IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ELOUISE PEPION COBELL, et al.,

Plaintiffs-Appellees,

v.

GALE A. NORTON,
Secretary of the Interior, et al.,

Defendants-Appellants.

No. 05-5388

[Civil Action No. 96-1285 (D.D.C.)]

REPLY TO OPPOSITION TO MOTION FOR STAY PENDING APPEAL, AND OPPOSITION TO MOTION TO VACATE THIS COURT'S ADMINISTRATIVE STAY

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room, 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

INTRODUCTION AND SUMMARY

The October 20, 2005 injunction requires Interior to disconnect from the internet all computers and computer systems housing or having access to individual Indian trust data, as broadly defined in the court's order. It further requires that those computers be disconnected from Interior's internal networks ("intranet"); from each other; and from third parties such as tribes and contractors. Preliminary Injunction, § IIA.[1]

Plaintiffs quarrel with the precise impact of the injunction on Interior's ability to perform its functions and to serve its clients (including the plaintiff class), but, for obvious reasons, they cannot disguise the sweeping effect of the ruling. On the other side of the scale, plaintiffs demonstrate no imminent irreparable harm that would result from granting a stay. The connections at issue have been in place for years. In that time, security has continually improved, as both the district court and the Inspector General observed. Plaintiffs have not demonstrated that a single class member has ever been harmed as a result of any security weaknesses.

Plaintiffs nevertheless urge that the government "make[s] no attempt to demonstrate that the district court abused its discretion," and that its "failure to challenge that exercise of discretion establishes that [it has] no probability of success" on appeal. Stay Opposition at 11.

Plaintiffs apparently do not comprehend the government's motion. In the first section of our argument ("The Order Cannot Be Reconciled With Basic Principles Of Equity" (Stay Motion at 12)),

---

[1]Subject to its exception for "protect[ion] against fires or other such threats to life, property, or national security," the order requires that any "Information Technology System," which is defined to include (among other things) "any computer," that houses or provides access to individual Indian trust data must "forthwith" be disconnected as follows:

1. from the Internet;
2. from all intranet connections, including but not limited to the VPX, ESN, or any other connection to any other Interior bureau or office;
3. from all other Information Technology Systems; and
4. from any contractors, Tribes, or other third parties.

Preliminary Injunction, §§ IA, IIA, IIC.

we identified the principal respects in which the district court's order departed from fundamental equitable canons.

First, although the chief purpose of a preliminary injunction is to maintain the status quo, this preliminary injunction would extend internet disconnection well beyond those bureaus already subject to disconnection, and would require extraordinary bureau-to-bureau and computer-to-computer disconnections that have never been required even under the terms of any prior order in this case. Preliminary Injunction, § IIA.[2] Plaintiffs do not and cannot argue otherwise.

Second, a preliminary injunction may not issue unless the plaintiffs have proven " that the [alleged] harm has occurred in the past and is likely to occur again, [or] that the harm is certain to occur in the near future." Stay Motion at 13 (quoting Wisconsin Gas Co. v. FERC, 758 F.2d 669, 674 (D.C. Cir. 1985) (per curiam)). Plaintiffs do not and cannot show that any named plaintiff or any member of the plaintiff class has ever experienced injury, or that any individual Indian trust data has ever been manipulated, as a result of hacking into Interior systems by persons other than the IG team and the court's former Special Master.

Third, the preliminary injunction gives short shrift to the crucial principle that equity must take into account an injunction's adverse effect on third parties and on the public. See Stay Motion at 14. The computer networks subject to the district court's order are relied upon not only by Interior itself in serving the public, but also by a host of other persons and entities, including, among others, federal agencies and members of the plaintiff class. See id. at 14-15. Plaintiffs make no attempt to explain how the injunction's real and immediate impact on the public is outweighed by the wholly speculative harm to themselves.

---

[2]Although our appeal will challenge the court's order in its entirety, including its application to computers currently disconnected, our stay motion would only preserve the status quo as of the time of the October 20 injunction.

In short, quite apart from the other legal defects in the court's analysis, principles of equity require issuance of a stay pending an expedited appeal, and will ultimately compel vacation of the injunction on the merits.

ARGUMENT

I. FUNDAMENTAL PRINCIPLES OF EQUITY REQUIRE ISSUANCE OF A STAY PENDING APPEAL.

A. The Injunction Would Cause Grave, Immediate and Irreparable Harm to Interior's Services To the Public Including the Plaintiff Class.

Our stay motion demonstrated that the preliminary injunction would in large measure incapacitate a cabinet Department of the United States, especially insofar as Native American programs are concerned. Plaintiffs offer no plausible reason to disagree with this conclusion.

