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.	)	
	)	

INTERIOR DEFENDANTS' REPLY BRIEF IN SUPPORT OF 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

I. Overview of Relevant Proceedings

The government first moved to vacate the Consent Order that prevents Interior from reconnecting certain Information Technology ("IT") systems to the Internet when it filed Defendants' Motion to Vacate Consent Order Regarding Information Technology Security (Dkt. No. 3299) (Mar. 19, 2007) ("Motion to Vacate Consent Order"). In the Motion to Vacate Consent Order, we described the substantial changes in the federal law governing oversight of IT security since issuance of the Consent Order, see Motion to Vacate Consent Order at 14-19 (discussing, among other things, FISMA, the enhanced role of NIST, and Cobell v. Kempthorne, 455 F.3d 301 (D.C. Cir. 2006) ("Cobell XVIII"), cert. denied, 127 S.Ct. 1875 (2007)).

On May 14, 2007, this Court denied the motion to vacate the Consent Order without prejudice, Tr. 41:9-10 (May 14, 2007), but in doing so, the Court noted that the legal landscape

is different from the time when the Consent Order was entered. The Court further described the additional information to be provided by the government when it chose to renew its motion:

> [W]hen you're ready, come to me and say, "I want to connect the bureau." And I'm probably going to say yes, because I'm going to look at Cobell XVIII and say, "I don't really have the – the Court of Appeals doesn't want me to tinker around with this." But you haven't shown me – you haven't made the requisite showing that you have any security.

Tr. 40:12-18 (May 14, 2007). The Court continued:

> [W]hen you're ready to connect to the Internet, either all at once or bureau by bureau, come back and renew the motion, and I would say the chances are it's going to be granted. But I don't have the right showing before me to grant that motion at this time.

Tr. 41:10-14 (May 14, 2007).

Approximately five months later, Interior Defendants first filed Interior Defendants' Motion for Order That the Office of the Solicitor Information Technology System May Be Reconnected to the Internet (Dkt. No. 3450) (Nov. 9, 2007) ("Motion to Reconnect Solicitor's IT System"), and that motion has been fully briefed by the parties.[1] On February 11, 2008, Interior Defendants filed the motion that is the subject of this reply brief, Interior 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 (Feb. 11, 2008) (Dkt. No. 3507)

[1] See Plaintiffs' Opposition to the Motion to Reconnect Solicitor's IT System (Dec. 14, 2007) (Dkt. No. 3472) and Interior Defendants' Reply Brief in Support of Motion to Reconnect Solicitor's IT System (Dec. 21, 2007) (Dkt. No. 3476).

("Motion to Reconnect Remaining Systems and Vacate Consent Order"), and Plaintiffs filed their opposing brief (referred to below as "Plaintiffs' Opposition" or "Pl. Opp.") on March 26, 2008.[2] Our reply brief in support of our motion appears below.

II. Plaintiffs' Opposition Misstates the Principal Issue Before the Court and Disregards the Substantial Changes in the Law Governing Federal Information Technology Security Assessments Since Entry of the Consent Order

A. The Issue Before This Court is Whether Interior Defendants Have Made the "Requisite Showing" of Security With Regard to Systems Housing or Accessing Individual Indian Trust Data

In their Introduction to their opposing brief, Plaintiffs assert:

> [T]he question presented is: What evidence has been presented that refutes this Court's finding, left undisturbed by [Cobell XVIII], that individual Indian Trust data is in imminent risk of loss?

Pl. Opp. at 1. As we explain below, the correct issue is whether, under current federal law, the responsible officials at Interior have made the required assessments of the department's IT security and have deemed it adequate.

In presenting their issue for this Court, Plaintiffs make two significant errors. First, Plaintiffs are wrong in claiming that Cobell XVIII "left undisturbed" this Court's conclusion that individual Indian Trust data ("IITD") was "in imminent risk of loss." To the contrary, the D.C. Circuit expressly overturned that finding: "The class members have pointed to no evidence showing that anyone has already altered IITD by taking advantage of Interior's security flaws,

---

[2] Plaintiffs' Opposition to Interior 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 (Mar. 26, 2008) (Dkt. No. 3517).

nor that such actions are imminent." Cobell XVIII, 455 F.3d at 315 (emphasis added). Thus, Plaintiffs misstate the issue before the Court, and their attempt to analyze Interior Defendants' motion in light of that misstated issue is irrelevant.

Second, Plaintiffs are wrong in analyzing Interior Defendants' motion in terms of the Consent Order, without regard to the substantial developments in federal IT security law since issuance of the Consent Order. As we described in last year's motion, federal law governing oversight of IT security has changed substantially since issuance of the Consent Order. See Motion to Vacate Consent Order at 14-19 (discussing, among other things, FISMA, the enhanced role of NIST, and Cobell XVIII). It was in this context that this Court, recognizing the changed legal landscape, informed the government, "[Y]ou haven't made the requisite showing that you have any security," Tr. 40:17-18 (May 14, 2007) (emphasis added), and that

> [W]hen you're ready to connect to the Internet, either all at once or bureau by bureau, come back and renew the motion, and I would say the chances are it's going to be granted. But I don't have the right showing before me to grant that motion at this time.

Tr. 41:10-14 (May 14, 2007). The Court's comments did not reflect an intention to apply the terms of the outdated Consent Order

Thus, the correct issue is whether, in the wake of the changes in federal law, Interior Defendants have made what this Court referred to as "the requisite showing" of security. Contrary to Plaintiffs' assertion, that showing does not involve this Court making determinations about the adquacy of security for data on IT systems. See Cobell XVIII, 455 F.3d at 314 ("Notably absent from FISMA is a role for the judicial branch."). It requires a showing that the officials contemplated by federal law to make those determinations, most notably the agency head and the agency's Authorizing Official (or his or her "Designated Representative"), have

made the federally mandated IT security determination. See Motion to Reconnect Remaining Systems and Vacate Consent Order at 8 n.9 (definition of "Authorizing Official" and "Authorizing Official Designated Representative"); see also Cobell XVIII, 455 F.3d at 314 ("This is not a FISMA compliance case, whether or not such an animal exists elsewhere."). By our motion and its attached declarations, Interior Defendants have demonstrated that the federally mandated IT security determinations properly have been made with regard to the BIA, OHA, OST, and OHTA systems.

B. Plaintiffs' Opposition Relies Upon Reports Regarding General IT Security, Rather Than Reports Specific to Trust Systems or IITD

At the outset, Plaintiffs essentially repeat their arguments made in opposition to the Motion to Reconnect Solicitor's IT System, in which they discuss various reviews and evaluations of general IT security at Interior. Pl. Op. at 3-11 (discussing reports of Congress; the Government Accountability Office ("GAO"); Interior's external auditors, KPMG; and Interior's Inspector General ("IG")); see Plaintiffs' Opposition to Motion to Reconnect Solicitor's IT System at 6-10 (Dec. 14, 2007) (Dkt. No. 3472). As before with regard to the Solicitor's IT system, the reports discussed within Plaintiffs' Opposition are broadly directed at Interior and not specifically at IT systems related to IITD,[3] which are the subject of the Consent Order. Thus, Plaintiffs rely upon reports discussing various overall aspects of IT security at Interior, rather than addressing the specific question posed by current federal law, i.e., whether Interior

[3] In at least one case, a cited report's discussion was not even specific to Internet connectivity. See Pl. Opp. at 10 (referring to evaluations that "demonstrated the Department remains vulnerable to an inside attacker" and that "the evaluations revealed ineffective internal intrusion detection and prevention capabilities") (emphasis added). Moreover, this quoted section expressly addressed BLM, MMS, and NBC, i.e., currently "connected" bureaus not the subject of either IT motion before this Court.

Defendants have demonstrated that the federally mandated IT security determinations properly have been made.

Aside from the fact that Plaintiffs place great emphasis upon various reports from 2005-2007, there can be no serious contention that the existence of IT security weaknesses or vulnerabilities necessarily lead to the conclusion that a federal agency should disconnect its IT systems from the Internet. For example, Plaintiffs note that Interior was joined by the Defense Department, the State Department, and the Department of Agriculture as receiving failing grades from Congress in 2005 and 2006. Pl. Opp. at 4 and n.8. Surely, Plaintiffs have not suggested, nor could they, that the Department of Defense or the Department of State, which have national security responsibilities and which received the same grade as Interior, should be disconnected from the Internet because of the grades they received from Congress.

