United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued April 11, 2006 Decided July 11, 2006

No. 05-5388

ELOUISE PEPION COBELL, ET AL.,
APPELLEES

v.

DIRK KEMPTHORNE, SECRETARY OF THE INTERIOR, ET AL.,
APPELLANTS

Appeal from the United States District Court
for the District of Columbia
(No. 96cv01285)

Mark B. Stern, Attorney, U.S. Department of Justice, argued the cause for appellants. With him on the briefs were *Peter D. Keisler*, Assistant Attorney General, *Kenneth L. Wainstein*, U.S. Attorney, *Gregory G. Katsas*, Deputy Assistant Attorney General, *Robert E. Kopp*, *Thomas M. Bondy*, *Alisa B. Klein*, *Mark R. Freeman*, *I. Glenn Cohen*, and *Isaac J. Lidsky*, Attorneys.

Dennis M. Gingold argued the cause for appellees. With him on the brief were *Elliott H. Levitas*, *G. William Austin, III*, *Mark I. Levy*, and *Keith M. Harper*.

Before: TATEL and BROWN, *Circuit Judges,* and SILBERMAN, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* BROWN.

BROWN, *Circuit Judge*: This case presents for our review yet another clash in a lawsuit that has found its way onto our docket many times in recent years, resulting in seven published opinions from this court. *See In re Kempthorne*, --- F.3d ---- (D.C. Cir. 2006)*; Cobell v. Norton*, 428 F.3d 1070 (D.C. Cir. 2005) (*Cobell XVII*); *Cobell v. Norton*, 392 F.3d 461 (D.C. Cir. 2004) (*Cobell XIII*); *Cobell v. Norton*, 391 F.3d 251 (D.C. Cir. 2004) (*Cobell XII*); *In re Brooks*, 383 F.3d 1036 (D.C. Cir. 2004); *Cobell v. Norton*, 334 F.3d 1128 (D.C. Cir. 2003); *Cobell v. Norton*, 240 F.3d 1081 (D.C. Cir. 2001) (*Cobell VI*). The Department of the Interior appeals a district court order of injunctive relief requiring many of Interior's computer systems to be disconnected from the internet and internal computer networks. The district court sought to protect the integrity of individual Indian trust data (IITD) residing on Interior's computers. Because we conclude the court's broad grant of equitable relief was an abuse of discretion, we vacate the injunction.

I

We need not delve too deeply into the extensive and oft-repeated history of this case. Briefly, the Secretary of the Treasury and the Secretary of the Interior are currently the designated trustee-delegates for the Individual Indian Money (IIM) trust. *Cobell VI*, 240 F.3d at 1088-89. Interior is responsible for executing most of the government's trust duties, although Treasury holds and invests IIM funds. *Id.* Interior's Bureau of Indian Affairs (BIA) is responsible for managing the lands held by the trust, including lease approvals and income collection, while Interior's Office of Trust Funds Management (OTFM) deposits revenues, maintains IIM accounts for individual Indians, and distributes funds to beneficiaries. *Id.* at 1088.

In 1994, Congress passed the American Indian Trust Fund Management Reform Act (the 1994 Act), Pub. L. No. 103-412, 108 Stat. 4239 (1995), which "recognized the federal government's preexisting trust responsibilities" and "further identified *some* of the Interior Secretary's duties to ensure 'proper discharge of the trust responsibilities of the United States.'" *Cobell VI*, 240 F.3d at 1090 (quoting 25 U.S.C. § 162a(d)). These duties include "[p]roviding adequate systems for accounting for and reporting trust fund balances," "[p]roviding adequate controls over receipts and disbursements," "[p]roviding periodic, timely reconciliations to assure the accuracy of accounts," and "[p]reparing and supplying periodic statements of account performance and balances to account holders." *Id.* (internal quotation marks and ellipses omitted).

Appellees, beneficiaries of the IIM trust accounts, brought this class action suit in 1996 "to compel performance of trust obligations." *Id.* at 1086, 1092. Some of the proceedings subsequently conducted by the district court related to Interior's problems maintaining adequate computer security. On December 5, 2001, the district court entered a temporary restraining order requiring Interior to disconnect from the internet all information technology (IT) systems that housed or provided access to IITD. *See Cobell v. Norton*, 274 F. Supp. 2d 111, 113 (D.D.C. 2003) (*Cobell IX*). Later that month, Interior entered into a consent decree providing that it would only reconnect its systems to the internet with the consent of a special master, *id.* at 113-14; this arrangement resulted in about 95% of Interior's computers being reconnected within a year, *Cobell v. Norton*, 310 F. Supp. 2d 77, 82 (D.D.C. 2004) (*Cobell XI*). The special master came to suspect, however, that some of Interior's employees were thwarting efforts to test the security of Interior's IT systems. *Cobell IX*, 274 F. Supp. 2d at 114-24. The district court entered a preliminary injunction requiring Interior once again to disconnect all computers from the internet, with a

few exceptions, and allowing reconnection only upon the district court's approval. *Cobell v. Norton*, 310 F. Supp. 2d 98, 99-101 (D.D.C. 2004) (*Cobell XI Order*).

On appeal, we explained that the district court had "authority to exercise its discretion as a court of equity in fashioning a remedy to right a century-old wrong or to enforce a consent decree." *Cobell XII*, 391 F.3d at 257. As "[t]he district court did not order . . . wholesale programmatic changes" or "include particular tasks for Interior to perform based on policies developed by the district court," we rejected Interior's argument that the injunction "violated the separation of powers." *Id.* at 258. Nevertheless, we still found that the district court erred in issuing the preliminary injunction. The district court had erroneously shifted the burden of persuasion to Interior to show why disconnection was unnecessary, *id.* at 259, and had also erred by disregarding Interior's certifications on IT security as procedurally and substantively defective, *id.* at 260-61. Finally, we stated that the district court abused its discretion in granting the injunction without first holding an evidentiary hearing, as material facts were in dispute and almost nine months had passed since a previous hearing. *Id.* at 261-62.