Plaintiffs repeatedly quote the district court's statement that "BIA [the Bureau of Indian Affairs] and OST [Office of Special Trustee] have been disconnected from the Internet for years, yet still manage to carry out their Indian-related missions. Solutions implemented to allow these bureaus to function without access to the Internet should be fairly easily adapted and exported to other bureaus and offices." Op. 204 (quoted in Stay Opposition at 17, 29 n.44). This casual and unexplained assessment is incorrect in every relevant respect.

First, as Interior has prominently noted in its quarterly reports filed with the district court, ongoing internet disconnections have significantly hampered the agency's ability to carry out its missions. See, e.g., Quarterly Report No. 21 (5/2/05), at 9-10 [Docket #2950]. The court was simply wrong to suggest otherwise.

Second, neither plaintiffs nor the district court grasp the fundamental point that disconnecting one component may affect the operations of another component. For example, the October 20, 2005 order would require the Minerals Management Service (MMS) to sever its internet connection. That disconnection would undermine the MMS's own, very significant Indian-related functions. In addition, however, key Indian-related tasks performed by the Bureau of Indian Affairs and the Office

of Special Trustee also rely on the Minerals Management Service connection. Severing the MMS connection would thus cripple BIA and OST as well. See Cason Decl. 6-7.

Third, plaintiffs and the district court entirely overlook the impact of the required intranet disconnection. Under the court's October 20 decree, BIA, OST, and other affected components, including various systems of MMS and Interior's National Business Center (NBC), are not simply cut off from the internet; they are cut off from each other and from every other office and bureau within the Department. Preliminary Injunction, § IIA. To make the calamity complete, these systems must also dismantle internally within each office and bureau. Thus, every BIA computer must be disconnected from every other BIA computer, every OST computer must be disconnected from every other OST computer, and so on. Ibid. As the Cason declaration makes plain: "Under the terms of the order, these components not only would be unable to access the Internet, but, in addition, they would be unable to communicate with each other. Perhaps even more destructive, individual computers within the same network, bureau, or office would be disconnected from every other individual computer, in effect leaving each affected computer as a stand-alone unit isolated from every other computer in the Department of the Interior." Cason Decl. 4 (emphasis added). Severance of these multiple, internal communications links as required by the court's order would in and of itself disable critical functions performed by BIA, OST, and other bureaus, separate and apart from the harm that would flow from any internet disconnections. See Cason Decl. 6.

In a similar vein, plaintiffs urge that the court's order would not hinder the processing and disbursement of royalty payments to Indians and others because Interior has continued to make such payments notwithstanding the fact that BIA and OST have been disconnected from the internet since 2001. Stay Opposition at 18. As Mr. Cason explains, "[t]he proper and timely processing of payments of royalties, rents, and bonuses to individual Indians and Tribes stemming from leasing activities is dependent, not only upon an MMS Internet connection, but also upon internal connections (intranet) between two other Interior bureaus: OST and BIA." Cason Decl. 6. "If the internal connection among NBC, OST, and BIA were disconnected, as required by the Preliminary

Injunction, it would not be possible to provide timely and accurate royalty, leasing, and bonus payments to individual Indians and Tribes. This is separate from and in addition to the dislocation that would flow from cutting off MMS access to the Internet." Id. at 7.

Plaintiffs are likewise mistaken in claiming that delivery of social services benefits to Indians will not be interrupted as a result of the October 20 order because they have not been interrupted under the BIA internet disconnection that has been in place since 2001. Stay Opposition at 18. As Mr. Cason explains, and as plaintiffs do not dispute, the benefit programs in question rely upon a BIA computer system (the "SSAS" system) that is subject to the preliminary injunction's intranet disconnection mandate wholly apart from any existing internet disconnection. See Cason Decl. 5. "The SSAS system, used by BIA and Tribes, contains the financial, budgetary, and statistical data used to generate checks for public assistance and maintain [each] individual's files." Ibid. Thus, "[a]bsent access to SSAS, which would be precluded under the court's order, such payments would grind to a halt." Ibid.