Similar flaws may be found in Plaintiffs' analysis of the KPMG report cited in their brief. A review of the KPMG audit report confirms that it was issued in connection with a review of "Interior's internal controls over financial reporting" and the portions of the report upon which Plaintiffs rely are set forth in a section captioned "General and Application Controls over Financial Management Systems." Exhibit 1 to this Reply Brief, at 3-5. By its terms, the report is not related to TrustNet and ESN, as Plaintiffs wrongly imply. See Pl. Opp. at 7.[4]

---

[4] Moreover, Plaintiffs wrongly assert that Mr. Cason's supporting declaration and his concurrence with the findings of external auditors are "irreconcilably contradictory statements." Pl. Opp. at 7. This assertion reflects the flaw in Plaintiffs' argument, in which they cite statements about non-Trust issues and imply that they are findings with regard to the Trust systems at issue here. Id.

Plaintiffs also state, wrongly, that the CIO referenced in the IG's Performance and Accountability Report for Fiscal Year 2006 "is the same Chief Information Officer who . . . filed a statement [in support of the Motion to Reconnect Remaining Systems and Vacate Consent

Plaintiffs' analysis of these reports concludes with the following wholly insupportable statement:

> Simply put, Congress, the Government Accountability Office, KPMG, the IG – and, even the Interior defendant trustee-delegates in response to the foregoing reports and investigations – all agree that IT security at Interior exposes trust data, housed in systems connected to the Internet, to an imminent risk of undetectable loss, destruction, alteration, and misappropriation.

Pl. Opp. at 11 (emphasis in original). As a review of the reports cited by Plaintiffs and the foregoing demonstrates, Plaintiffs' characterization of the statements in these reports is completely without foundation.

III. The Motion to Reconnect Remaining Systems and Vacate Consent Order Demonstrates That Security Exists to Protect Data and That Interior Has Complied With the Requirements of FISMA

Contrary to Plaintiffs' argument, the issue before this Court is not whether Interior's overall IT security posture has areas for improvement, as determined by this Court. The reconnection issue (or, in the case of OHTA, connection issue) is whether, in the context of considering whether to vacate the Consent Order, Interior Defendants have demonstrated compliance with the types of security and risk analysis reviews mandated by Congress through FISMA and the enhanced role of NIST. See Motion to Reconnect Remaining Systems and Vacate Consent Order at 5-14 and Exhibits.

Interior Defendants' Motion to Reconnect Remaining Systems and Vacate Consent Order

---

Order.]" Pl. Opp. at 9 and nn.13-14. Putting aside the apparent dubiousness of the charges made in Plaintiffs' brief, the simple fact is that the CIO who signed the declaration referenced by Plaintiffs is a different individual than the individual referenced in the 2006 IG report. Mr. Howell became the CIO in May 2007. Exhibit 2 to this Reply Brief (Secretary announcement available at http://www.doi.gov/news/07_News_Releases/070511a.html).

is accompanied by sworn declarations[5] of Interior officials confirming both the existence of IT security measures for the subject IT networks and Interior's compliance with FISMA and NIST requirements. The specific elements of this showing were summarized in the motion seeking reconnection of BIA, OHA, and OST, and allowing connection of OHTA. See Motion to Reconnect Remaining Systems and Vacate Consent Order at 5-8 and Exs. 1-4 (discussing BIA); 8-10 and Exs. 1-2, 5-6 (discussing OHA); 10-12 and Exs. 1-2, 7-8 (discussing OST); 12-14 and Exs. 1-2, 9-10 (discussing OHTA). Plaintiffs ignore the detailed discussion in the motion and the supporting declarations, choosing, instead, to rely upon dated information from the 2005 hearing,[6] which resulted in a preliminary injunction being vacated in Cobell XVIII; to wholly

---

[5] Plaintiffs repeat their long-discredited complaint about the sufficiency of the jurat on the declarations. Pl. Opp. at 13 and nn.18 & 20, 15-16. Interior Defendants believe the declarations attached to the original motion are sufficient to demonstrate that the subject IT systems have adequate security in place and that a decision to reconnect (or, in the case of OHTA, connect) has been made, consistent with FISMA and NIST requirements. There is a distinction between providing sworn declarations for the Court's consideration as evidence (for which a jurat is required by Local Civil Rule 5.1(h)) and providing documents that serve as substantive evidence that Interior has complied with the requirements of federal IT security law. Thus, for purposes of this motion, Interior Defendants could have made the requisite showing of adequate security by attaching internal memoranda, rather than documents denominated as "declarations." Nevertheless, in the hope of mooting Plaintiffs' contentions about "insufficient jurats," we attached declarations bearing a jurat that conforms to the court's analysis in Cobell v. Norton, 391 F.3d 251, 260 (D.C. Cir. 2004) ("A declaration or certification that includes the disclaimer 'to the best of [the declarant's] knowledge, information or belief' is sufficient under the local rule, the statute.") (citations omitted).

[6] As the declarations attached to our motion demonstrate, in the almost three years since the 2005 hearing, Interior has undertaken considerable work to design, implement, and test the systems that are the subject of this motion. Information derived from the 2005 hearing is simply not relevant to assessing the status of IT security today. See, e.g., Pl. Opp. at 11-12 (discussing BIA's systems as of 2005).

The dated nature of the information cited by Plaintiffs is not the only flaw with their discussion, however. In at least one instance, Plaintiffs' discussion is grossly misleading about this Court's findings from the 2005 hearing. Plaintiffs baldly state, "Twelve BIA systems have

disregard the evolution in federal IT security law, beginning with FISMA; and to challenge, yet again, the sufficiency of the so-called "unqualified jurats" supporting the declarations. Pl. Opp. at 11-14, 16; see note 5, supra.

It is particularly significant that Plaintiffs' discussion states nothing about the FISMA- and NIST- directed roles and responsibilities of the Department CIO; the CIOs for BIA, OHA, OST, and OHTA; and the Authorizing Officials' Designated Representatives, all of whom executed detailed declarations filed in support of the Motion to Reconnect Remaining Systems and Vacate Consent Order.[7] Given the absence of Plaintiffs' discussion about matters such as Interior's CAP policy; the findings and recommendations of the various independent contractors engaged in connection with the Certification (or "Recertification") and Accreditation process; or the conclusions of the Authorizing Officials' Designated Representatives, we simply refer the Court to the sections of our motion cited in the preceding paragraph for further details demonstrating compliance with FISMA.

Plaintiffs argue that Interior Defendants' showing is insufficient because Interior Defendants did not file reports prepared by independent contractors, such as Security Test and

---

'defective' certification and accreditation documentation." Pl. Opp. at 12 (citing Cobell v. Norton, 394 F. Supp. 2d 164, 253 (D.D.C. 2005) (emphasis added), vacated, Cobell XVIII). In suggesting that this is the current state of the BIA systems, Plaintiffs do not disclose that, in fact, this Court found, "At BIA for example, twelve systems had defective C & A documentation that required that the systems be returned to IATO status." 394 F. Supp. 2d at 253 (emphasis added). This Court further explained that BIA took that action after the Department's then-CIO, Mr. Hord Tipton, issued a memorandum recommending that BIA "remand the accreditation status of the . . . twelve systems to interim authority to operate (IATO) with a 45-day expiry." Id. (quoting Tipton memorandum dated January 26, 2005).

[7] As we explained, while not mandated by FISMA, solely because of this litigation, Interior added an additional requirement for review by the Associate Deputy Secretary, Mr. Cason. Motion to Reconnect Remaining Systems and Vacate Consent Order at 8.

