Motion for Temporary Restraining Order and Preliminary Injunction (Apr. 11, 2005) (Dkt. No. 2926) ("Pl. Mot."). Significantly, Plaintiffs' motion stated that they had objected to entry of the December 17, 2001 Consent Order, Pl. Mot. at 7 note 16, and reiterated their "concerns about the inadequacy of the [Consent] Order," Pl. Mot. at 8. Thus, Plaintiffs rejected the protections of the Consent Order – which had been stayed by the Court's 2003 and 2004 Preliminary Injunctions – and asked the Court for broader injunctive relief than that provided by the Consent Order. E.g., Pl. Mot. at 6 (seeking TRO to "shut down – not merely disconnect[] from the Internet").

In response to Plaintiffs' motion, this Court "held a 59-day evidentiary hearing to

---

[6] For reasons of IT security, the Notice did not publicly disclose the relevant bureau or office.

evaluate Interior's current IT security." 455 F.3d at 308 (citing Cobell v. Norton, 394 F. Supp. 2d 164, 170 (D.D.C. 2005)). Following the hearing, this Court entered extensive findings of fact. See generally 455 F.3d at 308-11. In doing so, this Court made its own assessments regarding the adequacy of Interior's IT security program, rejecting and criticizing numerous aspects of the program. See 394 F. Supp. 2d at 247-70. Before proceeding to its legal conclusions, this Court concluded its factual determinations with its own judgment as to the level of security required to protect IITD:

> While all Interior IT systems generally should be expected to conform to industry and government standards for adequate IT security, its systems housing or accessing Trust Data must meet a higher standard. Any weaknesses in Trust systems identified during the IG's penetration testing, then, show both that the relevant system or network is not likely up to generally applicable security standards and, necessarily, that the relevant network or system does not meet the even higher fiduciary standard.

Id. at 270.

After concluding that "Interior has not properly emphasized IITD in its IT security efforts," id. at 272, this Court issued a wide-ranging injunction that generally directed the disconnection of all IT systems that housed or provided access to IITD "1. from the Internet; 2. from all intranet connections . . . ; 3. from all other [IT] Systems; and 4. from any contractors, Tribes, or other third parties." Id. at 277-78 (¶ II.A.).[7]

[7] The Court's injunction contained an exception for systems that "protect[ed] against fires or other such threats to life, property, or national security." 394 F. Supp. at 278 (¶ II.C).

This Court's injunction further provided for limited reconnections "not to exceed five (5) business days per month [of Trust systems] . . . for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." 394 F. Supp. 2d at 278 (¶ II.D).

Finally, this Court abandoned the Consent Order's process for reviewing proposals for the reconnection of IT systems – which it had pronounced a "failed process" as of 2003, 394 F. Supp. 2d at 168 – and substituted a new regimen whereby Interior was to submit reconnection proposals that were to

> include all of the following: (a) a uniform standard to be used to evaluate the security of all Information Technology Systems which House or provide Access to Individual Indian Trust Data within the custody or control of the United States Department of Interior, its bureaus, offices, agencies, agents, contractors, or any other third party; (b) a detailed process whereby the uniform standard will be applied to each such Information Technology System; (c) a detailed explanation of how such Information Technology System complies with the uniform standard; (d) copies of all documentation relevant to the security of each such Information Technology System; and (e) a plan to provide monitoring and testing on an ongoing basis and quarterly reporting to this Court regarding the security of such Information Technology Systems.

394 F. Supp. 2d at 279 (¶ E.1). This Court further ordered that Plaintiffs would be entitled to conduct discovery regarding each proposal and that they could file a response to the proposal within thirty days after concluding discovery. 394 F. Supp. 2d at 279 (¶ E.2). After that, the Court's order provided that it would "conduct any necessary evidentiary hearing and decide whether a proposed [IT] System may be reconnected and order further relief, as appropriate." 394 F. Supp. 2d at 279 (¶ E.3).