II

Before proceeding to our discussion of the current disconnection order, we pause to address an alleged conflict between our prior decisions in this case. Both parties cite this court's prior precedent in support of opposing perspectives. Interior argues that the district court, by issuing the new computer disconnection order, has improperly injected itself into the day-to-day management of the agency, ignoring this court's prior warnings against judicial entanglement in policy disputes. The class members argue that Interior's arguments are foreclosed by *Cobell XII*; they claim that *Cobell XIII* and *XVII* conflict with

that slightly earlier decision (as well as with *Cobell VI*), and that in deciding this case, we are not bound by the later opinions. As we explain, the alleged conflict is illusory, though some degree of confusion is understandable. In the course of this litigation, we have repeatedly described the interaction of the Administrative Procedure Act (APA) and the common law of trusts, though with slightly different emphases depending on the issue before us. Yet careful analysis reveals no significant, substantive disagreement between our decisions. As in earlier cases, both the APA and the common law of trusts apply in this case; the specific question to be addressed determines which body of law becomes most prominent.

In *Cobell VI*, we addressed the district court's finding that Interior had breached its trust duties. We noted that the class members sought injunctive and declaratory relief; thus, the federal government's sovereign immunity was waived under the APA. 240 F.3d at 1094-95. We also looked to the APA for resolution of another jurisdictional issue, i.e., the presence of final agency action, which is a prerequisite to judicial review. *Id.* at 1095. While we found no final action in that case, we nonetheless found the class members' claims to be reviewable, since under the APA, "federal courts may exercise jurisdiction to compel agency action 'unlawfully withheld or unreasonably denied.'" *Id.* (quoting 5 U.S.C. § 706). However, though we looked primarily to administrative law concepts in resolving jurisdictional issues, we did not proceed in the same manner when construing the trust duties implied by the 1994 Act. We acknowledged that under *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984), "ordinarily we defer to an agency's interpretations of ambiguous statutes entrusted to it for administration," but we declined to defer to Interior's interpretation of the Act. *Cobell VI*, 240 F.3d at 1100. We gave Interior's interpretation "'careful consideration,'" *id.* at 1101(quoting *Muscogee (Creek) Nation v. Hodel*,

851 F.2d 1439, 1445 n.8 (D.C. Cir. 1988)), but the normally-applicable deference was trumped by the requirement that "'statutes are to be construed liberally in favor of the Indians, with ambiguous provisions interpreted to their benefit,'" *id.* (quoting *Montana v. Blackfeet Tribe of Indians*, 471 U.S. 759, 766 (1985)).

In determining the scope of the government's duties, we found that both administrative law and trust law applied. "While the government's obligations are rooted in and outlined by the relevant statutes and treaties, they are largely defined in traditional equitable terms." *Id.* at 1099. Thus, "'the government's fiduciary responsibilities necessarily depend on the substantive laws creating those obligations,'" *id.* at 1098 (quoting *Shoshone-Bannock Tribes v. Reno*, 56 F.3d 1476, 1482 (D.C. Cir. 1995)), but "[c]ourts 'must infer that Congress intended to impose on trustees traditional fiduciary duties unless Congress has unequivocally expressed an intent to the contrary,'" *id.* (quoting *NLRB v. Amax Coal Co.*, 453 U.S. 322, 330 (1981)). At the same time, "[d]espite the imposition of fiduciary duties, federal officials retain a substantial amount of discretion to order their priorities." *Id.* The presence of fiduciary duties does limit this discretion: "When faced with several policy choices, an administrator is generally allowed to select any reasonable option," but choices made when acting as a trustee must also satisfy fiduciary obligations. *Id.* Thus, when we upheld the district court's finding that an accounting was required, we noted approvingly that "[t]he district court explicitly left open the choice of how the accounting would be conducted, and whether certain accounting methods, such as statistical sampling or something else, would be appropriate." *Id.* at 1104. "Such decisions," we concluded, "are properly left in the hands of administrative agencies." *Id.*

In *Cobell XII*, we reviewed the district court's first computer disconnection order. We pointed out that *Cobell VI* "did

not limit the district court's authority to exercise its discretion as a court of equity in fashioning a remedy to right a century-old wrong or to enforce a consent decree." 391 F.3d at 257. "[T]he narrower judicial powers appropriate under the APA do not apply" when the court is fashioning equitable remedies for breaches of fiduciary duties. *Id.* We stated that "because the underlying lawsuit is both an Indian case and a trust case in which the trustees have egregiously breached their fiduciary duties," the district court "retains substantial latitude, much more so than in the typical agency case, to fashion an equitable remedy." *Id.* at 257-58. We rejected Interior's argument that the district court's role should have been confined to "retaining jurisdiction and ordering periodic progress reports"; however, we still recognized limits on the district court's ability to craft relief. *Id.* at 258. The district court could not order "wholesale programmatic changes" or prescribe "particular tasks for Interior to perform based on policies developed by the district court." *Id.* While we ultimately vacated the disconnection order, we found that the district court properly "limited its role to accepting or rejecting the Secretary's proposals, rather than dictating their substance or even the standard for measuring the security of Interior's IT systems." *Id.*