Evaluation Reports ("ST&E Reports"), Risk Assessments, and reports setting forth "documented security control deficiencies for OHA and OST." Pl. Opp. at 14. They ground this argument upon the Court's reference to "IT reports" during the May 14, 2007 hearing. In making this argument, Plaintiffs partially quote two sentences and conclude that Interior Defendants "refuse to provide competent evidence." Id. The entire statement of the Court, however, hardly rings as a directive to file independent contractor reports, such as ST&E Reports, Risk Assessments, or any of the other highly technical and sensitive documents prepared in connection with the Certification and Accreditation process:

> But I don't see why Interior can't go ahead with its plans to connect these bureaus, and when you're ready, come to me and say, "I want to connect the bureau." And I'm probably going to say yes, because I'm going to look at Cobell XVIII and say, "I don't really have the -- the Court of Appeals doesn't want me to tinker around with this."
>
> But you haven't shown me -- you haven't made the requisite showing that you have any security. You haven't filed the IT reports, you haven't -- you say, "Oh, yeah, we have security," but you tell me that you're not even ready to connect the bureaus to the Internet. All this consent decree really does is to stop you at the last step of connecting to the IT. There's nothing in this consent decree, is there, that says that you can't prepare to connect.

Tr. 40:11-24 (May 14, 2007). Specifically, the statement of the Court in the paragraph preceding the Court's reference to "IT reports" reasonably leads to the conclusion that this Court did not intend to become engaged in such matters, consistent with Cobell XVIII.[8]

Rather than directing Interior Defendants to file particular reports, the Court directed

---

[8] Interior Defendants certainly did not understand the Court to be asking the government to provide information akin to the "over five million pages of documentation related to IT security in connection with the 2005 IT security evidentiary hearing." Pl. Opp. at 14. Aside from consuming 59 days for an evidentiary hearing, that proceeding ulitmately led to the preliminary injunction vacated by Cobell XVIII, which the Court specifically referenced in its comments on May 14, 2007.

Interior Defendants to make what the Court referred to as the "requisite showing" of IT security. While in May 2007, the Court concluded that Interior Defendants had not made a showing of "any security," the Court's statement did not direct the submission of detailed and sensitive IT security reports for the purpose of conducting a review of IT security,[9] and this is wholly consistent with the observation in Cobell XVIII that the federal judiciary should not become a participant in making assessments about the adequacy of an agency's IT security. See Cobell XVIII, 455 F.3d at 314 ("Notably absent from FISMA is a role for the judicial branch.").

IV. Plaintiffs' Analysis of the Consent Order Disregards and Mischaracterizes Both the Substantial Changes in Law Governing Federal IT Security Technology and Interior Defendants' Assessments Made Pursuant to Such Law

A. Plaintiffs' Lengthy Discussion of the Consent Order Ignores and Confuses the Import of FISMA and Cobell XVIII

Plaintiffs' discussion of the Consent Order and their assertion that Interior Defendants have failed to establish a basis for vacating the Consent Order simply disregard the substantial evolution of federal law governing IT security assessments since entry of the Consent Order or the facts established by Interior Defendants' motion and the supporting declarations. See Pl. Opp. at 17-31. In doing so, Plaintiffs initially follow the same tack as their opposition to the motion to reconnect the Solicitor's IT system. See Pl. Opp. at 18 ("Defendants identify no material change in law or fact that justifies ignoring the terms of the governing order . . . .");

[9] Plaintiffs' assertion that because Interior Defendants did not file the independent contractor reports, the Court should "enter an adverse inference that the security is not materially improved" and that "the reports would have been produced if they support[ed] defendants' motion" is groundless. See Pl. Opp. at 14. The conclusions of the reports are summarized in detailed declarations submitted with the Motion to Reconnect Remaining Systems and Vacate Consent Order, and Interior Defendants' decision not to submit highly technical and IT security-sensitive documents with the motion is both rational and understandable.

Plaintiffs Opposition to Motion to Reconnect Solicitor's IT System at 3 ("Defendants identify no material change in law or fact, let alone any change that purports to justify their disregard of the terms of the Consent Order.") (emphasis in original).

Unlike Plaintiffs' previous opposition to reconnection of the Solicitor's IT system, Plaintiffs compound their flawed analysis by asserting that "reconnection under these circumstances necessarily would result in a further breach of trust and irreparable harm to the plaintiff class," Pl. Opp. at 18, notwithstanding Cobell XVIII's clear statement that Plaintiffs "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." Cobell XVIII, 455 F.3d at 315. Plaintiffs repeat their unfounded and hyperbolic assertion later in their analysis, Pl. Opp. at 19 ("The extent to which trust data again would be placed at catastrophic risk in conjunction with reconnection to the Internet is material to a fair resolution of this litigation."), and further misrepresent Cobell XVIII's conclusion, id. ("[T]his Court has made unchallenged findings that the catastrophic risk has not abated.") (citing Cobell XVIII, 455 F.3d at 308)).[10]

Plaintiffs further advise the Court that "[d]iscovery and an evidentiary hearing" are required.[11] Pl. Opp. at 18. In doing so, Plaintiffs ignore Cobell XVIII's admonition that FISMA

---

[10] The discussion in Cobell XVIII cited by Plaintiffs referred only to unchallenged findings of fact regarding the development of IT security within Interior over "the last few years." It did not address "catastrophic risks" and, as previously explained, the appellate court actually found that Plaintiffs had failed to show "that anyone ha[d] already altered IITD by taking advantage of Interior's security flaws, nor that such actions [were] imminent." Cobell XVIII, 455 F.3d at 315.

[11] Plaintiffs also ask the Court to hold any ruling on the motions "in abeyance" until the Court concludes the proceedings scheduled to begin June 9, 2008. Pl. Opp. at 2 n.3, 22. Plaintiffs proffer no justification, other than the fact that none of the subject IT systems has been connected to the Internet since entry of the Consent Order and that "reconnection necessarily

"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" and that "[n]otably absent from FISMA is a role for the judicial branch." Cobell XVIII, 455 F.3d at 314.

Plaintiffs repeatedly seek to interject this Court's previous finding of "impossibility" in Cobell XX and their unfounded claim that there has been a finding that the government repudiated its accounting duties. Pl. Opp. at 19; see also id. at 20 (discussing receivership and restitution). It is sufficient to note that whatever results from the upcoming proceeding scheduled to begin on June 9, 2008, the product of that hearing will have no bearing on the obvious need for the Department of the Interior to have full Internet connectivity with its clients and the general public. See, e.g., Interior Defendants' Thirty-First Quarterly Status Report to the Court at 45-46 (Feb. 1, 2008) (Dkt. No. 3506) (discussing deleterious impacts of continued disconnnection from Internet) (excerpts attached as Exhibit 3 to this reply brief).

Plaintiffs conclude their argument with a lengthy, misguided invitation for the Court to conduct a hearing on Interior's compliance with federal IT security law, such as OMB Circular A-130 and NIST Guidance, including FIPS 199, FIPS 200, and Special Publication 800-53. Pl. Opp. at 23-29; see also id. at 29 (inviting Court to assess whether OHA's security evaluation complies with NIST Special Publication 900-18 (revision 1)). Simply put, the parties

---

would expose trust data to further systemic loss and destruction." Id. at 2 n.3. With regard to the former, Plaintiffs disregard the obvious continuing impacts upon Interior and the public served by Interior through disconnection, see, e.g., Interior Defendants' Thirty-First Quarterly Status Report to the Court at 45-46 (Feb. 1, 2008) (Dkt. No. 3506) (excerpts attached as Exhibit 3 to this Reply Brief), and with regard to the latter, Plaintiffs, again, simply ignore Cobell XVIII's confirmation that they "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." Cobell XVIII, 455 F.3d at 315.

participated in such an exercise in 2005 – one which consumed fifty-nine days for an evidentiary hearing – and that exercise resulted in a vacated preliminary injunction and an appellate decision cautioning both that the judiciary does not have a role under FISMA and that the Cobell matter "is not a FISMA compliance case, whether or not such an animal exists elsewhere." Cobell XVIII, 455 F.3d at 314.