2. The Court of Appeals' Opinion With Respect to This Court's 2005 Order

On July 11, 2006, the Court of Appeals vacated this Court's 2005 Order. Cobell v. Kempthorne, 455 F.3d 301 (D.C. Cir. 2006), petition for cert. filed, 75 U.S.L.W. 3333 (U.S. Dec 19, 2006) (No. 06-867). In doing so, the appellate court reviewed this Court's extensive findings and determinations regarding the adequacy of Interior's IT systems and the statutory scheme established by FISMA to manage and provide oversight of IT security risks. Id. at 308-14. The appellate court noted that "[n]otably absent from FISMA is a role for the judicial branch," id. at 314, and concluded that "[t]his is not a FISMA compliance case, whether or not such an animal exists elsewhere." Id. (dictum).

Having rejected a judicial role for FISMA oversight, the D.C. Circuit stated that Plaintiffs failed to demonstrate the potential for harm to their class, "hav[ing] pointed to no evidence showing that anyone has already altered IITD by taking advantage of Interior's security flaws, nor that such actions [were] imminent." 455 F.3d at 315. The appellate court further rejected this Court's assessment of harm to Interior, stating it was "dubious that the public interest would benefit from an injunction . . . ." Id.

The appellate court recognized, as this Court did, that "'it is generally considered impossible to create a perfectly secure IT environment.'" 455 F.3d at 315 (quoting 394 F. Supp. 2d at 269). Thus, the D.C. Circuit rejected a future oversight role:

> The inherently imperfect nature of IT security means that if we granted injunctive relief here, based only on Interior's security vulnerabilities and not on a showing of some imminent threat or specific reason to be concerned that IITD is a target, we would essentially be justifying perpetual judicial oversight of Interior's computer systems.

455 F.3d at 315. The Court of Appeals concluded its opinion with this instruction to this Court:

> If the district court conducts any further proceedings directed at providing equitable relief in the area of Interior's IT security, it must keep in mind the balance between administrative and trust law that we explained in Part II, supra. A court cannot order programmatic supervision of an agency's operations, nor can it displace an agency as the actor with primary responsibility for carrying out a statutory mandate by prescribing "particular tasks for Interior to perform based on policies developed by the district court." Cobell XII, 391 F.3d at 258.

455 F.3d at 317.

At this stage of the litigation, four major offices and bureaus remain disconnected from the Internet, i.e., the Bureau of Indian Affairs, the Office of the Special Trustee, the Office of Hearings and Appeals, and the Office of the Solicitor. Moreover, the mechanism created for authorizing the reconnection of IT systems – review by a special master – is unavailable given the absence of a special master and developments in the law that render judicial oversight improper. Finally, changes in the underlying facts of the past five-plus years, such as the well-documented investment of new resources to IT security, see, e.g., 394 F. Supp. 2d at 272, render the Consent Order wholly unnecessary and inappropriate, as a matter of law. For the reasons set forth below, this Court should vacate the Consent Order.

III. The Consent Order is Interlocutory in Nature and, as Such, This Court Has the Inherent Power to Vacate It in the Interest of Justice

Putting aside the question of whether the Consent Order is of any current relevance, given this Court's multiple orders to stay its terms and Plaintiffs' outright rejection of the Consent Order, there can be no serious dispute that the Consent Order fails to constitute a final judgment. Instead, it is most akin to an "adjudicat[ion of] fewer than all the claims" at issue, see

Fed. R. Civ. P. 54(b), and as such, it is an interlocutory order. "[I]t is well settled that a federal court which enters an interlocutory order has the inherent power to reconsider or revise the order in the interest of justice." In re MMS Builders, Inc., 101 B.R. 426, 430 (D.N.J. 1989) (citing, inter alia, John Simmons Co. v. Grier Brothers Co., 258 U.S. 82, 88 (1922)); see Advisory Committee Notes to Fed. R. Civ. P. 60(b) (1946 Amendment) ("[I]nterlocutory judgments . . . are left subject to the complete power of the court rendering them to afford such relief from them as justice requires."). Similarly, it is well-recognized that an injunction, such as the Consent Order, should be modified or vacated if required by changes in the underlying law or facts. As one district court has explained:

> [C]ourts have continuing jurisdiction to terminate, dissolve, vacate, or modify an injunction or an interlocutory order in the event that changed circumstances require it. The Court's power may arise from a change of law or a change of fact.

