

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 Robertson)
DIRK KEMPTHORNE, Secretary of the Interior, <u>et al.</u> ,)	
)	
Defendants.)	
_____)	

DEFENDANTS' REPLY BRIEF IN SUPPORT OF 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 submit the following reply brief in support of Defendants’ Motion to Vacate Consent Order Regarding Information Technology Security (Mar. 19, 2007) (Dkt. No. 3299)(“Motion to Vacate the Consent Order” or “Defendants’ Motion”).

I. Overview

On May 7, 2007, Plaintiffs filed their Opposition to Defendants’ Motion to Vacate Consent Order Regarding Information Technology Security (Dkt. No. 3319) (“Plaintiffs’ Opposition”). Their opposing brief contains numerous mischaracterizations of the Motion to Vacate the Consent Order, the current state of the law, and prior statements by Defendants. The following briefly addresses these flaws.

II. Plaintiffs’ Opposition Mischaracterizes the Relief Sought in
Defendants’ Motion and Disregards The Direction Set Forth in
This Court’s April 27, 2007 Memorandum Order

Contrary to Plaintiffs’ assertions, Defendants are not seeking to have the Court issue a

determination regarding the adequacy of Interior's IT security at any of the disconnected bureaus. See, e.g., Plaintiffs' Opposition at 9 (arguing that Court must allow plaintiffs "full discovery" and "hold[] an evidentiary hearing" before vacating the Consent Order); id. at 9-10 (incorrectly asserting that Defendants' Motion contends "IITD is secure" at disconnected bureaus); id. at 12-14 (setting forth allegations about the state of IT security). Rather, Defendants' Motion raises issues regarding the continuing propriety of general judicial oversight of IT systems, as set forth in the Consent Order, and such an argument is not dependent upon a factual finding as to the state of IT security. Thus, Defendants' Motion does not seek authority to reconnect disconnected IT systems; it seeks relief from the legal prohibition against Interior's agency head making the risk-based judgments mandated by FISMA.

The Court's April 27, 2007 Memorandum Order recognizes that the appropriate issue is whether the Court may still serve in the role established by the Consent Order in light of subsequent legal developments:

The argument I expect to hear on May 9 on the government's motion [3299] to vacate the IT consent order [1063] will deal with the consent order's continuing viability after the resignation of the Special Master and after successive rulings of the Court of Appeals limiting this Court's oversight of the government's IT systems -- with, in other words, whether and to what extent "ascertain[ing] the security posture of Information Technology ("IT") systems for Interior's offline bureaus and offices; the investigation and testing of those IT systems; security vulnerabilities; steps taken to mitigate and correct such vulnerabilities; specific incidents of improper access to, and theft and abuse of, Individual Indian Trust Data ("IITD"); and steps taken by offline bureaus and offices to reconnect to the Internet" [3314] at 1-2, remain the proper province of this Court after Cobell XII, Cobell XIII and Cobell XVIII.

Memorandum Order at 2-3.

Given the changes in the law resulting from the enactment of FISMA, mandatory standards promulgated by NIST, and the appellate decisions referenced in the Court's Memorandum Order, it is neither relevant nor appropriate to ask this Court to assess IT security at Interior. Indeed, that is the thrust of Defendants' Motion. Accordingly, while Interior does not agree with many of the factual assertions set forth in Plaintiffs' Opposition, the simple truth is that those assertions are not relevant for purposes of the May 14, 2007 hearing, as confirmed by the Court's Memorandum Order.

III. Plaintiffs' Opposition Is Fraught With Other Erroneous Statements

Plaintiffs' Opposition erroneously describes FISMA and Defendants' position regarding this statute. For example, Plaintiffs assert, "Contrary to the defendants' contention, FISMA did not impose on agency heads for the first time responsibility for IT security." Plaintiffs' Opposition at 4; see also id. at 16-17 ("However, once again, the Secretary's responsibility for IT security at Interior was not created by FISMA but existed at the time of the Consent Order."). Defendants' Motion does not assert that FISMA "created" agency head responsibility for IT security and, not surprisingly, Plaintiffs provide no citation to any statement that purportedly makes that assertion.