B. Interior Defendants Have Provided the Court With Both an Explanation of the Substantial Legal Changes Since Entry of the Consent Order and the Requisite Showing That Interior's Currently Disconnected IT Systems Have Security and Have Undergone Reviews Consistent With FISMA and NIST Requirements

Although Plaintiffs repeatedly assert Interior Defendants have failed to demonstrate a substantial change in the law justifying vacation of the Consent Order, Interior Defendants have previously described these legal developments in briefing to the Court. See Motion to Vacate Consent Order at 14-19. At the May 2007 hearing, in which the Court denied without prejudice our motion to vacate the Consent Order, the Court's inquiries expressly recognized the import of legal developments, such as Cobell XVIII, and advised Interior Defendants to provide additional facts – the "requisite showing" – to show that Interior had IT security in place for the subject IT systems. Tr. 40:12-18 (May 14, 2007).

The facts required are demonstrated by the Motion to Reconnect Remaining Systems and Vacate Consent Order and its supporting declarations. Although Plaintiffs' opposing brief is lengthy, little of it challenges the essential statements contained within the supporting declarations: aside from asking the Court to consider whether OHA's security evaluation complies with NIST requirements, Pl. Opp. at 29, Plaintiffs' only challenge to the supporting declarations appears in a footnote and a related text sentence, in which Plaintiffs complain that

"[o]nly passing reference is made [in the declarations] to FIPS 199 and NIST 800-53." Pl. Opp. at 28; see id. n.41.

Thus, the facts establishing the presence of adequate IT security for BIA, OHA, OST, and OHTA have been presented. Whether Interior's IT systems have adequate security, in light of a host of relevant factors, is a determination to be made by the responsible agency officials. The responsible officials at Interior have made the required assessment of the department's IT security, have deemed it adequate, and, accordingly, this Court should allow the requested reconnection. Moreover, insofar as no other bureaus or offices remain disconnected as a result of the Consent Order, the Court should vacate the Consent Order.

CONCLUSION

For the reasons set forth in Interior Defendants' Motion to Reconnect Remaining Systems and Vacate Consent Order and the foregoing reasons, Interior Defendants respectfully request this Court to issue an Order providing (1) that the IT system networks of BIA, OHA, and OST may be reconnected to the Internet, (2) that OHTA's OLE network may be connected to the Internet, and (3) that the December 17, 2001 Consent Order is vacated because it serves no further purpose in light of the changes in facts and law since its entry.

Dated: April 18, 2008

Respectfully submitted,

JEFFREY S. BUCHOLTZ
Acting 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 WARSHAWSKY (D.C. Bar No. 417170)
Senior Trial Counsel
GLENN D. GILLETT
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 616-0328
Facsimile: (202) 514-9163

ATTACHMENT

KPMG LLP
2001 M Street, NW
Washington, DC 20036

Independent Auditors' Report

Secretary and Inspector General,
U.S. Department of the Interior:

We have audited the accompanying balance sheets of the U.S. Department of the Interior (Interior) as of September 30, 2007 and 2006, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity (hereinafter referred to as "financial statements") for the years then ended. The objective of our audits was to express an opinion on the fair presentation of these financial statements. In connection with our fiscal year 2007 audit, we also considered Interior's internal controls over financial reporting and performance measures and tested Interior's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on these financial statements.

SUMMARY

As stated in our opinion on the financial statements, we concluded that Interior's financial statements as of and for the years ended September 30, 2007 and 2006, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

As discussed in our opinion, Interior revised its method of allocating certain costs and revenues between programs on the statement of net cost in fiscal year 2007. Also, as discussed in our opinion, in fiscal year 2007, Interior changed its method of accounting for and reporting of the reconciliation of net cost to budget, allocation transfers, and the Sport Fish Restoration and Boating Trust Fund (SFRBTF), to adopt changes in accounting standards and Office of Management and Budget (OMB) requirements.

Our consideration of internal control over financial reporting resulted in the following conditions being identified as significant deficiencies:

A. General and Application Controls over Financial Management Systems
B. Controls over Accruals
C. Controls over Undelivered Orders
D. Financial Reporting Controls
E. Controls over Charge Cards
F. Controls over Grants
G. Controls over the Indian Trust Funds

However, none of the significant deficiencies are believed to be material weaknesses.

We noted no deficiencies involving the design of the internal control over the existence and completeness assertions related to key performance measures.

The results of our tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements disclosed the following instance of noncompliance or other matters that are required to be reported under *Government Auditing Standards*, issued by the Comptroller General of the United States, and OMB Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*.

H. *Single Audit Act Amendments of 1996*

The following sections discuss our opinion on Interior's financial statements; our consideration of Interior's internal controls over financial reporting and performance measures; our tests of Interior's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements; and management's and our responsibilities.

OPINION ON THE FINANCIAL STATEMENTS

We have audited the accompanying balance sheets of the U.S. Department of the Interior as of September 30, 2007 and 2006, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity, for the years then ended.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the U.S. Department of the Interior as of September 30, 2007 and 2006, and its net costs, changes in net position, budgetary resources, and custodial activity for the years then ended, in conformity with U.S. generally accepted accounting principles.

As discussed in Note 20 to the financial statements, Interior's fiscal year 2007 statement of net cost is not comparable to its fiscal year 2006 statement of net cost because Interior revised its method of allocating certain costs and revenues between programs in fiscal year 2007. Also discussed in Note 22 to the financial statements, Interior changed its method of reporting the reconciliation of net cost to budget in fiscal year 2007. Further, as discussed in Note 27 to the financial statements, Interior changed its method of accounting for and reporting allocation transfers and the SFRBTF in fiscal year 2007.

The information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections is not a required part of the financial statements, but is supplementary information required by U.S. generally accepted accounting principles and OMB Circular No. A-136, *Financial Reporting Requirements*. We have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of this information. However, we did not audit this information and, accordingly, we express no opinion on it.

Our audits were conducted for the purpose of forming an opinion on the financial statements taken as a whole. The consolidating information in the Other Supplementary Information subsection within the Financial Report section is presented for purposes of additional analysis of the consolidated financial statements rather than to present the financial position and changes in net position of Interior's components individually. The consolidating information has been subjected to the auditing procedures applied in the audits of the financial statements and, in our opinion, is fairly stated, in all material respects, in relation to the financial statements taken as a whole. The Introduction, Performance Data and Analysis, the Other Accompanying Information sections, and the special account funds in the Other Supplementary Information subsection within the Financial Report section are presented for purposes of additional analysis and are not required

KPMG

as part of the financial statements. This information has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

INTERNAL CONTROL OVER FINANCIAL REPORTING

Our consideration of the internal control over financial reporting was for the limited purpose described in the Responsibilities section of this report and would not necessarily identify all deficiencies in the internal control over financial reporting that might be significant deficiencies or material weaknesses.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects Interior's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of Interior's financial statements that is more than inconsequential will not be prevented or detected by Interior's internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by Interior's internal control.

In our fiscal year 2007 audit, we consider the deficiencies described below to be significant deficiencies in internal control over financial reporting. However, we believe that none of the significant deficiencies described below are material weaknesses. Exhibit I presents the status of prior year reportable conditions.

A. General and Application Controls over Financial Management Systems

Interior continues to improve the security and controls over its information systems; however, we determined that Interior needed to improve controls in the areas described below, as required by OMB Circular No. A-130, *Management of Federal Information Resources.* These conditions could have affected Interior's ability to prevent and detect unauthorized changes to financial information, to control electronic access to sensitive information, and to protect its information.

1. *Entity-wide Security Program and Planning*
   An entity-wide security program, including security policies and a related implementation plan, is the foundation of an entity's security control structure. Interior did not fully document its certification and accreditation procedures for certain systems and applications, and did not perform certain procedures to support its certification and accreditations. Additionally, Interior had not certified and accredited one facility, used an earlier version than authorized for one of its applications, and had not assigned security responsibilities for one system. Finally, Interior did not establish agreements to document the minimum security requirements for the interconnections and interfaces between certain applications.

2. *Access Controls*
   Access controls protect computer resources from unauthorized modification, disclosure, and loss. Interior did not fully establish controls to prevent and detect unauthorized access. Interior did not formally document and approve policies and procedures regarding access control procedures, segregation of system roles and responsibilities, the monitoring and

revocation of inactive user accounts, monitoring security profile changes, and periodic recertification of user access for certain applications and systems.