University of Hawaii Professional Assembly v. Cayetano, 125 F. Supp. 2d 1237, 1240 (D. Haw. 2000) (citing, inter alia, In re Detroit Auto Dealers Ass'n, Inc., 84 F.3d 787, 789 (6th Cir. 1996), and United States v. Oregon, 769 F.2d 1410, 1416 (9th Cir. 1985)); see also Cobell v. Norton, 274 F. Supp. 2d at 133 (quotation and citations omitted).

In light of all that has transpired in this case since December 2001, including that (a) this Court expressly stayed the Consent Order's terms in the preliminary injunctions entered in 2003 and 2004, (b) this Court held a 59-day hearing and issued injunctive relief afterwards designed to supercede the terms of the Consent Order, (c) the judicial officer empowered to execute the terms of the Consent Order – the Special Master – ceased to address IT security issues when the

Court stayed the Consent Order in July 2003,[8] (d) Interior has devoted over $100 million to upgrade the security of its IT systems, (e) Plaintiffs have repeatedly rejected the Consent Order, and (f) the D.C. Circuit rejected the order entered by this Court following the 59-day hearing on IT security, justice plainly requires that the Consent Order be vacated. As we explain further below, the Consent Order should be vacated because substantial changes in the law and facts underlying its issuance have rendered the Consent Order no longer appropriate or justified.

IV. The Consent Order Should be Vacated Because Its Judicial Role for Oversight of Interior's IT Security Program Is Contrary to Subsequently Enacted Comprehensive Legislation

A. Federal Law Enacted After the Consent Order Makes the Executive Branch Principally Responsible for Determinations Regarding the Adequacy of IT Security and the Means to Achieve Adequate IT Security

When the Consent Order was entered in mid-December 2001, federal statutory law governing IT security within governmental entities was immature, and the role of the judiciary with regard to such matters was unclear. In the year following entry of the Consent Order, Congress undertook a major legislative effort to consolidate and strengthen federal law governing IT security within agencies. The result of this effort was FISMA, the purpose of which was summarized by its accompanying House Report as follows:

> The purpose of FISMA is to permanently authorize a government-wide risk-based approach to information security by eliminating GISRA's two-year sunset, and to further strengthen Federal information security by requiring compliance with minimum mandatory management controls for securing information and information systems, clarifying and strengthening current management and reporting requirements, and strengthening

[8] Further, as set forth in note 1, above, the Special Master resigned in April 2004.

> the role of [the] National Institute of Standards and Technology (NIST).
>
> In accomplishing this range of reforms, FISMA takes the significant step of consolidating current information security requirements spread across the GISRA, the Computer Security Act, the Clinger-Cohen Act, and the Paperwork Reduction Act. FISMA eliminates obsolete mandates, updates outmoded provisions, harmonizes overlapping requirements, and strengthens key requirements. The result is a clearer and stronger law to guide Federal agencies to provide needed improvements to the information security.

H.R. Rep. No. 107-787 (Part 1), at 54 (2002), reprinted in 2002 U.S.C.C.A.N. 1880, 1889.

Thus, among other things, FISMA consolidated various statutes and permanently established that the head of an agency – and no other person or entity –

> shall . . . be responsible for . . . providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction 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; . . . .

44 U.S.C. § 3544(a)(1)(A) (emphasis added); see Cobell v. Kempthorne, 455 F.3d at 313 (discussing and quoting 44 U.S.C. § 3544(a)(1)(A)).