One week later, in *Cobell XIII*, we applied these concepts to a "structural injunction" issued by the district court, upholding one portion of the injunction and vacating the rest. 392 F.3d at 478. We reiterated that under the APA, courts may only review specific agency action or unreasonable delay by an agency; courts cannot order "programmatic improvements," *id.* at 472 (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 891 (1990)) or "compel[] compliance with broad statutory mandates," *id.* (quoting *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 66 (2004)). At the same time, we acknowledged the role played by the common law of trusts, which "flesh[es] out the statutory mandates" assigned to Interior. *Id.* at 473. Yet even

the "availability of the common law of trusts cannot fully neutralize the limits placed by the APA and the [Supreme] Court's *Lujan* and *Southern Utah* decisions," as similar limits exist even within that venerable body of law:

> While a court might certainly act to prevent or remedy a trustee's wrongful intermingling of trust accounts, this does not imply that the normal remedy would be an order specifying *how* the trustee should program its computers to avoid intermingling, as opposed to, for example, barring the use of a program that had caused forbidden intermingling or was clearly likely to do so. See Bogert & Bogert, Law of Trusts and Trustees § 861, p. 22 ("If the trustee has been given discretion with respect to the act in question, . . . the court will not interfere by ordering him to take a certain line of conduct unless there is proof of an abuse of the discretion . . . ."). "[A] court of equity will not interfere to control [trustees] in the exercise of a *discretion vested in them by the instrument* under which they act." *Firestone Tire and Rubber Co. v. Bruch*, 489 U.S. 101, 111 (1989) (internal quotation marks and citation omitted).

Id.

Applying these standards, we upheld a portion of the district court's order that "in effect required discovery of Interior's plans consistent with the district court's broad case management authority." *Id.* at 474. However, other parts of the order went much further, requiring Interior to implement its trust management plan and identify areas where its plan might conflict with its fiduciary duties. *Id.* Essentially, the district court "propose[d] to use the 'plan' as a device for indefinitely extended all-purpose supervision of the defendants' compliance with . . . sixteen general fiduciary duties." *Id.* We held that such judicial monitoring was only appropriate to the extent that it was based on

specific findings of unlawful behavior, and we explained that the "district court cannot issue enforcement remedies . . . for trust breaches that it has not found to have occurred." *Id.* As the district court had not made sufficient findings that Interior had breached trust duties, its order to implement the trust management plan amounted to an overbroad "order to obey the law in managing the trusts." *Id.* at 475. Thus, we vacated the order "insofar as it direct[ed] Interior, rather than the plaintiffs, to identify defects in its proposal and require[d] the agency to comply" with its proposed trust management plan. *Id.* We also vacated a requirement that Interior compile a list of applicable tribal laws, as that instruction "seem[ed] a specification not of Interior's trust duties but of the court's preferred methodology for assuring Interior's fulfillment of those duties," and thereby "collide[d] with the APA, *Lujan*, and *Southern Utah*." *Id.*

Finally, in *Cobell XVII*, we vacated the district court's reissued injunction ordering a historical accounting. 428 F.3d at 1079. We noted the 1994 Act, which reaffirmed Interior's duty to provide an accounting, did not prescribe the scope of the accounting; thus, "[i]n the ordinary APA case Interior would clearly enjoy a high degree of deference to its interpretation of the 1994 Act, including its ideas on the appropriate trade-off between absolute accuracy and cost (in time and money)." *Id.* at 1074. We recognized, however, that although the class members' "core claim" was brought under the APA (as they sought to compel agency action that had been unreasonably delayed), the dispute was "not an ordinary APA case." *Id.* The common law of trusts limited the deference we would give to Interior's interpretation of the Act. *Id.* Still, "because the IIM trust differs from ordinary private trusts along a number of dimensions, the common law of trusts [did not] offer a clear path for resolving statutory ambiguities" regarding accounting methodology. *Id.* As neither statutory language nor trust principles established a "definitive balance between exactitude and cost" in performing

the accounting, we concluded "the district court owed substantial deference to Interior's plan." *Id.* at 1076. We noted that "[t]he choices at issue required both subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." *Id.* Hence, the district court erred when it "quite bluntly treated the character of the accounting as its domain" and "displaced Interior as the actor with primary responsibility for 'working out compliance with the broad statutory mandate.'" *Id.* (quoting *S. Utah*, 542 U.S. at 66-67) (brackets omitted).

While our prior decisions in this case have thus relied on administrative law and trust law to varying degrees on different occasions, we have always clearly held that both bodies of law apply. Because this case involves the management of a trust, our decisions draw on the principles of trust law developed by Anglo-American jurisprudence over the course of nearly a thousand years of experience using this venerable legal structure.[1] Yet because we are addressing the operations of an executive agency, we are also bound by the rules of administrative law (despite the somewhat less-storied pedigree of the APA, a relative newcomer at only sixty years old). Where these two bodies of law would lead us to different results, we must decide which of the two more appropriately governs the specific

---

[1] The history of "the use" as a method of conveying property can be traced back to a "slight but unbroken thread of cases, beginning while the Conquest is yet recent." 2 Frederick Pollock & Frederic William Maitland, *The History of English Law* 231 (2d ed. 1923). Indeed, "the development from century to century of the trust idea" has been called "the greatest and most distinctive achievement performed by Englishmen in the field of jurisprudence." 1 Austin Wakeman Scott & William Franklin Fratcher, *The Law of Trusts* § 1 (4th ed. 1987) (quoting Frederic William Maitland, Selected Essays 129 (1936)).

question at hand. Thus, we looked to the APA to find a waiver of sovereign immunity, allowing the class members to seek nonmonetary relief against the government. *Cobell VI*, 240 F.3d at 1094. Similarly, we applied APA standards in determining whether Interior had unreasonably delayed the performance of its duties, thereby subjecting itself to judicial review. *Id.* at 1095-96. Such analysis was necessary because our jurisdiction is limited to addressing specific agency action or inaction. *Cobell XIII*, 392 F.3d at 472. On the other hand, while the trust relationship arises out of statutes, the government's obligations "are largely defined in traditional equitable terms." *Cobell VI*, 240 F.3d at 1098-99; *see also Cobell XII*, 391 F.3d at 257. We rely on the common law to "flesh out" the statutory mandates and determine the precise contours of the government's responsibilities. *Cobell XIII*, 392 F.3d at 473; *see also Cobell XVII*, 428 F.3d at 1074-75; *Cobell XII*, 391 F.3d at 257; *Cobell VI*, 240 F.3d at 1099, 1101.

