UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, *et al.*,	:	
	:	
Plaintiffs,	:	
	:	
v.	:	Civil Action No. 96-1285 (JR)
	:	
DIRK KEMPTHORNE, Secretary of the Interior, *et al.*,	:	
	:	
Defendants.	:	

ORDER

Pending before the Court are Defendants' Motion for Order that the Office of the Solicitor Information Technology System May be Reconnected to the Internet [3450]; and Defendants' Motion for an Order (1) Authorizing the Reconnection to the Internet of Information Technology Systems of the Bureau of Indian Affairs, the Office of Hearing and Appeals, and the Office of the Special Trustee, (2) Confirming that the Office of Historical Trust Accounting May Connect its Information Technology System to the Internet, and (3) Vacating the December 17, 2001 Consent Order Regarding Information Technology Security [3507]. For the reasons discussed below, both motions are **granted.**

Discussion

Weaknesses within Interior's information technology systems housing Individual Indian Trust Data (IITD) have received a great deal of attention in this case. After orders, reports, hearings, injunctions, disconnections, reconnections, and

appellate opinions too numerous and complex to be recited here, five bureaus and offices within Interior remain disconnected from the internet. Conditions for the reconnection of those bureaus and offices, and a process for evaluating Interior's compliance with those conditions, are set forth in the Consent Order entered more than six years ago, on December 17, 2001 [1063]. It provides that

> Interior may reconnect to the Internet any information technology system that houses or provides access to individual Indian trust data. At least seventy-two (72) hours before reconnecting, Interior shall give actual notice to the Special Master and Plaintiffs' counsel with appropriate documentation of its intent to reconnect. At that time, Interior shall provide its plan to reconnect to the Special Master. The Special Master shall review the plan and perform any inquiries he deems necessary to determine if it provides adequate security for individual Indian trust data. If the Special Master objects to the plan because it does not provide adequate security for individual Indian trust data, he shall inform Interior of his objections and Interior shall work with the Special Master to attempt to resolve those objections. Interior shall not reconnect until such objections have been resolved to the satisfaction of the Special Master. If the Interior Defendants and the Special Master cannot resolve the Special Master's objections, notwithstanding their best efforts, the Interior Defendants may seek relief from the Court [. . .] [T]his Consent Order may be vacated by this Court once the Court has determined the Interior Defendants are in full compliance with this Consent Order and Interior's relevant information technology systems are in compliance with the applicable standards outlined in OMB Circular A-130.

Consent Order [1063] at 7-8. Three subsequent IT security orders superseded the Consent Order, but each of them was vacated on appeal, Cobell XII, 391 F.3d 251 (D.C. Cir. 2004); Cobell XVIII,

455 F.3d 301 (D.C. Cir. 2006), leaving the 2001 Consent Order in place by default.

The Consent Order was drafted by the government and entered over plaintiffs' objections, but today the government wants it vacated, and it is plaintiffs who insist that the Order should remain in place. Plaintiffs' argument is that the government has not met its burden of demonstrating that the five bureaus and offices are ready for reconnection. They identify several recent reviews critical of the current state of IT security within Interior,[1] and they claim that declarations of Interior officials attesting to the adequacy of IT security are in direct, irreconcilable conflict with such reports. See Plaintiffs' Opposition [3517] at 7-8. Plaintiffs read Cobell XII as requiring this court to hold an evidentiary hearing before ruling on IT security matters where genuine issues of materials fact are in dispute. Id. at 19, citing 391 F.3d at 261-62.