In addition, Interior did not consistently complete the appropriate level of investigation for users, obtain and maintain rules of behavior forms, obtain and maintain user access approval forms, obtain and maintain awareness training evidence, review and document reviews of user access to ensure conflicting access rights are not granted, limit users to one account, limit access of administrator accounts, follow its password policies, perform and document periodic re-certifications to ensure that all users are authorized and the level of access rights was appropriate, or identify and review changes to user account and security profiles. Finally, Interior did not consistently monitor or remove inactive user accounts, remove access of separated users in a timely manner, complete the appropriate exit procedures, or maintain exit clearance documentation for certain systems.

3. *System Software Controls*
System software controls protect computer resources from unauthorized modification, disclosure, and loss. Interior had not implemented formal change management procedures for one system, and had not formally approved procedures regarding the system development life-cycle, segregation of duties, administrator access, and audit logging for certain systems. In addition, Interior did not consistently establish controls to limit access to systems, document the approval for system software changes, maintain system change documentation, identify and monitor for inappropriate changes to systems, review system change logs, or monitor activities performed by administrators.

4. *Software Development and Change Controls*
Software development and change controls ensure that only authorized programs and modifications are implemented. Interior needs to improve its change management policies to ensure that it includes detailed testing procedures for normal and emergency changes for certain applications and configuration management. Interior did not use library management software to control changes to one of its applications, fully segregate software development and change duties, and identify and review changes to ensure the changes were approved for certain applications.

5. *Service Continuity*
Service continuity plans protect information resources, minimize the risk of unplanned interruptions, and recover critical operations should interruptions occur. Interior did not have a finalized, approved, fully documented, and/or tested contingency plan to be used in the event of service disruption for certain systems and applications. Interior did not have a comprehensive plan to train certain essential employees on emergency responsibilities outlined within the critical system and application contingency plans. Interior also did not demonstrate that certain contingency plan test results and corrective actions were reviewed by the appropriate officials. Furthermore, Interior did not track and report service interruptions for one application or fully establish environmental controls for one of its server rooms. In addition, Interior personnel involved with media sanitization were not always aware of policies and procedures. Finally, Interior did not consistently sanitize tapes, maintain evidence that backup tapes were completed, use a tape library log, store backup tapes at off-site locations, or test backup tapes.

6. *Segregation of Responsibilities*
   Proper segregation of responsibilities helps prevent and detect unauthorized actions. Interior did not formally document application-specific roles or access privileges that should be segregated for certain financial systems or formally document compensating controls when access privileges cannot be segregated. In addition, Interior did not consistently require management to review the design and operation of segregation of responsibility controls. Finally, Interior did not fully segregate responsibilities for certain applications and systems.

Recommendations

We recommend that Interior continue to improve the security and general controls over its financial information systems to ensure adequate security and protection of the information systems as follows:

1. Certify and accredit its facilities and systems, perform all certification and accreditation procedures, fully document its certifications and accreditations, assign security responsibilities, and establish agreements for interconnections and interfaces between applications.
2. Establish controls to prevent and detect unauthorized access, develop and finalize access control policies, complete investigations, obtain and maintain user access documentation, review and approve user access, restrict access, follow password policies, periodically re-certify user access, monitor user account and security profile changes, monitor inactive accounts, remove access of separated users timely, complete the appropriate exit procedures, and maintain exit documentation.
3. Implement and approve change management procedures, establish controls to limit access to systems, document the approval for system software changes, maintain system change documentation, identify and monitor for inappropriate changes to systems, review system change logs, and monitor activities performed by administrators.
4. Improve its change management policies, use library management software to control software changes, fully segregate software development and change duties, and identify and review changes.
5. Finalize, approve, and test contingency plans and related training plans, review test results and corrective actions, track and report service interruptions, establish environmental controls, communicate and follow media sanitation policies, and control and test back up tapes.
6. Formally document application-specific roles or access privileges that should be segregated, periodically review segregation of duties, and fully segregate responsibilities.

Management Response

Management has prepared an official response presented as a separate attachment to this report. In summary, management agreed with our findings and its comments were responsive to our recommendations. We did not audit Interior's response and, accordingly, we express no opinion on it.

B. Controls over Accruals

In accordance with Federal accounting standards, Interior is required to record liabilities based on the probable future outflow or other sacrifice of resources as a result of past transactions or events. Interior did not properly develop its accounts payable accrual methodology at two Interior components to consider changes in operations, and did not properly test the assumptions used to calculate its accounts payable accrual at two Interior components. In addition, Interior did not ensure that its accounts payable accruals consistently agreed to the supporting documentation

or consistently documented its approval of the accounts payable accruals. Furthermore, Interior did not fully consider the results of its grants accrual analysis and adjust its grant accrual methodology appropriately for one of its grant programs.

As a result of our observations, Interior adjusted its accrual methodologies, tested its assumptions, and increased its accruals by $154 million. However, Interior did not effectively review the accrual adjustments because Interior did not properly de-obligate $58 million of undelivered orders when Interior recorded the accrual adjustments. As a result of our observations, Interior recorded the de-obligation.

Recommendations

We recommend that Interior implement the following recommendations to improve controls over its accruals:

1. Evaluate and revise accounts payable accrual methodologies for changes in operations.
2. Test the assumptions used in the accounts payable accrual, including the subsequent activity report, to ensure that the subsequent activity report is accurate and complete.
3. Analyze the grants accrual analysis to ensure that the results support the grant accrual methodology.
4. Require supervisors to compare the accounts payable accrual adjustments from the accounting system to the calculations and the supporting documentation to ensure that the amounts are properly recorded and to document approval evidencing completion of comparison.

Management Response

Management has prepared an official response presented as a separate attachment to this report. In summary, management agreed with our findings and its comments were responsive to our recommendations. We did not audit Interior's response and, accordingly, we express no opinion on it.

C. Controls over Undelivered Orders

Undelivered orders should be promptly recorded, properly classified, and accounted for, in order to prepare timely and reliable reports. Interior policies requires its components to review and certify undelivered orders quarterly, including undelivered orders with no activity during the past 12 months, and to de-obligate invalid obligations; however, four of the nine Interior components did not effectively follow these policies. Two of the Interior components did not review and certify undelivered orders because the components were unable to obtain certain undelivered order reports from the accounting system. Two other components certified the undelivered order balances; however, the components did not effectively certify the undelivered order balances because they incorrectly certified 16 of the 166 undelivered orders tested. In addition, Interior did not consistently maintain documentation or modify orders that had expired in a timely manner to support its undelivered orders. As a result of our observations, Interior analyzed and decreased its undelivered orders by $80 million. Subsequent to management's analysis and adjustment, we identified 6 additional exceptions in the 281 undelivered orders tested at one Interior component.

Recommendations

We recommend that Interior implement the following recommendations to improve controls over its undelivered order balances:

1. Provide training to program and finance personnel on certifying and closing out undelivered orders.
2. Configure its accounting system to provide undelivered order reports.

3. Review and certify all undelivered order balances, on at least a quarterly basis.
4. Monitor and close out as appropriate undelivered orders with minimal to no activity during the past three months, on at least a quarterly basis.
5. Modify expired orders in a timely manner.
6. Improve and maintain documentation to support its undelivered order balances.

Management Response
Management has prepared an official response presented as a separate attachment to this report. In summary, management agreed with our findings and its comments were responsive to our recommendations. We did not audit Interior's response and, accordingly, we express no opinion on it.

D. Financial Reporting Controls

Interior needs to improve financial reporting controls to ensure transactions are properly recorded for reliable financial reports. Interior did not properly classify certain financial transactions resulting in over $181 million of activity being reported in the other fund column, rather than the earmarked fund column on the statement of changes in net position and resulting in misclassifications of $188 million in the reconciliation of net cost to budget disclosure and other note misclassifications. In addition, Interior did not effectively segregate responsibilities because certain individuals have the authority to both enter and approve journal entries in the accounting system without a secondary review at four of the nine Interior components.

Recommendations
We recommend that Interior implement the following to improve the recording and reporting of financial transactions:

1. Require a second person to analyze the financial statements and disclosures to ensure financial transactions are properly classified and presented and document such review.
2. Configure the accounting system to prevent the same individual from entering and approving journal entries in the accounting system or require an individual who does not have access to enter or approve journal entries to compare the journal entries recorded in the financial systems to the approved journal entries to ensure that all journal entries have been approved and were properly entered into the financial system, and document evidence of completion of the comparison.