The two bodies of law overlap in shaping our ability to grant relief once a specific breach of an established duty has been found. Because "an on-going program or policy is not, in itself, a 'final agency action' under the APA," our jurisdiction does not extend to reviewing generalized complaints about agency behavior. *Cobell VI*, 240 F.3d at 1095. Consequently, as each case only presents the court with a narrow question to resolve, it can have no occasion to order wholesale reform of an agency program. *Id.*; *see also Cobell XIII*, 392 F.3d at 472; *Cobell XII*, 391 F.3d at 258. Still, "because the underlying lawsuit is both an Indian case and a trust case in which the trustees have egregiously breached their fiduciary duties," the court "retains substantial latitude, much more so than in the typical agency case, to fashion an equitable remedy." *Cobell XII*, 391 F.3d at 257; *see also Cobell VI*, 240 F.3d at 1109. These equitable powers, limited at one end of the spectrum by the court's inability to order broad, programmatic reforms, are also

limited in the opposite direction by an inability to require the agency to follow a detailed plan of action. The court generally may not prescribe specific tasks for Interior to complete; it must allow Interior to exercise its discretion and utilize its expertise in complying with broad statutory mandates. *Cobell VI*, 240 F.3d at 1099, 1106; *see also Cobell XII*, 391 F.3d at 258. These restraints are put in place by both administrative law, *see Cobell XVII*, 428 F.3d at 1076 (quoting *S. Utah*, 542 U.S. at 66-67), and trust law, *see Cobell XIII*, 392 F.3d at 473 (quoting *Firestone Tire & Rubber Co.*, 489 U.S. at 111). The ability of the agency itself to exercise its discretion is somewhat constrained, however. Rather than its normal freedom to choose "any reasonable option," the agency's actions must satisfy fiduciary standards. *Cobell VI*, 240 F.3d at 1099.

III

With this background in mind, we turn to the most recent computer disconnection order issued by the district court. After we vacated the previous disconnection order in *Cobell XII*, the class members filed a motion in the district court for a new injunction that would yet again require disconnection of Interior's computers from the internet. *Cobell v. Norton*, 394 F. Supp. 2d 164, 169 (D.D.C. 2005) (*Cobell XVI*). In response, the district court held a fifty-nine day evidentiary hearing to evaluate Interior's current IT security. *Id.* at 170.

In its extensive findings of fact, which Interior does not challenge, the district court reviewed the development of Interior's IT security over the last few years. In a 2002 report to Congress, the Office of Management and Budget (OMB) stated that less than a third of Interior's IT systems had an up-to-date security plan and that less than a fourth of the systems had passed a security certification and accreditation process. *See id.* at 189. OMB noted that these statistics were not necessarily

reliable, as Interior lacked a complete inventory of its IT systems. *Id.* Additionally, OMB found that Interior had not implemented some of its own security policies. *Id.* In 2003, Interior's Inspector General (IG) evaluated the Department's security pursuant to the Federal Information Security Management Act (FISMA). *Id.* at 177, 190. The IG cited the same problems reported by OMB the previous year, and also found that Interior did not have an effective program for providing security training to employees and contractors. *Id.* at 190-92.

The IG's 2004 report found that Interior's IT security management program was "effectively designed" to meet FISMA's requirements but again concluded that the program had not been consistently implemented. *Id.* at 193-94. The IG tested twenty systems and found that the majority of them had not been properly certified and accredited. *Id.* at 194. Interior had particularly failed to provide sufficient oversight of IT systems run by contractors and to document security procedures adequately. *Id.* at 194-95. Interior did conduct some security testing on its IT systems, but it relied primarily on a tool that scanned only for the twenty most serious security weaknesses. *Id.* at 196. Also, the IG again noted that Interior needed to develop consistent policies for IT security training. *Id.* at 198.

The IG also conducted extensive testing of the security of Interior's wireless networking technology in 2003 and 2004. *Id.* at 223. Diann Sandy, who managed this testing, found Interior likely still lacked a complete inventory of its wireless devices. *Id.* at 226. Sandy's team also identified several other problems with Interior's management of its wireless network security, including failure to manage the range of its wireless signals, insufficient security controls on its wireless networks, and inadequate physical security in locations with wireless networks.

Id. at 227.[2] Sandy also oversaw a review of Interior's "plan of action and milestones" (POA & M) program. *Id.* at 229. For each IT system or program where a security weakness had been located, Interior was supposed to have a POA & M that would identify the actions needed to correct the weakness and specify a schedule for correction. *Id.* at 230. Sandy's review found that not all known weaknesses were included in Interior's departmental POA & M and that many weaknesses reported as corrected had not actually been fixed. *Id.* at 231-33.

In the 2005 FISMA evaluation, the IG added a significant new element to its evaluations of Interior's IT security by hiring contractors to conduct external penetration testing. *Id.* at 199-202. The penetration testing was designed to identify systems' vulnerabilities by simulating attacks by outside parties with limited prior knowledge of Interior's computer systems. *Id.* at 203. Under the "Rules of Engagement" governing the testing, the contractors could use a wide variety of tools, including licensed security software, publicly-available freeware, custom developed utilities, and social engineering techniques. *Id.* at 203 & n.18. Although the contractors were prohibited from modifying files, disabling users, or denying service, their goal was to gain "administrator" or "root" privileges, which would enable them to control the targeted systems. *Id.* at 203.