Plaintiffs' cryptic remarks regarding the harm to Departmental procurement, pay and personnel activities are equally wide of the mark. Stay Opposition at 18-19. As the Cason declaration makes plain, "[i]n order to function properly, core systems such as FFS [the Federal Financial System] must have an internal (Intranet) connection within Interior to Department bureaus and offices, even apart from any Internet connection." Cason Decl. 9. But "[t]he court's order severs those internal links, at least with respect to those bureaus that house or have access to [IITD], including, for example, MMS, BIA, and OST." Ibid. "The aggregate effect of destroying those links would be enormous: it would remove the Department's basic ability to sustain the integrity of its financial management operations." Ibid. As Mr. Cason reiterates, "[a]utomated systems such as FFS, FPPS, and IDEAS are absolutely critical to the ability of the Department to maintain the basic electronic infrastructure that allows it to perform such fundamental operations as financial management, payroll and personnel, and procurement. For Interior's purposes, the functioning of these systems requires that they be connected not only to the Internet, but also internally to other

Interior components and systems (Intranet)." Cason Decl. 10; see also ibid. ("The disconnection of both Internet and intranet connections would, for a significant part of the Department, result in an inability to process personnel actions in a timely or effective manner.").

The same holds true for plaintiffs' comments regarding the preliminary injunction's impact on e-mail and telephone service. Stay Opposition at 19. Referring to ongoing internet disconnections, plaintiffs note that "for years, the BIA, among others, has had no email capacity." Ibid. This assertion encompasses only external, internet-based email, and overlooks the Department's intranet-based email that has not been disturbed by previous internet disconnections. As Mr. Cason attests in his declaration, the disruption of the latter email capability imposed by the October 20 order's internal bureau-to-bureau and computer-to-computer disconnection requirements would be crippling to the Department:

> The Preliminary Injunction's requirement that the Interior Department disconnect specified Intranet connections would also prevent employees of the affected bureaus and offices from communicating with each other by e-mail. This is because e-mail communication is dependent upon access to a mail server, and for bureau-to-bureau or bureau-to-office connections, access to the Virtual Private Exchange (the "VPX"). Virtually every major organization, whether inside or out of the government, is dependent upon the ability to communicate by e-mail; the Interior Department is no exception, particularly given the geographic breadth of areas under Interior's stewardship. Wholly apart from all of its other effects, the Preliminary Injunction's disconnection order would cripple the operations of the Department by stripping affected bureaus of this vital means of internal communications.

Cason Decl. 10-11 (emphases added). And, while plaintiffs seek to quibble with the precise extent of the order's reach regarding Voice-Over-Internet-Protocol (VOIP) telephones, they do not dispute that the order covers such devices, nor do they mention much less contest that, under the order, the BIA's national help desk "would be unavailable because the help desk system employs VOIP technology." Cason Decl. 11.

Next, plaintiffs purport to take issue with our extensive showing that the preliminary injunction, by requiring widespread severing of Interior's external and internal electronic communications links, would itself undermine IT security. See Cason Decl. 11; see also id. at 12-13. Plaintiffs' sole point is that the hearing testimony, including testimony of government witnesses,

shows that a user of a stand-alone computer could, if necessary, download a "patch" from a non-Interior computer and then "upload" the update. See Stay Opposition at 19. In other words, if we understand plaintiffs correctly, an Interior employee whose computer is subject to the court's disconnection order could download needed software from a separate computer not covered by the court's order, save it on a diskette, and then load the software onto his work computer. See ibid. Under this scenario, the employee could not electronically transfer the software from his computer to any other Interior computer, because the court's order would have severed such computer-to-computer links. Preliminary Injunction, § IIA. Thus, what plaintiffs appear to be proposing is that Interior employees could individually obtain diskette copies of security updates and load them on to their computers, on an ongoing, piece-by-piece and computer-by-computer basis. The fact that plaintiffs would claim with a straight face that this kind of scheme could in any setting reflect an appropriate (and secure) way to operate a massive IT portfolio is itself extraordinary. Perhaps more fundamentally, plaintiffs simply fail to address the many other aspects of computer security that would be degraded if the court's preliminary injunction were to go into effect. See Cason Decl. 11.

Finally, plaintiffs declare that "it is illogical that accountings * * * would be impaired by the October 20 injunction," Stay Opposition at 20, and that "[n]othing in the injunction suggests, under even the most strained reading, that it would adversely impact the accounting process." Ibid. Plaintiffs do not reveal how they expect the agency to continue its ongoing accounting work without use of its computer networks. Nor do they directly confront Associate Deputy Secretary Cason's assessment that "[t]he complex task of performing the accountings for IIM beneficiaries and preparing account statements simply cannot be accomplished without use of the Department's computer systems and access to underlying data." Cason Decl. 4.