FISMA also enhanced the role of NIST[9] by "requiring OMB to promulgate information security standards developed by NIST." H.R. Rep. No. 107-787 (Part 1), at 58 (2002), reprinted in 2002 U.S.C.C.A.N. 1880, 1893. Following the enactment of this statute, NIST established the

[9] NIST is a non-regulatory agency of the Commerce Department's Technology Administration. http://www.nist.gov/public_affairs/general2.htm.

"Federal Information Security Management Act Implementation Project," and since 2003, NIST has promulgated standards which are mandatory for federal agencies and standards of "general interest" to the IT security community."[10]

Finally, as a result of FISMA, NIST's Implementation Project contemplates two additional phases to follow the Phase 1 development of standards and guidance. Phase 2, known as the "Organizational Credentialing Program," is intended to "focus on the development of a

---

[10] As of December 21, 2006, NIST had promulgated the following standards in final form:

- FIPS Publication 199, entitled "Standards for Security Categorization of Federal Information and Information Systems" (February 2004)
- FIPS Publication 200, entitled "Minimum Security Requirements for Federal Information and Information Systems" (March 2006)
- Special Publication 800-37, entitled "Guide for Security Certification and Accreditation of Federal Information Systems" (May 2004)
- Special Publication 800-53, entitled "Recommended Security Controls for Federal Information Systems" (February 2005)
- Special Publication 800-59, entitled "Guideline for Identifying an Information System as a National Security System" (August 2003)
- Special Publication 800-60, entitled "Guide for Mapping Types of Information and Information Systems to Security Categories" (June 2004)
- Special Publication 800-18 (Revision 1), entitled "Guide for Developing Security Plans for Federal Information Systems" (February 2006).
- Special Publication 800-53 (Revision 1), entitled "Recommended Security Controls for Federal Information Systems" (December 2006)

See http://csrc.nist.gov/sec-cert/ca-schedule.html (Phase 1 development schedule). In addition, a "Guide for Assessing the Security Controls in Federal Information Systems," referred to as Special Publication 800-53A, was in the process of being revised following publication in draft form for public comment and the receipt of comments. Id.

program for credentialing public and private sector organizations to provide security assessment services for federal agencies." http://csrc.nist.gov/sec-cert/ca-proj-phases.html. Phase 3, known as the "Security Tool Validation Program," is to "focus on the development of a program for validating commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) security tools."

In light of the passage of FISMA and the supporting NIST pronouncements, there can be no doubt that Congress has established new and extensive mandatory requirements for agency IT security programs with discrete and substantive roles for a variety of parties. Indeed, as the D.C. Circuit observed, "FISMA . . . includes a role for OMB, the Department of Commerce, the NIST, the Comptroller General, Congress, the public, and multiple officials with each agency subject to the statute." Cobell v. Kempthorne, 455 F.3d at 314. The Court continued, however, "Notably absent from FISMA is a role for the judicial branch." Id. As we explain below, the Consent Order's provisions for judicial review of Interior's IT security system run afoul of FISMA and the scheme Congress subsequently established for IT security oversight.

B. The Consent Order Inserts the Court Into the Role of the Decisionmaker Regarding the Levels and Forms of IT Security Required to Protect IITD, Contrary to FISMA's Assignment of This Responsibility to the Secretary of Interior

The Consent Order was entered almost one year before FISMA's enactment, and as explained above, its scheme made the Court, acting through the then-existing Special Master, solely responsible for determinations as to whether Interior's IT security was "adequate" to protect IITD. Thus, while FISMA makes the Secretary of the Interior responsible for assessing

"the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of [IITD]," 44 U.S.C. § 3544(a)(1)(A), the Consent Order provided for no such assessment. This is critical, because FISMA makes the Secretary responsible for IT security protections "commensurate" with his risk-management determinations.[11] By comparison, the Consent Order is essentially standardless, requiring the Special Master to assess whether IT security is "adequate" but providing no benchmark for assessing "adequacy."