Scott Miles performed the penetration testing of systems at several of Interior's bureaus. Testing at the Bureau of Land Management (BLM) revealed a number of vulnerabilities that put the systems at risk of unauthorized access from the internet. *Id.* at 205. Miles was able to gain administrator privileges to at least two systems after initial penetration of the network,

---

[2] In April 2004, Interior issued a moratorium on the use of wireless technology, *id.* at 237-38, although apparently some offices may not be complying with the directive, *id.* at 241.

including an email archiving system and a system used to manage data from land surveys. *Id.* at 206. Some of BLM's systems' vulnerabilities were due to conscious policy choices regarding interagency access to information, rather than mere failure to implement security practices. *Id.* Still, BLM severed most of its systems' internet access as a result of the testing. *Id.* at 205. Penetration testing of the BIA network had to be performed on-site, as that bureau was already disconnected from the internet; only one BIA location had its network tested. *Id.* at 209-11. Miles found that the BIA network would have "an extremely small footprint for such a large organization" if it were reconnected. *Id.* at 210. However, Miles did observe "a server room with quite a few servers in it" at the BIA facility, leading him to question whether he had truly been given access to their entire network. *Id.* at 211. Miles also tested the network at Interior's Bureau of Reclamation (BOR), where he was able to access multiple BOR systems through one particular vulnerability in a web application. *Id.* at 212. The penetration was not noticed by BOR for seven days, and it took three more days to block access to other systems. *Id.* at 213. In contrast, Miles was not able to penetrate into any systems at Interior's Mineral Management Service (MMS), despite finding a few vulnerabilities. *Id.* at 213-14.[3]

Testing of the systems at Interior's National Business Center (NBC) was performed by another contractor, Philip Brass, who was able to enter NBC's most sensitive networks and gain access to financial records and other data. *Id.* at 215-16. Brass initially exploited a vulnerability in an NBC web application and successfully used that entrance point to access several other linked databases and even another agency's network. *Id.*

---

[3] Miles did discover another system containing some MMS data that was run by a "non-governmental entity," but he was not able to obtain permission to fully test that system's vulnerabilities. *Id.* at 214.

at 217-19. Ultimately, Brass was able to access personal information regarding over 72,000 Interior employees; for dramatic effect, he assembled dossiers on several high-level officials, including data such as social security numbers and even a list of bank card charges. *Id.* at 218.

After reviewing these and other evidentiary findings, the district court concluded that, though Interior had made significant progress in improving its IT security over the previous few years, "severe and sometimes catastrophic problems remain." *Id.* at 249.

> Certification and accreditation documents have been found to be incomplete, or sometimes missing entirely, resulting in the decertification of systems. The most critical IT security process, the departmental POA & M program, is currently broken, resulting in uncertainty both as to the nature and number of weaknesses in IT systems, and as to whether and to what extent known weaknesses have been corrected. Interior has not implemented a coherent policy to ensure that wireless networking devices do not compromise the security of wired networks. Interior has not even begun to fulfill its responsibility to ensure that its systems and data housed on private contractor networks are adequately secure . . . . System inventories are incomplete, IT security training is inadequate, and mission-critical systems lack essential, fundamental technical controls.

Id. The district court found that Interior's IT managers "seem incapable of ensuring the implementation of IT security policies on the one hand, and recognizing fundamental, systemic flaws in those policies on the other." *Id.* Additionally, the district court identified deficiencies in Interior's management of internal network security against threats from sources such as employees, contractors, and tribes—i.e., those who could misuse

legitimate network access. *Id.* at 254-55. The district court found that Interior had "no concrete plans for implementation" of penetration testing against internal threats, and that Interior "has not incorporated evaluation of third-party systems housing Interior assets into its overall IT security program." *Id.* at 255-56.

The district court particularly criticized Interior's handling of Indian trust data, pointing out that Interior lacked "any standard, department-wide definition of trust data." *Id.* at 261. The district court speculated that "fundamental confusion" over what constitutes trust data "may be a cause of Interior's continuing inability to carry out what seems to be the most immediate, commonsense step to securi[ng] electronic trust data—namely segregating IITD on secure servers separate from Interior's accessible IT networks and systems." *Id.* Interior did categorize trust systems as "high risk," not because it had "made a firm determination that they represented high risk but to give them priority within the department" due to Interior's "court environment," presumably a reference to this litigation. *Id.* at 261-62. Several Interior employees objected to categorizing trust systems as "high risk" under the current guidelines, as no "potential result for loss of human life or . . . catastrophic impact" would result if the systems became inoperable; those employees argued that a "moderate" categorization would be more appropriate. *Id.* at 263. The district court faulted this reasoning, finding that it did not "take into account the special impacts that a breach of the confidentiality, integrity, or availability of IITD would have on both individual Indian trust beneficiaries and Interior." *Id.* at 263-64. Because "any loss of trust data carries the additional potential impact of legal liability for breach of fiduciary duty," the district court found that "[i]ntuitively, . . . Interior ought to incorporate these additional impacts into its data sensitivity classifications," such as by "treating Trust data and Trust systems as 'high risk.'" *Id.* at 264.

> The Court is thus concerned that Interior may be presently failing to incorporate its fiduciary obligations to preserve IITD into its IT security policy generally, and into its [certification and accreditation] program specifically. To be sure, certification and accreditation is the standard with which Interior must comply to adhere to OMB's guidance for complying with FISMA. However, the Court cannot accept certification and accreditation alone as sufficient to show that Interior's IT systems are presently adequately secure to comply with Interior's fiduciary obligations as Trustee-delegate for the IIM trust.