As Mr. Cason stressed, in a part of his declaration to which plaintiffs make no reference, the October 20 order provides that computers subject to the court's disconnection requirement must be disconnected not only from the internet and from each other, but also "from any contractors, Tribes, or other third parties." Preliminary Injunction, § IIA. And, "OST's access to the Trust Funds

Accounting System ('TFAS') is [an] example of third-party connectivity that would be severed by the Preliminary Injunction." Cason Decl. 4. In particular, "TFAS is the accounting and investing system that controls and enables the processing of Indian trust funds; it is hosted by SEI, a major contractor in the field of trust management and banking. The loss of access to TFAS would have a broad and devastating impact upon individual Indians and Tribes." Ibid. "Among other things, OST utilizes TFAS to make payments on behalf of beneficiaries to nursing homes, foster care facilities, automobile and mortgage financing institutions, hospitals, and schools. The disconnection of access to TFAS would have a crippling effect on OST's ability to make these and related kinds of payments, and also upon Interior's basic ability to prepare account statements for hundreds of thousands of Individual Indian Money (IIM) account holders and holders of other accounts." Id. at 5. Nothing in plaintiffs' conclusory assertions provides even the slightest basis for calling this analysis into this question.

B. A Stay Would Result In No Countervailing Harm to Plaintiffs.

Plaintiffs bear the burden of demonstrating that they have, in fact, been harmed; that recurrence of such harm is imminent; and that the harm would be irreparable.

Plaintiffs have not satisfied any of these requirements. They have not shown that a single plaintiff has ever been harmed by unauthorized hacking. Inasmuch as no plaintiff has ever experienced harm in the past, and inasmuch as Interior's security is indisputably subject to significant and continuing improvement, there is no basis for concluding that the harm that has never previously occurred is likely to occur for the first time in the near future. Finally, if hacking did occur, there is no reason to believe that its effects would be irremediable.

Plaintiffs assert that Interior's "widespread failure to implement the most basic protections, such as intrusion detection systems, audit logs and monitoring, ensures that whatever harm comes to Plaintiffs-Beneficiaries will not be detected and cannot be cured" (Stay Opposition at 24); that Interior's "IT systems lack intrusion detection systems, auditing logs, monitoring and other controls whereby unauthorized access would ever be detected" (id. at 25); and that "[t]he truth is that

Interior's IT security is so poor that Trustee-Delegates cannot detect or monitor unauthorized intrusions" (id. at 27). What these statements have in common is that none of them is supported by a record citation. In reality, Interior's systems feature a "defense in depth" (Op. 101) approach to IT security, involving multiple firewalls and routers, intrusion detection mechanisms, and security monitoring, see, e.g., McWhinney, 7/20/05 PM at 37 ("[e]ach of these entities has their own series of firewalls, network intrusion detection sensors, and routers"). Even in instances where the IG's professionals were able to exploit potential weaknesses, they "noted the presence of several kinds of security controls that [were] in keeping with the 'best practices' of the IT security community," Op. 81, and system elements "that were compromised ... exhibited a number of good security practices such as up to date security patches, security monitoring software, and strong password policies that eliminate many common vulnerabilities and reduced the impact of identified vulnerabilities," Op. 89 (quoting contractor report).

Of course, the fact that a security architecture is in place does not mean that Interior's systems are impervious to penetration. The ultimate question for the agency is whether its IT security is adequate, not whether its systems are impregnable.

It does not assist plaintiffs that, in August 2005, subsequent to the close of the district court's evidentiary hearing, MMS detected four instances of unauthorized access to one of its reporting applications. See Stay Opposition at 26. The application in question was a "portal" site (which posts reports for industry users to view), and, as the government noted in reporting the matter to the court, "there is no reason to believe that the integrity of any data has been compromised." Docket #3147 at 1 (8/25/05). Based on its external penetration testing of MMS, Interior's IG had concluded around the same time that no significant vulnerabilities were found that allowed penetration into MMS networks or unauthorized access to information. See ibid.

C. Plaintiffs' Efforts To Have This Court Disregard The Cason Declaration Are Meritless.

Plaintiffs urge that the Court should disregard the showing of harm set forth in the Cason declaration, insisting that evidence of harm should have been introduced at the hearing itself and was not.