Similarly, and on a related point, Plaintiffs assert that "defendants' position is without foundation for FISMA merely consolidated and reaffirmed obligations regarding IT security existing at the time of the Consent Order." Plaintiffs' Opposition at 15. Again, Plaintiffs cite no authority for this assertion. As Defendants' Motion explained, when Congress passed FISMA, it

clearly did view the legislation as changing the law. Defendants' Motion at 4-5. For example, we quoted from the House Report accompanying the legislation, which stated that FISMA

- 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] two-year sunset;
- Strengthen[ed] Federal information security by requiring compliance with minimum mandatory management 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;
- Clarify[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.

Simply put, Plaintiffs' assertion that FISMA wrought no changes in the law lacks any foundation.

Plaintiffs' discussion of Interior's 28th Quarterly Report is also erroneous. Plaintiffs' Opposition at 11-12. Among Plaintiffs' claims is the following: "BIA still, even at this late date, has no certification and accreditation or proper authority to operate its IT systems." Id. (citing

28th Quarterly Report at 45). In fact, the 28th Quarterly Report only refers to a single BIA system that was in the process of undergoing the Certification and Accreditation (“C&A”) process:

BIA completed the Trust Active Directory root services C&A package in August 2006. This system provides authentication services for TrustNet, which is the network supporting the disconnected bureaus. A meeting held in December 2006 resolved a majority of the issues without the need to develop an MOU. The remaining issues involve deployment of the system across the trust bureaus. Full accreditation is expected upon resolution of these issues.

Interior Defendants’ 28th Quarterly Report to the Court at 45 (Feb. 1, 2007) (Dkt. No. 3290). It did not refer to BIA, as a whole.

Moreover, the BIA system referenced in the 28th Quarterly Report did, in fact, receive Authorization to Operate (thereby confirming completion of the C&A process) shortly after February 1, 2007, and this was reported on in the 29th Quarterly Report: “The Trust Active Directory, described in the previous report to the court, received full [Authorization to Operate] status on February 15, 2007.” Interior Defendants’ 29th Quarterly Report to the Court at 42 (May 1, 2007) (Dkt. No. 3318).

Plaintiffs’ erroneous assertion, that BIA has no C&A or authority to operate any of its IT systems, is not supported any statement in the 28th Quarterly Report. Moreover, inasmuch as the IT security status of BIA was the subject of significant evidence adduced during the 59-day IT security hearing in 2005, including the submission into evidence of copies of the C&A documents for almost all of BIA’s applications and systems, Plaintiffs’ misstatement about BIA, as a whole, cannot be reconciled with record evidence. Finally, Plaintiffs’ failure to note that the

C&A process for the one BIA system referenced in the 28th Quarterly Report had, in fact, received Authorization to Operate (thereby confirming the completion of the C&A process), as documented in the 29th Quarterly Report (filed almost one week before the Plaintiffs' Opposition was filed), defies explanation.

As a final example, Plaintiffs repeat, at length, their "first-in-time" arguments, in which they claim that Cobell VI and Cobell XII are controlling and binding upon later, allegedly inconsistent opinions of the D.C. Circuit. Plaintiffs' Opposition at 27-30. The D.C. Circuit squarely addressed and rejected Plaintiffs' assertion in its 2006 opinion. Cobell v. Kempthorne, 455 F.3d 301, 303-07 (D.C. Cir. 2006), cert. denied, 127 S. Ct. 1875 (2007). Accordingly, this Court should disregard the final three pages of Plaintiffs' Opposition, inasmuch as it represents an attempt to relitigate an issue already decided by the D.C. Circuit.

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
JOHN WARSHAWSKY (D.C. Bar No. 417170)
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

May 11, 2007

CERTIFICATE OF SERVICE

I hereby certify that, on May 11, 2007 the foregoing *Defendants' Reply Brief in Support of 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