Id. Hence, the district court found "an overall failure of departmental IT-management to place the proper emphasis on compliance with Interior's fiduciary obligations in implementing the department's overall IT security program." *Id.* at 266.

While acknowledging that "it is generally considered impossible to create a perfectly secure IT environment," the district court nonetheless stated that "Interior's fiduciary obligation to preserve IITD requires that IT security take a prominent position among the department's priorities." *Id.* at 269. The district court faulted the IG for failing "to place special emphasis on scrutinizing" the security of trust data. *Id.* at 270. It acknowledged that Interior has "a variety of non-Indian customers to serve, and a massive amount of non-Indian Trust related data and IT infrastructure to secure," and noted that Interior could not "overemphasize some areas of IT security at the expense of others." *Id.* Still, it stated that

> Interior's fiduciary obligations as Trustee-Delegate for the IIM trust differentiate its IT security position from that of other federal agencies. While all Interior IT systems generally should be expected to conform to industry and government standards for adequate IT security, its systems

> housing or accessing Trust Data must meet a higher standard.

Id.

Based on these findings, the district court decided to grant the class members' request for an injunction. The district court found that the class members, "having already succeeded in the initial phases of this litigation [regarding Interior's breach of trust duties], have certainly demonstrated a substantial likelihood of success on the merits" of their action for an accounting. *Id.* at 273. Next, the district court found that corruption or loss of trust records would be an irreparable injury to the class members and that the "evidence demonstrates that the current state of IT security at Interior places IITD at imminent risk of corruption or loss." *Id.* The district court acknowledged that issuing an injunction would cause "inevitable harm to Interior," as the department's operations would be disrupted by an order requiring the disconnection of computer systems. *Id.* at 274. While conceding that injunctive relief would not be "likely to prove popular in governmental circles," the district court decided that it could fashion relief "that minimizes the impact of disconnection on Interior's ability to function and service its customers." *Id.* Indeed, the district court speculated that a disconnection order may be in Interior's own best interest, as it could "illuminate the pervasive problems that continue to plague Interior's IT security environment." *Id.* at 274-75. Still, it conceded, "[p]riorities will likely have to be shuffled, resources will likely have to be redirected, and processes will likely have to be adapted temporarily." *Id.* at 275.

Finally, the district court found that the public interest supported issuing an injunction. Systems serving critical functions such as fire suppression could be exempted from disconnection, and, the court found, "Interior will be able to

work around the absence of Internet connectivity in the short term to continue to provide services to the Indians while it secures their IITD." *Id.* The district court found that as "IIM trust beneficiaries comprise approximately 1/600th of the population of the country," the class members' interests "are a good percentage of the public interest in general." *Id.* The district court also found that the interests of the rest of the public supported the same conclusion: "As far as Interior's other customers are concerned, their interests are similarly best protected if Interior's IT systems are adequately secure," and "[e]very citizen of this country has an interest in seeing his or her government carry out its legal duties." *Id.*

The order issued by the district court required Interior to "disconnect all Information Technology Systems that [h]ouse or provide [a]ccess to Individual Indian Trust Data" from the internet, "all intranet connections," "all other Information Technology Systems," and "any contractors, Tribes, or other third parties." *Id.* at 277-78.[4] The court gave Interior twenty days to identify systems not housing or providing access to IITD,

---

[4] The court defined "Information Technology System" as

> Any computer, server, equipment, device, network, intranet, enclave, or application, or any subsystem thereof, that is used by Interior or any of its employees, agents, contractors, or other third parties in the electronic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or other information, including without limitation computers, wireless devices (e.g. Blackberrys) and networks, voice over the Internet protocol (VOIP), ancillary equipment, devices, or similar services or protocols, including support services, software, firmware, and related resources.

Id. at 276-77.

permitting the class members to contest those designations. *Id.* at 278. The district court exempted from disconnection IT systems "necessary for protection against fires or other such threats to life, property, or national security," although the class members could contest those system designations as well. *Id.*

Interior would be allowed to reconnect any IT systems housing or providing access to IITD for up to five days per month, in order to receive or distribute trust funds or "conduct[] other necessary financial transactions." *Id.* In order to permanently reconnect the affected systems, Interior would be required to file a proposal including "all of the following":

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

Id. The class members could then respond to any such proposal, after which the Court would "conduct any necessary evidentiary hearing and decide whether a proposed Information Technology System may be reconnected and order further relief, as appropriate." *Id.*

IV

Interior argues that "[n]othing in . . . FISMA could plausibly be construed to mandate [the] disconnections" ordered by the district court. Appellant's Br. 48. As a brief examination of the statutory structure will demonstrate, this argument fails to address the real issues in this case, as we are concerned with Interior's trust duties, not with the decisions made by Interior under FISMA. FISMA is intended to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3541(1). The statute is also designed to "recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks." *Id.* § 3541(2). To achieve those goals, FISMA assigns responsibilities to the Director of OMB and to the head of each agency.

FISMA makes the head of each agency 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" agency information. *Id.* § 3544(a)(1)(A). The agency head must ensure that senior agency officials assess "the risk and magnitude" of those possible harms and implement "policies and procedures to cost-effectively reduce risks to an acceptable level." *Id.* § 3544(a)(2)(A)-(C). He must also ensure that senior officials "periodically test[] and evaluat[e]" these security controls. *Id.* § 3544(a)(2)(D).