This argument is without basis. First, if plaintiffs mean to suggest that the government did not present evidence of harm at the hearing, they are entirely incorrect. Several witnesses testified that an order destroying electronic communications would make it virtually impossible for the agency to carry out essential functions. See, e.g., Brown, 6/30/05 PM at 67-74; Ekholm, 7/8/05 AM at 11-14; Smith, 7/12/05 PM at 56-57; Haycock, 7/14/05 PM at 70-74; McWhinney, 7/21/05 PM at 4-7. Moreover, the disruption caused by an internet disconnection had already been amply set out in the record even prior to this summer's IT hearing, in the government's declarations submitted to the district court in March 2004, in connection with the request for a stay of its March 15, 2004 IT injunction. See Declaration of Interior CIO W. Hord Tipton (3/22/04); Declaration of Interior Secretary Gale A. Norton (3/22/04) [Docket #2549]; see also Op. 201 ("To be sure, Interior put on evidence of the ways in which the department's operations were disrupted by this Court's last disconnection order," and "Interior has also made much of the financial functions carried out by NBC and MMS, and the effects that a loss of Internet connectivity would have on the department's ability to service its customers, many of whom are other governmental agencies.").

It should also be noted, however, that certain significant features of the injunction could not have been addressed directly at the hearing, because they emerged for the first time in the order itself. For example, the October 20 order contains extraordinarily broad definitions of IITD and "Information Technology System" that extend well beyond any previous definitions of those terms in this case. These definitions were not proposed at any time during the presentation of evidence at the hearing and appeared, for the first time, in a proposed order submitted by plaintiffs after the government's evidence had closed. See Docket #3107 (7/28/05). Similarly, the injunction provides

that under specified conditions Interior may "reconnect" disconnected computers and computer systems for up to five business days per month. That provision likewise was never proposed prior to the close of the government's evidence. See ibid. Thus, these features of the injunction, and their substantial implications for Interior, could not have been the subject of the government's hearing testimony because they came into play only after the testimony had concluded. (The district court had also made clear that there would be no post-trial submissions of proposed findings of fact or conclusions of law.)[3]

Plaintiffs also present the declaration of Mona Infield, a BIA employee based in Albuquerque, New Mexico who has IT-related job responsibilities. Stay Opposition at 12-13. In her declaration, Ms. Infield complains that, prior to preparing his declaration in support of a stay, Mr. Cason should have spoken with her and did not. See Infield Decl., ¶4. Mr. Cason is the Associate Deputy Secretary of the Department, with offices at headquarters in Washington, D.C. Prior to signing a litigation declaration in a short time frame, Mr. Cason cannot feasibly consult with each employee nationwide who may be involved with IT-related tasks, and is under no requirement to do so. As explained in his declaration, Mr. Cason, in fulfilling his Secretarial-level trust reform responsibilities, is involved at the Departmental level with the overall development and maintenance of Interior's IT systems, and, in that capacity, coordinates with the Department's Chief Information Officer (CIO) and the CIO's for the Department's separate bureaus and offices. See Cason Decl. 1. Accordingly, with respect to BIA's systems, Mr. Cason consults with the BIA's CIO, who in turn may and does rely upon the expertise of BIA staff in the field.

---

[3]Plaintiffs' suggestion that the government cannot complain about the "5 day" provision because it was the government that suggested it borders on the absurd. See Stay Opposition at 12, 14. Plaintiffs seek to point to a provision in the agreed-upon December 17, 2001 consent order that plaintiffs portray as analogous. See ibid. The cited provision, however, contained no 5-day time limitation at all, and it was also issued in a context that involved internet but not intranet disconnections. See 12/17/01 Order at p.6.

In any event, Ms. Infield's attempt to call Mr. Cason's declaration into question fails on its own terms. Ms. Infield seeks to impugn Mr. Cason's statement that "even if some limited portion of essential services could be provided during the 5-day window, the apparent premise of this provision – that Interior's interconnected computer systems can be brought 'down' (disconnected) for substantial periods of time, and then brought 'up' (reconnected) for short periods, and then 'down' and 'up' over and over again, and still retain their functional capacity – misunderstands on the most fundamental level how such complex, integrated computer systems work." Cason Decl. 3. According to Ms. Infield, "it would be difficult for me to conclude that 'functional capacity' would be materially reduced by compliance with the Preliminary Injunction." Infield Decl., ¶7. Ms. Infield, however, focuses on a single, general sentence in the initial "Overview" section of the Cason declaration. Mr. Cason's statement is comprehensively explained and elaborated upon in a three-page substantive section of his declaration of which Ms. Infield makes no mention and with which she does not take issue. See Cason Decl. 12-14. As fully set forth in that section of the Cason declaration, which Ms. Infield does not dispute, "[c]omplex, integrated computer systems that continually process massive amounts of data in real time cannot feasibly be operated on the kind of 'up and down' basis contemplated by the court's order." Cason Decl. 13. Ms. Infield's suggestion that disconnecting and reconnecting large-scale, interconnected automated data processing systems is analogous to switching on and off a light bulb in one's home blinks reality. See Infield Decl., ¶8 ("the solution is as simple as turning on and off a light switch in a house").[4]