The conflict between FISMA and the Consent Order goes beyond the absence of a standard for assessing the adequacy of IT security. Because it effectively provided the Special Master with unfettered discretion to reject reconnection plans based upon his view that the security was not adequate, the Special Master's decisionmaking was not bound by NIST's guidelines, including those mandated by Congress. E.g., FIPS Publication 199 ("Standards for Security Categorization of Federal Information and Information Systems") and FIPS Publication 200 ("Minimum Security Requirements for Federal Information and Information Systems").

Finally, the D.C. Circuit's July 2006 opinion recognized the problem inherent in making the Court, rather than the Secretary of the Interior, responsible for assessing harm that may result

---

[11] The Secretary of Interior discharges his responsibility for making such FISMA-directed determinations utilizing tools such as the Inspector General's conduct of threat assessments as well as external penetration testing, as discussed in note 5, above. For example, the Inspector General recently conducted a threat assessment of an Interior information technology system and issued a Report of Finding and Recommendations on March 13, 2007 (notice of this report is provided in a separate filing). This work was in accord with FISMA (and NIST standards) which make the Secretary of Interior responsible for assessing the results of the vulnerability and threat assessments by the Inspector General and making determinations regarding responses and curative actions. Consistent with the D.C. Circuit's opinion in July 2006, FISMA does not contemplate a judicial role in this process. Cobell v. Kempthorne, 455 F.3d at 314.

from IITD being compromised and making determinations regarding IT security:

> The district court stated that the interests of "Interior's other customers . . . are best protected if Interior's IT systems are adequately secure." [394 F. Supp. 2d] at 275. . . . Interior's duties extend far beyond the administration of these trust accounts. Would the public interest be served more fully by allowing Interior to continue its normal operations while improving IT security, or, as the district court implies, by ordering disconnection and forcing Interior to find alternate methods for completing some tasks without network access? The district court assumed that disconnection would create a net benefit, but it failed to explain its logic in arriving at this conclusion – and in light of the far-reaching effects this order would have on Interior's operations, we are skeptical that the district court could provide such an explanation.

455 F.3d at 316-17.

Thus, the appellate court rejected this Court's assessments of potential risk and magnitude of harm to IITD, as well as its determination that "commensurate" IT security protection required disconnection of Interior's systems, and such a result is wholly consistent with FISMA's direction that the agency head – in this case, the Secretary of the Interior – make such determinations. Moreover, the appellate court confirmed that FISMA provides no role for the judiciary. 455 F.3d at 314. Accordingly, because the Consent Order provides that this Court – not the Secretary of the Interior – is to make determinations as to what forms of IT security are necessary to be "adequate" to protect IITD, it is contrary to Congress's dictates under the subsequently enacted FISMA and the implementation of FISMA by Executive entities such as OMB and NIST, as confirmed by the 2006 opinion of the D.C. Circuit. Thus, the Consent Order must be vacated because a substantial change in the law renders it impermissible.

V. The Consent Order Should be Vacated Because the Facts Supporting Its Issuance Have Changed Substantially Since December 2001

More than five years have passed since the entry of the Consent Order and, at this stage, Plaintiffs cannot seriously dispute that the deficiencies which led to the entry of the Consent Order are no longer present in Interior's IT systems. See SEC v. Vision Communications, Inc., 1995 WL 109037 *2 (D.D.C. Mar. 6, 1995) ("An injunction may be dissolved where, for instance, changed circumstances eviscerate the justification therefor . . . .") (citing United States v. Swift & Co., 286 U.S. 106 (1932)). As noted above, within a year following entry of the Consent Order, approximately 95 percent of Interior's IT systems had been reconnected to the Internet. Cobell v. Kempthorne, 455 F.3d at 303.