The Director of OMB is charged with "developing and overseeing the implementation of policies, principles, standards, and guidelines on information security." *Id.* § 3543(a)(1). He may "enforce accountability for compliance" with FISMA's

requirements by "tak[ing] any action that [he] considers appropriate, including an action involving the budgetary process or appropriations management process." *Id.* § 3543(a)(4); 40 U.S.C. § 11303(b)(5)(A). Additionally, the Director must review each agency's security programs at least annually and approve or disapprove them. 44 U.S.C. § 3543(a)(5). Finally, he must report to Congress annually regarding agency compliance, including identifying "significant deficiencies in agency information security practices" and planned remedial actions to address such deficiencies. *Id.* § 3543(a)(8).

Each agency must "develop, document, and implement an agencywide information security program" approved by the Director of OMB. *Id.* § 3544(b). In addition to the requirements discussed above, the program must include "security awareness training" for agency personnel and contractors and "procedures for detecting, reporting, and responding to security incidents." *Id.* § 3544(b)(4), (7). Each agency is required to report annually to the Director of the OMB and to Congress on "the adequacy and effectiveness" of its security program, including reporting any "significant deficienc[ies]." *Id.* § 3544(c)(1), (3). Within each agency, an independent auditor, generally that agency's Inspector General, must perform an independent annual evaluation of the security program; the results of this evaluation must be included in OMB's report to Congress. *Id.* § 3545(a)-(g). Finally, the Comptroller General is also required to "periodically evaluate and report to Congress" on agencies' implementation of FISMA. *Id.* § 3545(h).

In complying with their obligations under FISMA, the Director of OMB and agency heads must also ensure compliance with information security standards promulgated by the Department of Commerce. *See, e.g.*, *id.* §§ 3543(a)(1)-(2), 3544(a)(1)(B)(i) (incorporating the requirements of 40 U.S.C. § 11331). The Secretary of Commerce can make those standards

"compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of Federal information systems." 40 U.S.C. § 11331(b)(1). The Secretary of Commerce must exercise this authority "in coordination with the Director of [OMB]" and must base the standards on "standards and guidelines developed by the National Institute of Standards and Technology" (NIST). *Id.* § 11331(a)(1). The NIST, in turn, is required by statute to "consult with other agencies and offices" (including at least six enumerated agencies) when developing its standards and guidelines. 15 U.S.C. § 278g-3(c)(1). The purpose of such collaboration is to "improve information security and avoid unnecessary and costly duplication of effort," as well as to ensure that the standards and guidelines "are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems." *Id.* § 278g-3(c)(1)(A), (B). The NIST's standards and guidelines must not require "specific technological solutions or products" and must "permit the use of off-the-shelf commercially developed" products as much as possible. *Id.* § 278g-3(c)(5), (7). The NIST must give the public a chance to comment on proposed standards and guidelines, *id.* § 278g-3(c)(2), and must provide agencies with assistance with implementation, *id.* § 278g-3(d)(2).

FISMA, nestled as it is within this multilayered statutory scheme, thus 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. We are far from certain that courts would ever be able to review the choices an agency makes in carrying out its FISMA obligations,[5] but we need not explore that question any

[5] Interior has not argued that FISMA is a "statute[] preclud[ing] judicial review" under 5 U.S.C. § 701(a).

further today. The only issue we need to decide here is whether the district court was justified in granting such broad equitable relief to the class members, not whether Interior's actions have been sufficient to achieve the goals of FISMA.[6] We express no opinion as to whether FISMA would on its own require Interior to disconnect its IT systems from the internet and internal networks. This is not a FISMA compliance case, whether or not such an animal exists elsewhere.

V

We thus arrive at the question of whether the equitable relief granted by the district court was proper. The district court styled this relief as a preliminary injunction, *Cobell XVI*, 394 F. Supp. 2d at 272, but the injunction is more than merely "preliminary." "The usual role of a preliminary injunction is to preserve the status quo pending the outcome of litigation." *Dist. 50, United Mine Workers of Am. v. Int'l Union, United Mine Workers of Am.*, 412 F.2d 165, 168 (D.C. Cir. 1969). The ultimate relief sought in this case is an accounting of the IIM trust, but the role of the injunctive relief granted by the district court was not to protect the class members' interests while the court determines whether an accounting would take place. The class members have already prevailed on their most fundamental arguments: the court has recognized their right to an accounting and found that Interior has unreasonably delayed providing that accounting. *See Cobell VI*, 240 F.3d at 1095-97. The injunction serves as a preparatory step toward that eventual accounting (whatever its form), as the district court intended to protect

[6] Accordingly, we need not consider the propriety of the district court's choice to criticize the security levels that Interior assigned to trust data, nor whether Interior acted consistently with FISMA in upgrading the security levels of IITD based on its "court environment." *See Cobell XVI*, 394 F. Supp. 2d at 21-64.

electronic trust records while an accounting could be planned and completed. Thus, although the nature and scope of the accounting have yet to be determined, the disconnection order cannot accurately be called a "preliminary" injunction. Rather, it is a collateral portion of the ultimate relief sought by the class members.

We review the decision to issue an injunction for abuse of discretion. *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 320 (1982); *Woerner v. U.S. Small Bus. Admin.*, 934 F.2d 1277, 1279 (D.C. Cir. 1991). To determine whether injunctive relief is appropriate, we must balance the equities and hardships on both sides, *Woerner*, 934 F.2d at 1279, and must pay particular regard to whether such relief would further the public interest, *Romero-Barcelo*, 456 U.S. at 312.

We are unconvinced the class members demonstrated that they would necessarily suffer harm without this injunction. To be sure, the evidence of flaws in Interior's IT security is extensive. The penetration testing demonstrated that an individual with the requisite skills and resources could gain access to many of Interior's systems. We are not so naïve as to deny the possibility that such an individual may indeed hack into Interior's systems and even alter IITD, especially given that the spotlight of this litigation may make Interior's systems an inviting target. Similarly, a disgruntled employee, contractor, or Tribe member could choose to use legitimate access to Interior's networks for malicious purposes, taking advantage of the connections between different systems to do widespread damage to trust data.