As a further part of their effort to discredit his 2005 declaration, plaintiffs also seek to attack Mr. Cason's trial testimony from 2003, in which Mr. Cason invoked the concept of "bulletproof[ing]" to describe ongoing efforts to improve aspects of Interior's IT security, and spoke

---

[4]In her declaration, Ms. Infield makes a number of other assertions, including assertions regarding her employment status at Interior. This stay reply is not the place to debate those statements, but we note that we by no means necessarily agree with them, and the government reserves the right to respond in the district court, as appropriate, to plaintiffs' November 8, 2005 notice calling Ms. Infield's declaration to the district court's attention.

in terms of having "driven the vulnerabilities down close to zero for our perimeter security at the Department overall." Stay Opposition at 22. This assault on Mr. Cason's 2003 testimony was a significant theme of plaintiffs' 2005 hearing presentation, see, e.g., 7/18/05 PM at 45, 54-55 (Cason), but it was not accepted by the district court. Nowhere in its 205-page opinion did the district court endorse plaintiffs' theory that Mr. Cason's prior testimony in this case (or the government's briefs citing that testimony) was in any material way false or misleading. As Mr. Cason took pains to emphasize with respect to the Department's IT security in his 2003 testimony, in a portion of the transcript that plaintiffs ignore, "It's not perfect, it will probably never be perfect, it's better now, and the direction we're headed at the moment is we feel pretty confident that our external perimeter security is reasonably good and that we're starting reviews of all the internal systems to harden them further[.]" Cason, 6/4/03 AM at 38. This testimony cannot plausibly be described as even remotely false or misleading.

Indeed, as plaintiffs essentially admit, their contentions regarding Mr. Cason's 2003 testimony ultimately center around the choice of scanning standards that are utilized to test perimeter security. See Stay Opposition at 23. Mr. Cason's 2003 testimony was made in the context of the "SANS Top 20 List," which is an accepted industry standard for critical vulnerabilities scanning of IT systems within the government and the private sector. See ibid.; see also Op. 58 (SANS Top 20 List includes "the ones that come from the FBI that have been identified as the most critical weaknesses throughout the IT world") (citation omitted). In contrast, the penetration testing conducted by the Inspector General and featured at the 2005 hearing went beyond the "SANS Top 20" vulnerabilities, as part of a larger and more comprehensive program undertaken with the encouragement of Interior's senior management to monitor and assess fuller security controls that had been placed on Interior's IT systems, see Stay Motion at 15-16. As plaintiffs' argument reflects, the choice of scanning regimens is inherent in the kind of security testing at issue here, and judgments about which scanning standards are appropriate for which purposes are an intrinsic element of any institution's self-testing program.

Finally, to the extent that plaintiffs seek to call into question Mr. Cason's declaration, we note that, in its recent, November 15, 2005 decision ruling vacating the district court's re-issued accounting injunction, this Court placed prominent reliance upon two separate declarations of Mr. Cason. One of those declarations, like Mr. Cason's declaration here, was filed directly in this Court. See Cobell v. Norton, No. 05-5068 (D.C. Cir. Nov. 15, 2005), Slip op. at 3, 5, 15.

II. THE GOVERNMENT IS HIGHLY LIKELY TO PREVAIL ON APPEAL.

As we have shown, the government is highly likely to prevail on appeal because the preliminary injunction departs from basic principles of equity. The order is also vulnerable on a host of other grounds.

A. Plaintiffs Do Not Cite A Single "Finding of Fact" That Could Justify The District Court's Disconnection Order.

Plaintiffs declare that the government "do[es] not challenge the district court's findings of fact" and thus "concedes the factual findings below." Stay Opposition at 10. See also id. at 2 (arguing that "[i]n their motion to stay, Trustee-Delegates fail to even challenge the district court's findings, much less show any to be clearly erroneous").

It is unclear what plaintiffs mean by this. As emphasized in our stay motion, and as plaintiffs do not dispute, the district court's principal "finding of fact" underlying the entire preliminary injunction was that experts retained by Interior's Inspector General's Office were able in certain respects to "hack" into some of Interior's systems. The question is not whether this fact-finding is correct; the question is its significance. As noted in our stay motion, the individual who personally conducted much of the hacking in question testified at the hearing that the kind of "penetration testing" conducted by his firm on behalf of government and private clients is generally successful about 75 percent of the time. Miles, 5/18/05 PM at 62; see also Brass, 5/9/05 PM at 85 (same).