Defendants maintain that the Consent Order has been overtaken by events: that changes in law and fact since its entry render it obsolete. See Rufo v. Inmates of Suffolk County, 502 U.S. 367, 388 (1992) ("A consent decree must of course be modified if, as it later turns out, one or more of the obligations placed upon the parties has become impermissible

[1] See, e.g., Seventh Report Card on Computer Security at Federal Departments and Agencies (2007), available at http://republicans.oversight.house.gov/Media/PDFs/FY06FISMA.pdf.

under federal law."). They submit that provisions of the Consent Order requiring the Special Master and this Court to assess the adequacy of IT security are in conflict with the Federal Information Security Management Act of 2002 ("FISMA"), which was enacted after the entry of the Consent Order. Pub. L. No. 107-347, Title III, §§ 301-305. Under FISMA, it is the agency head who is "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 information[.]" 44 U.S.C. § 3544(a)(1)(A). Indeed, in vacating the last two IT security injunctions in this case, the Court of Appeals observed, "FISMA . . . includes a role for OMB, the Department of Commerce, the NIST, the Comptroller General, Congress, the public, and multiple officials within each agency subject to the statute. Notably absent from FISMA is a role for the judicial branch." Cobell XVIII, 455 F.3d at 314.

Plaintiffs correctly note that Defendants have not attempted to comply with the terms of the 2001 Consent Order in their reconnection motions, but it is unclear how they could have done so, considering that the Special Master has resigned, and that the majority of the Order's provisions pertain to his role in the reconnection process. Plaintiffs urge the Court to perform the judicial functions delegated to the Special Master,

suggesting that, despite the Court of Appeals' recent declaration that this is "not a FISMA compliance case," Cobell XVIII, 455 F.3d at 214, "the relief provided in a consent decree need not conform to the limits on court-ordered relief," Cf. Local Number 93, Intern. Ass'n of Firefighters v. City of Cleveland, 478 U.S. 501, 530 (1986) (O'Connor, J., concurring); cited in Plaintiffs' Opposition to Defendants' Office of the Solicitor Reconnection Motion [3472] at 5.

Under the Consent Order, it is the obligation of the Special Master (and, ultimately, the Court) to determine whether the IT security of systems housing IITD is adequate. Consent Order [1063] at 7. Once each disconnected bureau and office has demonstrated adequate IT security, the Consent Order may be vacated, so long as the Court finds that the agency's overall IT security is in compliance with OMB Circular A-130. Id. But it would be inappropriate, after FISMA and Cobell XVIII, for this Court to adjudicate agency compliance with OMB Circular A-130. Congress has assigned the role of weighing acceptable risks to heads of agencies. The Consent Order established a parallel track for evaluating IT security which may have been logical at an earlier stage of the case. At one point, my statements in court may have suggested an intent to proceed along that track and hold an evidentiary hearing before allowing Interior offices and bureaus to reconnect. On May 14, 2007, I noted that we were

not "working on a clean slate," and denied the motion to vacate the Consent Order because the government had not "made the requisite showing that [it had] any security." May 14, 2007 Hrg. Tr. At 40-41. But it is now clear that the Consent Order's parallel judicial track cannot be reconciled with applicable law. See, e.g., Cobell XVIII, 455 F.3d at 315-16, disapproving of "perpetual judicial oversight of Interior's computer systems," based only on a "list of vulnerabilities[.]"

I have before me the declarations of Authorizing Officials within each agency seeking connection or reconnection, see, [3450] Exhibits 1-4; [3507] Exhibits 1-10, all of which describe the bureau or office's successful completion of the agency's Connection Approval Process. The declarations indicate that the officials have performed their FISMA-assigned roles. The Congressional and Inspector General reports indicating that the Interior department, overall, continues to receive failing grades on its IT report card are troubling, but I have no authority to act in response to them, nor do I have any colorable suggestion that the declarations before me -- pertaining not to IT security overall, but instead to specific bureaus housing IITD -- were made in bad faith. Since my resolution of these motions turns not on a weighing of the evidence, but on a legal conclusion that it is not my role to weigh IT security risks, the Court of Appeals instruction that district judges "may not

resolve the state of Interior's IT systems security without conducting a hearing on the evidence in dispute" is inapplicable. Cobell XII, 391 F.3d at 261.

For these reasons, I find that the Consent Order is of no further use and must be vacated. The five disconnected offices and bureaus may be connected.

It is **SO ORDERED.**

JAMES ROBERTSON
United States District Judge