Yet such concerns, though quite plausible, lack the specificity needed to justify injunctive relief, especially given the magnitude of the harm that this injunction would cause Interior. The class members have pointed to no evidence showing that

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

We do not mean to understate the dangers of lax IT security, but as the district court acknowledged, "it is generally considered impossible to create a perfectly secure IT environment." *Cobell XVI*, 394 F. Supp. 2d at 269. The inherently imperfect nature of IT security means that if we granted injunctive relief here, based only on Interior's security vulnerabilities and not on a showing of some imminent threat or specific reason to be concerned that IITD is a target, we would essentially be justifying perpetual judicial oversight of Interior's computer systems. In order to return to normal operations, Interior would be faced with the nearly impossible task of ensuring that its systems have no exploitable weaknesses whatsoever, rather than addressing a more specific danger to IITD. Moreover, nearly any system administrator who maintains data for private trusts could be in danger of facing similar claims for relief, as only the unreachable goal of perfect security would be sufficient to counter general fears of data tampering by internal threats or external hackers. At the very least, something more than a list of vulnerabilities is required to show that the class members may be harmed, as the next consideration—the harm faced by Interior—weighs so heavily against granting injunctive relief.

The district court seemingly disregarded the harm an injunction would cause to Interior and those depending on Interior's services. By focusing on the need for Interior to improve its IT security, and arguing that disconnection would "help to illuminate the pervasive problems that continue to

plague Interior's IT security environment," *Cobell XVI*, 394 F. Supp. 2d at 275, the district court glossed over the immensity of the disruption that would occur to Interior's operations. The district court's order provides a process for determining which of Interior's IT systems house or provide access to trust data and would therefore be subject to disconnection. *Id.* at 278. Because we stayed the district court's order pending this appeal, *Cobell v. Norton*, No. 05-5388 (D.C. Cir. Dec. 9, 2005) (per curiam) (unpublished order), that process was not completed; we therefore cannot be certain which systems would be subject to disconnection.

Despite this lack of certainty, we do not doubt that compliance with the injunction would cause significant hardship to Interior. The district court defined IITD extremely broadly, including not only land titles and IIM account data but all records that indirectly relate to such data, as well as all past communications with beneficiaries and all other information ever used by Interior (or any other agency or contractor) "in connection with the government's [m]anagement of [i]ndividual Indian [t]rust [a]ssets." *Cobell XVI*, 394 F. Supp. 2d at 277. Defined in this way, IITD encompasses far more information than could reasonably be required to complete an accounting of the IIM trust. Based on this overbroad definition, the district court found that IITD was "pervasive . . . in virtually every Interior bureau or office." *Cobell XVI*, 394 F. Supp. 2d at 258. It is probable, therefore, that a very high percentage of Interior's IT systems would be subject to disconnection, with serious consequences.

Interior's Chief Information Officer (CIO) explained that many of Interior's functions would be hindered by the disconnection of the computers in question. For example, he stated that the Minerals Management Service relies heavily on automated systems and access to the internet in order to receive, process,

and disburse mineral revenues from federal and Indian leased lands. He stated that disconnection "will prevent or hinder MMS from being able to make timely monthly disbursements of over $500 million in mineral revenues to States, Indians, and Treasury accounts." Former Secretary of the Interior Gale Norton herself stated that Interior cannot "conduct its activities properly . . . without access to the Internet." The district court acknowledged that "compliance with the Court's order will likely . . . be difficult," *id.* at 275, yet it made no effort to address the specific ways in which its order would interfere with Interior's operations. We also cannot find any support whatsoever for the district court's belief that merely allowing Interior to reconnect its computers for five days per month would be sufficient to avoid serious harm.

Finally, we are dubious that the public interest would benefit from an injunction, despite the district court's one-sided analysis of this issue. The district court stated that the interests of "Interior's other customers . . . are best protected if Interior's IT systems are adequately secure." *Id.* at 275. However, the question of what level of security would be "adequate[]" for non-trust purposes was most decidedly not before the district court. Additionally, although "[e]very citizen of this country has an interest in seeing [the] government carry out its legal duties," *id.*, Interior's duties extend far beyond the administration of these trust accounts. Would the public interest be served more fully by allowing Interior to continue its normal operations while improving IT security, or, as the district court implies, by ordering disconnection and forcing Interior to find alternate methods of completing some tasks without network access? The district court assumed that disconnection would create a net benefit, but it failed to explain its logic in arriving at this conclusion—and in light of the far-reaching effects this order would have on Interior's operations, we are skeptical that the district court could provide such an explanation.

We therefore conclude that the district court's order cannot stand. The overbroad definition of IITD used in the order makes clear that the order was not tailored to protect the integrity of the specific data Interior will need to perform an accounting. While the class members may face some risk of harm if IITD housed on Interior's computers were compromised, we have not been shown that this possibility is likely, nor that it would substantially harm the class members' ability to receive an accounting. We are confident that the harm Interior would immediately face upon complying with the disconnection order outweighs the class members' need for an injunction. We also believe that the public interest would not be furthered by hobbling Interior's ability to use its IT systems. While the class members' entitlement to an accounting is not in doubt, the equities and harms involved in this case do not, on balance, justify requiring Interior to take such a drastic step.

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

VI

Due to the significant harm that this injunction would cause to Interior and the paucity of evidence that the class members' right to an accounting would be harmed without injunctive relief, we vacate the district court's order.

So ordered.