Indeed, although plaintiffs' opposition purports to stress the district court's fact-findings, Stay Opposition at 10-11, the court conspicuously made no finding that computer security standards at Interior pose significantly greater risks than security conditions at other government agencies or

in the private sector. Plaintiffs do not claim otherwise and cite no fact-finding that could, on any plausible theory, compel affirmance of the injunction.

It is unclear what if any fact-finding could ever justify an order requiring a cabinet agency to disassemble its electronic communications networks. Plaintiffs identify no such finding here, and none exists.

B. The District Court Has Improperly Arrogated To Itself The Computer Security Responsibility For A Federal Agency.

The fundamental premise of the injunction is that the court can properly weigh the significance of computer security problems and direct the expenditure of scarce resources to deal with those problems while shutting down an array of other services. As this Court explained in vacating the district court's first structural injunction, it is not for a "supervising court, rather than the agency, to work out compliance with the broad statutory mandate," a regime that would improperly "inject[] the judge into day-to-day agency management." Cobell v. Norton, 392 F.3d 461, 472 (D.C. Cir. 2004) (quoting Norton v. Southern Utah Wilderness Alliance, 124 S. Ct. 2373, 2381 (2004)). The court's error in undertaking supervision of computer security is further highlighted by this Court's November 15, 2005 decision vacating the district court's re-issued accounting injunction. Cobell v. Norton, No. 05-5068 (D.C. Cir. Nov. 15, 2005). In vacating that injunction, this Court emphasized that the district court had "erroneously displaced Interior as the actor with primary responsibility for 'work[ing] out compliance with the broad statutory mandate.'" Slip op. 10 (citation omitted). The Court further explained that the district court had failed to accord appropriate deference to the agency in making choices that "required both subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." Ibid.

The present injunction is similarly flawed. It does not conclude that Interior's computer infrastructure is less reliable than that of other agencies or private entities housing equally or more sensitive data, or that it fails to comply with any specific, substantive requirement of federal law.

Because it identifies no objective security standard that has been violated, it also cites no standard that Interior could satisfy to ensure a right to operate its computers. Preliminary Injunction, § IIE.3.

In effect, the order concludes that security should be better, and that scarce dollars should be shifted to protect IIM accounts because of the special nature of a fiduciary duty. Indeed, to a large extent, the district court's injunction is based on the court's explicitly calling into question whether the more than $100 million that Interior has committed to IT security in recent years has been "allocated" appropriately, and on the court's related belief that it, rather than Interior, should be the ultimate arbiter of the agency's "priorities." See, e.g., Op. 189 ("Interior's relatively large financial commitment to IT security means nothing if those resources are not properly allocated."); Op. 191 ("Interior's fiduciary obligation to preserve IITD requires that IT security take a prominent position among the department's priorities."); see also Op. 182 ("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."); Op. 193 (criticizing IG's "failure to place special emphasis on scrutinizing Interior's efforts to provide adequate security for IITD housed on or accessed by Interior's IT systems," which demonstrated "a serious deficiency in Interior's overall IT security program with respect to Interior's fiduciary obligations").

With considerable understatement, the court acknowledged that compliance with its order would be "difficult," and that "[p]riorities will likely have to be shuffled, resources will likely have to be redirected[.]" Op. 203. This Court's decisions, including its most recent decision of November 15, 2005, make clear that the court has no authority to reset priorities based on its own calculus and to undertake direction of a cabinet agency's computer security.[5]

---

[5]Plaintiffs maintain that this Court's 2004 decision vacating the March 2004 IT injunction "stressed the broad authority of the district court as a court of equity in this Indian trust case," Stay (continued...)

C. Plaintiffs Mistakenly Seek To Invoke Internal Executive Branch Policies Under Which The Decision Whether To Authorize Operation Of An IT System Would Never Be Made Without Regard To Operational Needs.

Plaintiffs seek to place reliance upon guidelines promulgated by the National Institute of Standards and Technology (NIST), arguing that those guidelines "endorse[]" the kind of relief ordered here. Stay Opposition at 15-16. As noted in the district court's opinion, the cited NIST publications provide guidance to federal agencies regarding various aspects of information security. See generally Op. 13-37. They provide no basis for a court to order an executive Department to disconnect its computers from the internet or from each other. Indeed, plaintiffs embrace the proposition that it is "best practice" for an agency's CIO to retain the authority to disconnect a system if warranted by security concerns. See Stay Opposition at 16 & n.19. The district court's order openly usurps that authority.