In fact, the improvements to the security of Interior's IT systems have been extensive and substantial. In April 2005, Interior's Chief Information Officer informed this Court:

> 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 [of Interior]. The state of IT security as of December 2001 is not comparable to what exists today, which is dramatically improved.

Defendants' Opposition to Plaintiffs' Consolidated Motion for Temporary Restraining Order and Preliminary Injunction, Declaration of W. Hord Tipton ¶ 5 (Apr. 18, 2005) (Dkt. No. 2933); see also Trial Tr. 65 (June 7, 2005) (testimony of IG auditor confirming that Interior had spent at least $100 million to improve IT security); Trial Tr. 20 (July 18, 2005) (testimony of Associate Deputy Secretary Cason) ("As I understand from the budget office, we've spent well in excess of $100 million since the initial TRO on IT security related activities.").

Even in the course of issuing its preliminary injunction in 2005, this Court acknowledged

substantial changes to and improvements in IT security since it issued the Consent Order:

> It is also undeniable that Interior has made strides in the IT security arena. The Court is aware that, when IT security became an issue in this litigation some years ago, Interior was forced to begin from square one. Many of the individuals who testified in this evidentiary hearing are competent, conscientious, and well-intentioned. Interior's progress in a period of five years is laudable.

394 F. Supp. 2d at 272; see also id. at 247 ("The IG's FY 2003 FISMA report noted that Interior had made significant progress in creating an adequate IT security program, especially in light of 'almost 20 years of neglecting information system security requirements.'"), 248 ("In FY 2004, the IG again made note of Interior's progress, although not in as much detail."), 249 ("There can be no doubt that Interior has made substantial progress in implementing a comprehensive departmental IT security program in a very short time . . . ."), 259 ("To be sure, the 'old' [internal network backbone] has been upgraded, and additional firewall devices have been placed around all points of access to the 'backbone.'"), 270 ("The Court also notes the great progress that Interior's Inspector General has made in the IT security arena.").

Finally, in response to this Court's orders, Interior has provided highly detailed discussions of many of the improvements in its Quarterly Reports to the Court.[12] Even a cursory

---

[12] See 8th Status Report of Interior at 39-49, 50-51 (Jan. 16, 2002) (Dkt. No. 1090); 9th Status Report of Interior at 12-24, 25-26 ("Computer and Business Systems Architecture") (May 1, 2002) (Dkt. No. 1274); 10th Status Report of Interior at 8-22 (Aug. 1, 2002) (Dkt. No. 1405); 11th Status Report of Interior at 7-21 (Nov. 1, 2002) (Dkt. No. 1586); 12th Status Report of Interior at 9-18 (Feb. 3, 2003) (Dkt. No. 1764); 13th Status Report of Interior at 9-17 (May 1, 2003) (Dkt. No. 2049); 14th Status Report of Interior at 9-22 (Aug. 1, 2003) (Dkt. No. 2165); 15th Status Report of Interior at 6-17 (Nov. 3, 2003) (Dkt. No. 2356); 16th Status Report of Interior at 5-16 (Feb. 2, 2004) (Dkt. No. 2455); 17th Status Report of Interior at 5-9 (May 3, 2004) (Dkt. No. 2565); 18th Status Report of Interior at 4-8 (Aug. 2, 2004) (Dkt. No. 2622); 19th Status Report of Interior at 4-9 (Nov. 1, 2004) (Dkt. No. 2748); 20th Status Report of Interior at 4-9 (Feb. 1, 2005) (Dkt. No. 2827); 21st Status Report of Interior at 4-10 (May 2, 2005) (Dkt.

review of these status reports confirms the extensive nature of changes to Interior's IT security over the past five-plus years and the fact that the improvements have been made both to systems reconnected to the Internet under the Consent Order process and to systems that still remain disconnected.