Management Response
Management has prepared an official response presented as a separate attachment to this report. In summary, management partially agreed with our findings and its comments were responsive to our recommendations. Management believes that there are adequate and mitigating controls. We did not audit Interior's response and, accordingly, we express no opinion on it.

Auditors' Response to Management's Response
As summarized above, Interior did not effectively segregate responsibilities because we identified certain individuals have the authority to both enter and approve journal entries in the accounting system without a secondary review. In addition, Interior implemented the mitigating controls after we identified the control deficiency and the mitigating controls did not operate effectively because the same people who performed the mitigating controls had the ability to enter and approve journal entries and therefore Interior did not segregate the responsibilities over journal entries. Therefore, we continue to believe that the control deficiencies identified constitute a significant deficiency.

KPMG

E. Controls over Charge Cards

Interior issues purchase, fleet, and travel charge cards to its employees to streamline acquisition and payment procedures and to reduce the administrative burden associated with traditional and emergency purchasing of travel items, supplies, and services. Interior uses charge cards to purchase goods and services totaling several hundred million dollars. In conjunction with the issuance of these cards, Interior published the *Integrated Charge Card Program Guide*. This guide sets forth restrictions on the use of the cards as well as certain internal control procedures such as timely and complete reconciliation of billing statements by the cardholders and approving officials.

However, we determined that Interior did not consistently follow these internal control procedures because we identified 69 exceptions in the 361 statements that we tested at 3 of the 7 Interior components that we tested. For example, cardholders and supervisors did not always sign and date the charge card statements, did not consistently sign and date the charge card statements in a timely manner, and did not consistently maintain charge card receipts to support the charges.

Recommendations

We recommend that Interior perform the following:

1. Continue to provide training to personnel on proper charge card procedures.
2. Require approving officials to be more diligent in monitoring and enforcing compliance with Interior's charge card policies.
3. Periodically test a sample of charge cards for compliance with Interior's charge card policies.

Management Response

Management has prepared an official response presented as a separate attachment to this report. In summary, management agreed with our findings and its comments were responsive to our recommendations. We did not audit Interior's response and, accordingly, we express no opinion on it.

F. Controls over Grants

Interior is required to monitor its grantees in accordance with the *Single Audit Act Amendments of 1996,* and the related OMB Circular No. A-133, *Audits of States, Local Governments, and Non-Profit Organizations* (OMB Circular No. A-133). Interior needs to improve controls over grant monitoring at four Interior components. Interior did not maintain documentation that Interior formally communicated the grant award name, grant number, catalog of federal domestic award number, and/or the list of applicable laws and regulations to the grantees for 32 of the 45 grant awards tested at one component. Interior also did not have a complete listing of grantees to ensure that it obtained Single Audit reports and issued management decisions on audit findings for one Interior component. In addition, two Interior components did not obtain Single Audit reports within nine months of the grantee's fiscal year-end for 13 of 44 grantees tested and did not issue management decisions on audit findings within six months after receipt of Single Audit reports or ensure that the grantees completed appropriate and timely corrective action on such findings for 8 of the 66 grantees tested. Further, two Interior components, did not obtain or follow up on past due Financial Status Reports for 15 of the 77 grantees tested. Additionally, one Interior component did not obtain Grant Performance Reports for 8 of 32 grantees tested or obtain Annual Reports for 3 of the 32 grantees tested. Finally, Interior did not review the reconciliation from the grant system to the accounting system at one Interior component.

KPMG

Recommendations

We recommend that Interior perform the following to improve its grant monitoring process:

1. Review the grant award to ensure that the grant awards include the award name and number, the catalog of federal domestic number and title, award year, if the award is for research and development, and list of laws and regulations and document approval on the grant award.
2. Maintain a complete and accurate listing of grantees to enable monitoring of receipt of Single Audit Reports and issuance of management decisions on findings.
3. Follow up on Single Audit, Financial Status, Grant Performance, and Annual Reports not received and consider the need to limit future grant awards until these reports are received.
4. Issue management decisions on audit findings within six months after receipt of Single Audit reports and verify that grantees take appropriate and timely corrective action.
5. Require a supervisor to review the reconciliation from the grant system to the accounting system and to document evidence of such review.

Management Response

Management has prepared an official response presented as a separate attachment to this report. In summary, management agreed with our findings and its comments were responsive to our recommendation. We did not audit Interior's response and, accordingly, we express no opinion on it.

G. Controls over the Indian Trust Funds

The United States Congress has designated the Secretary of the Interior as the trustee delegate with responsibility for the financial and non-financial resources held in trust on behalf of American Indian Tribes (Tribal Trust Funds), individual Indians, and other trust funds (hereafter collectively referred to as the Indian Trust Funds). The Secretary carries out this fiduciary responsibility through the Office of the Special Trustee for American Indians (OST), Indian Affairs (IA), other Interior bureaus, and agreements with American Indian Tribes.

The Indian Trust Funds' balances include two categories: (1) Trust Funds that are held by Interior because the corpus of specific accounts is non-expendable or the funds that are held for future transfer to Indian Tribes upon satisfaction of certain conditions and thus are reflected in Interior's financial statements; (2) Trust Funds for Indian Tribes and individual Indians that are considered non-Federal accounts and thus are not reflected in Interior's financial statements but are disclosed in a footnote to Interior's financial statements, in accordance with the accounting standards.

Interior has invested a significant amount of resources to improve controls over Indian Trust Funds; however, we noted that Interior needs to continue its efforts to resolve historical differences for items 1 through 4 below, and to improve procedures and internal controls for entering and maintaining Trust Fund information, including recording receivables, to ensure that the Indian Trust Funds' activity and balances are recorded properly and timely, as follows:

1. Trust Fund Balances

The financial information systems and internal control procedures used in the processing of Indian Trust Fund transactions have suffered historically from a variety of system and procedural internal control weaknesses. In addition, Interior is burdened with the ongoing impact of decades of accumulated discrepancies in the accounting records. Furthermore, certain Indian Trust Fund beneficiaries do not agree with the trust fund balances and/or have requested an accounting of the Indian Trust Funds. However, Interior has invested a significant amount of resources identifying historical records, isolating and working to

KPMG

resolve historical differences, and preparing an accounting of the Indian Trust Fund balances and will continue with this historical accounting effort.

2. *Individual Indian Monies Subsidiary Ledger*
The control account for Individual Indian Monies (IIM) account holders represents the aggregate net balance of trust funds held on behalf of IIM account holders, house accounts, and suspense accounts as reflected in the detailed subsidiary ledger of IIM accounts (subsidiary ledger). The control account balance has historically not agreed to the sum of the balances from the subsidiary ledger, and it cannot be determined which balance, if either, is correct. The amount invested for IIM is based on the IIM control account balance. Consequently, the balance of funds invested for IIM account holders may not be correct, which in turn would affect interest earnings. As of September 30, 2007, the aggregate sum of all balances included in the subsidiary ledger exceeded the control account by approximately $6 million.

   As of September 30, 2006, the subsidiary ledger contained negative account balances totaling approximately $44 million (of which approximately $164,000 was attributed to individual Indian accounts as of September 30, 2006). During fiscal year 2007, management adjusted the subsidiary ledger eliminating the negative account balances totaling approximately $44 million (of which approximately $113,000 was attributed to individual Indian accounts as of September 30, 2007); however, we were unable to conclude on the propriety of such adjustment.

3. *Special Deposit Accounts*
As of September 30, 2007 and 2006, there were approximately 13,000 and 22,000 special deposit accounts reflected in the subsidiary ledger with balances totaling approximately $33 million and $36 million, respectively. In accordance with Title 25 of the Code of Federal Regulations and as directed by IA, historically OST recorded receipts into special deposit accounts within the subsidiary ledger when the recipient trust fund account was unknown at the time of receipt. When IA identifies the trust fund account(s), OST transfers the amount from the special deposit account(s) to the designated trust fund account(s) in accordance with IA instructions. A significant number of special deposit accounts have remained inactive for the past several years and new special deposit accounts were established during fiscal year 2007 and 2006. As of September 30, 2007, a significant number of special deposit accounts represent historical balances and continue to require resolution.