However, even considered on its own terms, plaintiffs fundamentally misapprehend the NIST framework. Plaintiffs posit that external and internal disconnection of Interior computer systems were required because the IG had conducted successful "penetration testing" of some of those systems. But under the NIST guidelines to which plaintiffs refer, it is basic that an agency may keep a system on-line notwithstanding perceived security risks if, in the agency's judgment, there is an "important mission-related need to place the information system into operation." NIST SP 800-37, at 41 (cited at Op. 20). Plaintiffs' treatment of security as an absolute imperative that trumps all other considerations thus violates not only fundamental principles of equity (and common sense), but is also at odds with the very NIST guidelines which plaintiffs purport to invoke. Under those guidelines, an agency's determination whether to authorize operation of a system in light of inevitable security risks simply cannot be made without regard to the agency's operational needs. See ibid.

---

[5](...continued)
Opposition at 9, and in that respect is "binding" (id. at 10). This Court's November 15, 2005 ruling leaves no doubt that plaintiffs' view of the district court's role in this litigation (see id. at 8-10) is overly expansive and incorrect.

Plaintiffs give short shrift to another critical aspect of the NIST framework: "likelihood of exploitation." NIST SP 800-30 (cited at Op. 28). As NIST's guidelines also make clear, "the notion of a 'threat' is not to be confused with the likelihood of exploitation, which is a separate concept[.]" Ibid. As NIST explains, a vulnerability to an IT system may exist in the abstract, without regard to the likelihood that the vulnerability may actually be exploited. Thus, "the likelihood of exploitation is a distinct step in [the] risk assessment." Ibid. In particular, the likelihood of exploitation of a given vulnerability will be deemed low if the threat-source "lacks motivation or capability," or if controls are in place to impede the vulnerability from being exercised. Ibid. As noted in our stay motion, the district court, in assuming responsibility for IT security and ordering the immediate, sweeping disconnection of Interior computers and computer systems, disregarded entirely the issue of the "motivation or capability" (ibid.) of potential hackers other than the IG's retained professionals.

Plaintiffs cite hearing testimony suggesting that it is possible that a hacker "could be successful" in breaching Interior's computer security "with time, patience, and access to a community of other hackers." Stay Opposition at 27. Even assuming this speculation were correct in theory, it begs the question whether hackers might realistically have any interest in Interior's systems, let alone those housing or accessing IITD. It also skips over the point that a malicious hacker seeking to break into government computer files, unlike authorized personnel retained by the IG, faces the possibility of criminal sanctions for doing so. See 18 U.S.C. § 1030; see also Brass, 5/9/05 AM at 64 ("a long stay in Leavenworth"). In the end, plaintiffs offer no evidence of any kind, and the district court cited none, that any relevant "community of hackers" (Stay Opposition at 27) would be motivated to hack in to the Interior systems at issue in this case.

Plaintiffs do not advance their argument by seizing upon the suggestion in the district court's opinion that Interior's computers may be subject to "hundreds of millions" of intrusion attempts. See Stay Opposition at 28 (citing Op. 195). Any computer that is connected to the internet, even a basic home computer with a standard firewall, is subject to constant scanning from outside sources,

much of which is automatically generated. The fact that a large IT portfolio such as Interior's will over time be subject to many such "pings" says absolutely nothing, one way or the other, about the underlying nature or quality of its IT security.

CONCLUSION

For the foregoing reasons, and for the reasons stated in our stay motion, the district court's October 20, 2005 preliminary injunction should be stayed pending appeal. We also reiterate our request that the Court order expedited briefing to resolve the issues presented by the district court's order at the earliest possible time.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

KENNETH L. WAINSTEIN
United States Attorney

GREGORY G. KATSAS
Deputy Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
I. GLENN COHEN
(202) 514-5089
Attorneys, Appellate Staff
Civil Division, Room, 7531
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

NOVEMBER 2005

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of November 2005, I caused copies of the foregoing reply and opposition to be sent to the Court and to the following by hand delivery:

The Honorable Royce C. Lamberth
United States District Court
United States Courthouse
Third and Constitution Ave., N.W.
Washington, D.C. 20001

Keith M. Harper
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
(202) 785-4166

G. William Austin
Mark I. Levy
Kilpatrick Stockton
607 14th Street, N.W.
Washington, D.C. 20005
(202) 508-5800

and to the following by federal express, overnight mail:

Elliott H. Levitas
Law Office of Elliott H. Levitas
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309-4530
(404) 815-6450

and to the following by regular, first class mail:

Dennis Marc Gingold
Law Office of Dennis Marc Gingold
607 14th Street, N.W., Box 6
Washington, D.C. 20005

Earl Old Person (pro se)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417

Thomas M. Bondy
THOMAS M. BONDY