Thus, even if Plaintiffs take issue with Interior's prior statements to the Court, Plaintiffs cannot dispute that the IT security in place today bears no resemblance to that of five-plus years ago. Indeed, that indisputable fact led to this Court's conducting the 59-day hearing "to evaluate Interior's current IT security." Cobell v. Norton, 455 F.3d at 308 (citing Cobell v. Norton, 394 F. Supp. 2d at 170) (emphasis added). Consequently, there can be no serious dispute that the facts originally justifying the entry of the Consent Order have changed materially.

VI. Plaintiffs Cannot Meet Their Burden of Establishing the Need for Any Continuing Injunction With Regard to Interior's IT Security

In light of the material changes in both law and facts since December 2001, this Court should vacate the Consent Order. In addition, the law plainly provides that Plaintiffs bear the burden of demonstrating that any other injunctive relief – including an order modifying the Consent Order – is necessary with regard to Interior's IT security. See, e.g., Knapp Shoes, Inc. v. Sylvania Shoe Manufacturing Corp. 15 F.3d 1222, 1225 (1st Cir. 1994), cited in Paradise Distributors, Inc. v. Evansville Brewing Co., 906 F. Supp. 619, 624 n.6 (N.D. Okla. 1995)); see

---

No. 2950); 22nd Status Report of Interior at 6-14 (Aug. 1, 2005) (Dkt. No. 3112); 23rd Status Report of Interior at 4-12 (Nov. 1, 2005) (Dkt. No. 3205); 24th Status Report of Interior at 3-11 (Feb. 1, 2006) (Dkt. No. 3228); 25th Status Report of Interior at 2-10 (May 1, 2006) (Dkt. No. 3243); 26th Status Report of Interior at 2-8 (July 31, 2006) (Dkt. No. 3256); 27th Status Report of Interior at 43-51 (Nov. 1, 2006) (Dkt. No. 3271); 28th Status Report of Interior at 43-49 (Feb. 1, 2007) (Dkt. No. 3290).

also Cobell v. Norton, 391 F.3d at 259 ("[I]t was error to shift the burden of persuasion to the Secretary to show why disconnecting most of Interior's IT systems was unnecessary to ensure the security of IITD, and the error was not harmless.") (citations omitted).

The D.C. Circuit's analysis of Plaintiffs' inability to sustain its burden for this Court's 2005 IT order applies equally to explain why Plaintiffs cannot meet their burden to demonstrate that any injunctive relief is appropriate at this time.[13] Initially, the Court of Appeals recognized Plaintiffs' inability to demonstrate "likelihood of success" when it stated:

> The class members have pointed to no evidence showing that anyone has already altered IITD by taking advantage of Interior's security flaws, nor that such actions are imminent. Even if someone did penetrate Interior's systems and alter IITD, we have been shown no reason to believe that the effects would likely be so extensive as to prevent the class members from receiving the accounting to which they are entitled.

455 F.3d at 315; see also id. at 317 ("While the class members may face some risk of harm if IITD housed on Interior's computers were compromised, we have not been shown that this possibility is likely, ..."). Further, the appellate decision squarely rejected Plaintiffs' assertion that a preliminary injunction was necessary to prevent irreparable harm. See id. at 315 ("We are unconvinced the class members demonstrated that they would necessarily suffer harm without

---

[13] The D.C. Circuit has described Plaintiffs' burden as follows:

> A court considering a plaintiff's request for a preliminary injunction must examine whether: (1) there is a substantial likelihood plaintiff will succeed on the merits; (2) plaintiff will be irreparably injured if an injunction is not granted; (3) an injunction will substantially injure the other party; and (4) the public interest will be furthered by an injunction.

Davenport v. International Brotherhood of Teamsters, AFL-CIO, 166 F.3d 356, 360 (D.C. Cir. 1999) (citing Serono Laboratories, Inc. v. Shalala, 158 F.3d 1313, 1317-18 (D.C. Cir. 1998)).

this injunction.").

The Court of Appeals' analysis of harm to Interior and the public was similarly dispositive:

> To determine whether injunctive relief is appropriate, we must balance the equities and hardships on both sides and must pay particular regard to whether such relief would further the public interest.