4. *Undistributed Interest and Unusual Balances*
OST and/or IA had not been able to determine the proper recipients of undistributed interest related to Tribal Trust Funds of approximately $2.0 million as of September 30, 2006. However, in prior years OST commissioned a report to assist in determining the recipients of these funds, and based on that report distributed the balance of these funds during fiscal year 2007. Additionally, OST and/or IA have not been able to determine the proper recipients of undistributed interest related to IIM of approximately $3.8 million and $3.6 million as of September 30, 2007 and 2006, respectively. Furthermore, there were Tribal Trust Funds accounts with negative cash balances totaling approximately $721,000 as of September 30, 2007 and 2006, which continue to require resolution.

KPMG

5. *Entering and Maintaining Trust Fund Information*
The regional and agency offices of IA perform a critical role in the initial input and subsequent changes to the Indian Trust Funds' information disclosed by Interior. We noted weaknesses in the following areas:

a. *Trust Fund Records*
IA did not consistently maintain ownership records for rights of way lease agreements on lands held in trust for the Indian Trust Funds because IA was unable to provide evidence of ownership for 38 of the 45 lease agreements tested. Additionally, IA did not consistently obtain appraisals from the Bureau of Land Management prior to entering into the lease agreements related to lands held in trust for the Indian Trust Funds. Finally, IA did not consistently follow its policies contained in Part 53 of the Indian Affairs Manual because IA did not obtain and approve Forest Management Plans for 2 of 30 locations tested.

b. *Distribution of Funds to OST*
IA did not consistently sign the Trust Funds Receivable Worksheet prior to submitting funds to OST for 9 of the 115 items tested. In addition, IA did not consistently transfer funds to OST within 24 hours of the lease agreement approval for 15 of 115 items tested and within 24 hours of receipt for 3 of the 115 items tested in accordance with its policies. Finally, IA did not use the fastest means possible in forwarding funds to the lockbox in accordance with its policies for 5 of 115 items tested.

c. *Accounts Receivable*
IA had not fully developed and communicated standardized policies and procedures for establishing, tracking, and pursuing historical accounts receivable for the Indian Trust Funds. This resulted in inconsistent processes and increases the risk that amounts due to Indian Trust Funds are not identified and ultimately collected.

d. *Probate Backlog*
IA did not consistently enter probate orders for land title into the trust management systems timely. Although IA made progress in reducing the backlog, IA indicated that it had probate orders that had not been prepared, adjudicated, recorded, and/or encoded. IA expects to have the backlog resolved in September 2009. This increases the potential for untimely distributions of income to the account holders of the Indian Trust Funds.

e. *Supervised and Restricted Accounts*
IA did not consistently perform reviews over active supervised accounts. Finally, although each of the regions that we visited had compiled a listing of active supervised accounts, the regions expended significant efforts generating the listing. IA has identified reports from the Trust Fund Accounting System (TFAS) and Strata Vision, which list all active supervised accounts and needs to work with OST to ensure its timely distribution to the appropriate agency offices.

Recommendation
We recommend that Interior develop and implement procedures and internal controls to address the deficiencies in controls related to Indian Trust Funds.

KPMG

Management Response
Management has prepared an official response presented as a separate attachment to this report. In summary, management disagreed with the findings because management believes that its efforts to address internal control deficiencies in the Indian Trust Funds are substantially complete and that the auditors' report did not contain findings suggesting current operational control deficiencies. We did not audit Interior's response and, accordingly, we express no opinion on it.

Auditors' Response to Management's Response
As summarized above, we identified control deficiencies in the current year that adversely affect Interior's ability to initiate, authorize, record, process, and report Indian Trust Fund data reliably. Therefore, we continue to believe that the control deficiencies identified constitute a significant deficiency.

* * * * *

We noted certain additional matters that we have reported to management of Interior in a separate letter dated November 13, 2007.

INTERNAL CONTROL OVER PERFORMANCE MEASURES

Our tests of internal control over performance measures, as described in the Responsibilities section of this report, disclosed no deficiencies involving the design of the internal control over the existence and completeness assertions related to key performance measures.

COMPLIANCE AND OTHER MATTERS

Our tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements, as described in the Responsibilities section of this report, exclusive of those referred to in the *Federal Financial Management Improvement Act of 1996* (FFMIA), disclosed one instance of noncompliance or other matters that is required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 07-04, and is described below.

H. *Single Audit Act Amendments of 1996*

As discussed in the Internal Control over Financial Reporting section of this report, Interior did not perform adequate monitoring of grantees in accordance with the *Single Audit Act Amendments of 1996* and the related OMB Circular No. A-133. Interior needs to ensure that it communicates grant award information, obtains Single Audit, Financial Status, Grant Performance, and Annual Reports, and issues management decisions on audit findings in a timely manner.

Recommendation
We recommend that in fiscal year 2008, Interior obtain Single Audit, Financial Status, Grant Performance, and Annual Reports and issue management decisions on audit findings in accordance with the requirements of the *Single Audit Act Amendments of 1996* and the related OMB Circular No. A-133.

Management Response
Management has prepared an official response presented as a separate attachment to this report. In summary, management agreed with our findings and its comments were responsive to our

recommendation. We did not audit Interior's response and, accordingly, we express no opinion on it.

* * * * *

The results of our tests of compliance as described in the Responsibilities section of this report, exclusive of those referred to in FFMIA, disclosed no other instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 07-04.

The results of our tests of FFMIA disclosed no instances in which Interior's financial management systems did not substantially comply with the three requirements discussed in the Responsibilities section of this report.

RESPONSIBILITIES

Management's Responsibilities. The United States Code Title 31 Sections 3515 and 9106 require agencies to report annually to Congress on their financial status and any other information needed to fairly present their financial position and results of operations. To meet these reporting requirements, Interior prepares and submits financial statements in accordance with OMB Circular No. A-136.

Management is responsible for the financial statements, including:

- Preparing the financial statements in conformity with U.S. generally accepted accounting principles;
- Preparing the Management's Discussion and Analysis (including the performance measures), Required Supplementary Information, and Required Supplementary Stewardship Information;
- Establishing and maintaining effective internal control; and
- Complying with laws, regulations, contracts, and grant agreements applicable to Interior, including FFMIA.

In fulfilling this responsibility, management is required to make estimates and judgments to assess the expected benefits and related costs of internal control policies.

Auditors' Responsibilities. Our responsibility is to express an opinion on the fiscal year 2007 and 2006 financial statements of Interior based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin No. 07-04. Those standards and OMB Bulletin No. 07-04 require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of Interior's internal control over financial reporting. Accordingly, we express no such opinion.

KPMG

An audit also includes:

- Examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements;
- Assessing the accounting principles used and significant estimates made by management; and
- Evaluating the overall financial statement presentation.

We believe that our audits provide a reasonable basis for our opinion.

In planning and performing our fiscal year 2007 audit, we considered Interior's internal control over financial reporting by obtaining an understanding of Interior's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and OMB Bulletin No. 07-04. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*. The objective of our audit was not to express an opinion on the effectiveness of Interior's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of Interior's internal control over financial reporting.

As required by OMB Bulletin No. 07-04 in our fiscal year 2007 audit, with respect to internal control related to performance measures determined by management to be key and reported in the Management's Discussion and Analysis and Performance sections, we obtained an understanding of the design of internal controls relating to the existence and completeness assertions and determined whether these internal controls had been placed in operation. We limited our testing to those controls necessary to report deficiencies in the design of internal control over key performance measures in accordance with OMB Bulletin No. 07-04. However, our procedures were not designed to provide an opinion on internal control over reported performance measures and, accordingly, we do not provide an opinion thereon.

As part of obtaining reasonable assurance about whether Interior's fiscal year 2007 financial statements are free of material misstatement, we performed tests of Interior's compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of the financial statement amounts, and certain provisions of other laws and regulations specified in OMB Bulletin No. 07-04, including certain provisions referred to in FFMIA. We limited our tests of compliance to the provisions described in the preceding sentence, and we did not test compliance with all laws, regulations, contracts, and grant agreements applicable to Interior. However, providing an opinion on compliance with laws, regulations, contracts, and grant agreements was not an objective of our audit and, accordingly, we do not express such an opinion.

Under OMB Bulletin No. 07-04 and FFMIA, we are required to report whether Interior's financial management systems substantially comply with (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level. To meet this requirement, we performed tests of compliance with FFMIA Section 803(a) requirements.

This report is intended solely for the information and use of Interior's management, Interior's Office of Inspector General, OMB, the U.S. Government Accountability Office, and the U.S. Congress and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 13, 2007

Exhibit I

U.S. DEPARTMENT OF THE INTERIOR

Status of Prior Year Findings

September 30, 2007

Ref	Condition	Status
A	Controls over the Indian Trust Funds	This condition has not been corrected and is repeated in fiscal year 2007. See finding G.
B	Application and general controls over financial management systems	This condition has not been corrected and is repeated in fiscal year 2007. See finding A.
C	Controls over property, plant, and equipment	This condition has been corrected.
D	Reporting the Sport Fish Restoration and Boating Trust Fund	This condition has been corrected.
E	Controls over the U.S. Park Police Pension Plan	This condition has been corrected.
F	Controls over charge cards	This condition has not been corrected and is repeated in fiscal year 2007. See finding E.
G	Control assessment and assurance statement process	This condition has been corrected.
H	Controls over spending authority	This condition has been corrected.
I	Museum collections	This condition has been corrected.
J	*Single Audit Act Amendments of 1996*	This condition has not been corrected and is repeated in fiscal year 2007. See finding H.
K	Potential non-compliance with the *Anti-Deficiency Act*, acquisition regulations, and leasing laws and regulations	This condition has been corrected.
L	*Federal Financial Management Improvement Act of 1996*	This condition has been corrected.

U.S. Department of the Interior

NEWS

U.S. Department of the Interior

Office of the Secretary
FOR IMMEDIATE RELEASE
May 11, 2007

Contact:
Chris Paolino, (202) 208-6416

Kempthorne Names Michael Howell Chief Information Officer

WASHINGTON – Secretary of the Interior Dirk Kempthorne today announced that Michael Howell will become the Chief Information Officer for the Department of the Interior on May 14, 2007.

"Mike has a wealth of experience and a track record of accomplishment that that makes him well qualified for this position," Kempthorne said. "We are confident that he will provide the leadership to manage and enhance the Department's information technology infrastructure and programs."

The Chief Information Officer reports directly to the Secretary. The Office of the Chief Information Officer provides leadership to the department and its bureaus in all areas of information management and technology.

Howell is being promoted from his current position as the assistant director for Information Resources and Technology Management and Chief Information Officer for the U.S. Fish and Wildlife Service. At FWS, Howell was responsible for all aspects of information resources and technology management, policy, budget, strategic planning, and operations in the Fish and Wildlife Service.

Mike previously served as chief of the Information Technology Portfolio Management Division in the Department's Office of the Chief Information Officer, where he was responsible for overseeing the management of the Department's $900 million a year portfolio of IT investments. Earlier, Mike also served for two years as the acting CIO and deputy CIO for the Bureau of Land Management.

For five years in BLM's headquarters budget office, Mike was responsible for the budgets of a number of programs, including the Information Technology, Wildland Fire and Central Hazardous Materials appropriations. He ultimately led the development of BLM's entire budget.

Mike spent four years at BLM's Oregon State Office as a branch chief, responsible for software application development, Global Information System applications, and data and records management programs. He managed IT and GIS support for the President's Northwest Forest Plan and the Interior Columbia Basin Ecosystem Management Project. Mike spent seven years in BLM's Eugene District on forest inventory, land use planning, and National Environmental Policy Act analysis. He worked five years in a variety of forest management jobs in the Medford District in southwest Oregon. Mike's career began with the U.S. Forest Service in the Coeur d'Alene National Forest in Idaho and the Olympic National Forest in Washington.

A native of Bethlehem, Pennsylvania, Mike graduated in 1977 from Pennsylvania State University with a bachelor of science degree in Forest Science with a minor in Wildlife Management. In 2005, he completed the Chief Information Officer certificate program at the National Defense University IRM College. Mike and his wife Gretchen have a son, Sean, and a daughter, Victoria.

— DOI —

U.S. Department of the Interior
1849 C Street, NW
Washington, DC 20240
webteam@ios.doi.gov
Last Updated on 05/11/07

Status Report to the Court
Number Thirty-One

For the Period
July 1, 2007 through December 31, 2007

February 1, 2008

implemented throughout Interior, and challenges still remain in the C&A program and system configuration management.

- As reported in the *Status Report to the Court Number Thirty*, on March 13, 2007, OIG issued a Notice of Findings and Recommendations. Interior took the necessary steps to respond to the findings in that report, and the OIG investigation that was initiated as a result of this NFR is completed. On July 18, 2007, Interior released version 1.0 of the Defense-in-Depth Strategic Plan. Interior considers the matter closed.

Delays and Obstacles

Like other federal agencies, Interior must address many challenges regarding the integration, performance, funding, security, and data integrity of IT systems. Interior initiated or completed steps to address some of the challenges reported in this and previous reporting periods. However, delays and obstacles listed below impede progress in achieving Interior's IT management goals.

Staffing

Interior continues to experience high staff and management turnover in critical IT positions, particularly IT security.

Funding and Resources

- Limited congressional appropriations have impacted the ability of Interior to fill personnel vacancies, complete projects and meet deadlines.
- Court orders requiring bureaus and offices to maintain email backup tapes for indefinite periods require the acquisition and maintenance of an extremely large volume of expensive backup tape media. This cost burden on Interior bureaus and offices has diverted funding from other Interior programs.

Denied Internet Access

Four Interior bureaus and offices (BIA, OHA, OST and SOL) have not been permitted by the Court to have Internet access since December 5, 2001. As previously reported and detailed in the *Status Report to the Court Number Twenty-Eight*, lack of Internet access impedes work processes and the ability to communicate effectively, both internally and externally.

Lack of access to the Internet continues to cause daily inefficiencies for the off-line bureaus. Specific examples include:

- Litigation in federal court and administrative tribunals with multiple parties located all over the country is commonplace in Interior. In many cases, the judge and all of the parties except Interior conduct all of their legal matters over the Internet. Some tribunals require electronic filing. Interior attorneys use slow and perennially-busy fax machines to send and receive lengthy documents, causing delay and inconvenience not only for themselves but for the other parties. Alternatively, they must leave their offices and travel to their homes or their client agencies' offices (if those locations have computers authorized for such use) in order to send and receive documents. This time-wasting scenario is multiplied when drafts must be exchanged between field offices and

headquarters, between client agencies and the Solicitor's Office, and between the Department of Justice and the Solicitor's Office.

- Much information critical to Interior is accessible only on-line. Examples are some tribal statutes and regulations, the U.S. Patent and Trademark Office registry of logos and trademarks, GAO opinions, and licenses for commercial products being used by Interior.
- Participation in certain federal initiatives such as Continuity of Operations Plans, Influenza Pandemic Planning, and Homeland Security projects, is difficult if not impossible without Internet access, since some of these projects require review of sensitive documents available only through limited-access, secure Internet portals.
- Investigation of criminal use of Interior-owned seals and logos on the Internet (a problem especially for the National Park Service) cannot be accomplished on off-line computers.
- Ordinary office procedures that occur hundreds of times per day, which, if done on-line would take only seconds or minutes, instead require multiple telephoning and/or faxing. Support, program, and professional staff must have basic information for a wide variety of purposes: phone numbers of specific staff in government agencies; date of death for probates; vehicle values for tort claims; airline schedule and mileage for travel planning; price comparison for procurement activities; tracking information to locate FedEx packages, etc.

Assurance Statement

I concur with the content of the information contained in the Information Technology section of the *Status Report to the Court Number Thirty-One.* The information provided in this section is accurate to the best of my knowledge.

Date: January 24, 2008

Name: *Signature on File*
Michael J. Howell, Jr.
Department of the Interior Chief Information Officer