455 F.3d at 315 (citing Weinberger v. Romero-Barcelo, 456 U.S. 305, 312 (1982), and Woerner v. SBA, 934 F.2d 1277, 1279 (D.C. Cir. 1991)). With this in mind, the Court of Appeals proceeded to reject, in no uncertain terms, the propriety of injunctive relief as to the IT systems:

> The district court seemingly disregarded the harm an injunction would cause to Interior and those depending on Interior's services. By focusing on the need for Interior to improve its IT security, and arguing that disconnection would "help to illuminate the pervasive problems that continue to plague Interior's IT security environment," the district court glossed over the immensity of the disruption that would occur to Interior's operations.

455 F.3d at 316 (quoting 394 F. Supp. 2d at 275); see also 455 F.3d at 316 ("[W]e do not doubt that compliance with the injunction would cause significant hardship to Interior."). Further, the Court of Appeals rejected the conclusion that the public interest would be served by an injunction mandating disconnection of Interior's IT systems. 455 F.3d at 316.[14]

Thus, the D.C. Circuit's opinion does more than simply provide further support for

---

[14] Indeed, there should be no dispute that, at a time of ever-expanding use of the Internet to conduct government business, the dimensions of the "disruption" caused by disconnection continue to become considerably greater. See, e.g., H.R. Rep. No. 107-787 (Part 1), at 46 (2002), reprinted in 2002 U.S.C.C.A.N. 1880, 1881 ("The Federal Government, as well as State and local governments, are increasingly turning to the Internet and other information technologies to conduct the business of government.") ("Background and Need for [FISMA] Legislation").

vacating the Consent Order. Its analysis confirms that if Plaintiffs ask this Court to impose some other form of injunctive relief with respect to Interior's IT systems, e.g., modification of the Consent Order, they will not be able to sustain their burden.

CONCLUSION

The Consent Order – which Plaintiffs have repeatedly rejected – is predicated upon a legal landscape that no longer exists following the enactment of FISMA and the issuance of appellate decisions in this case. Further, the Consent Order is predicated upon facts long ago overcome by years of change and substantial and costly improvements to Interior's IT security. Accordingly, this Court should enter an Order vacating the Consent Order in the interest of justice upon the grounds that substantial changes in the law and the undisputed facts since entry of the Consent Order render it no longer appropriate or justified, as a matter of law.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

MICHAEL F. HERTZ
Deputy Assistant Attorney General

J. CHRISTOPHER KOHN
Director

/s/ Robert E. Kirschman, Jr.
ROBERT E. KIRSCHMAN, JR. (D.C. Bar No. 406635)
Deputy Director
JOHN T. STEMPLEWICZ
Senior Trial Counsel
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 616-0238
Facsimile: (202) 514-9163

March 19, 2007

CERTIFICATE OF SERVICE

I hereby certify that, on March 19, 2007 the foregoing *Defendants' Motion to Vacate Consent Order Regarding Information Technology Security* 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, et al.,	)	
Plaintiffs,	)	
v.	)	Case No. 1:96cv01285 (JR)
DIRK KEMPTHORNE, Secretary of the Interior, et al.,	)	
Defendants.	)	

ORDER

This matter comes before the Court on *Defendants' Motion to Vacate Consent Order Regarding Information Technology Security* (Dkt. No.). Upon consideration of the Defendants' Motion, any Opposition by Plaintiffs, Reply thereto, and the entire record of this case, it is hereby

FOUND: that the December 17, 2001 *Consent Order Regarding Information Technology Security* (Dkt. No. 1063) is no longer appropriate or justified, as a matter of law and it is hereby;

ORDERED: VACATED as of this date.

SO ORDERED.

Hon. James Robertson
UNITED STATES DISTRICT JUDGE
United States District Court for the
District of Columbia

Date:_____