UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
Plaintiffs,	)	Civil Action No. 96-1285 (RCL)
v.	)	
GALE A. NORTON, et al.,	)	
Defendants.	)	

MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO PLAINTIFFS' MOTION FOR AN ORDER TO SHOW CAUSE WHY THE DEPARTMENT OF THE INTERIOR SECRETARY, GALE NORTON, AND HER SENIOR MANAGERS AND COUNSEL SHOULD NOT BE HELD IN CIVIL AND CRIMINAL CONTEMPT FOR VIOLATING COURT ORDERS

Plaintiffs seek findings of civil contempt and criminal contempt against Secretary of the Interior Gale Norton, Deputy Secretary Steven Griles, Associate Deputy Secretary James Cason, Chief Information Officer Hord Tipton, contractor employee Hart Rossman, and Department of Justice attorneys Robert McCallum, Jr., Peter Keisler, Stuart Schiffer, Christopher Kohn, Sandra Spooner, John Stemplewicz, Glenn Gillett, and John Warshawsky (collectively, “the Named Individuals”). Plaintiffs' motion ("IT Contempt Motion") is an unfounded and misguided attempt to criminalize the Interior Defendants' filing of quarterly status reports, compliance with the preliminary injunction dated July 28, 2003, and the process by which this Court undertakes to resolve issues related to allowing the Department of the Interior ("Interior") to reconnect, or keep connected to the internet, information technology ("IT") systems that house or allow access to individual Indian trust data ("IITD").

The preliminary injunction concerns the security of Interior's IT systems to prevent unauthorized access of IITD through the internet. The Interior Defendants, and their counsel,

have complied with each requirement set forth in the preliminary injunction.[1] Notably, the Interior Defendants have provided the Court with certifications representing that IT Systems which remain connected to the internet either contain no IITD, are secure from unauthorized access, or are essential for protection against fires or other threats to life and safety. Plaintiffs have filed their comments regarding these certifications. In addition, the Interior Defendants have filed proposed procedures setting forth a method of approving individual reconnections of IT systems that remain disconnected from the internet, and of determining whether the reconnected systems should stay reconnected. These certifications and the Interior Defendants' proposed procedures remain pending before this Court.

The Court's December 21, 1999 Order directed Defendants to file with the Court, and serve upon Plaintiffs, quarterly status reports setting forth and explaining steps taken to rectify what the Court had found to be breaches of the Defendants' trust obligations. The Interior Defendants have filed reports in compliance with this order, and the reports have discussed the status of Interior's IT systems. Contrary to Plaintiffs' assertions, these reports do not contain misrepresentations, either affirmatively or by omission, nor do they conflict with four other subsequently issued government reports upon which Plaintiffs rely.[2]

---

[1] Defendants have appealed the issuance of the preliminary injunction. A briefing schedule for the appeal has not been set. While Defendants believe that the issuance of the preliminary injunction was reversible error, they nevertheless have complied with the terms of the injunction while the matter is on appeal. The showing made in this memorandum of compliance with the terms of the injunction is not a waiver of any arguments the Defendants may wish to assert on the appeal of the injunction.

[2] Plaintiffs cite to: (1) the September 8, 2003, Department of the Interior report for OMB entitled "Financial Management Status Report and Strategic Plan (FY 2004-FY2008); (2) the September 22, 2003, OIG Annual Evaluation of the Information Security Program of the Department of the Interior; (3) the September 12, 2003, General Accounting Office report entitled "Information Technology: Department Leadership Crucial to Success of Investment

(continued...)

BACKGROUND

On November 14, 2001, the Special Master issued a Report and Recommendation Regarding the Security of Trust Data at the Department of the Interior, which identified deficiencies in the security of Interior's IT systems that the Master believed could detrimentally affect the integrity of IITD. Following the issuance of the Master's report, the Court entered a temporary restraining order on December 5, 2001 (amended December 6, 2001) that required Interior to disconnect from the internet all systems housing IITD. On December 17, 2001, the Court approved the Consent Order, which established the procedures Interior would be required to follow, under the Master's oversight, before reconnecting its systems to the internet.

With the exception of special procedures applicable to temporary reconnections for testing and the provision of certain necessary services, Consent Order at 6-7, the Consent Order generally provided that Interior could reconnect systems following notice to the Special Master if such systems (a) did not house or provide access to individual Indian trust data or (b) housed or provided access to individual Indian trust data, provided adequate security existed. Id. at 5-7. For systems housing or providing access to individual Indian trust data, the Consent Order provided, "The Special Master shall review the plan [for reconnection] and perform any inquiries he deems necessary to determine if it provides adequate security for individual Indian trust data." Id. at 7. Finally, the Consent Order provided "that the Special Master shall verify compliance with this Consent Order and may conduct interviews with Interior personnel or contractors or conduct site visits wherever information technology systems or individual Indian trust data is housed or accessed." Id.

---

[2](...continued)
Reforms at Interior; and (4) the December 9, 2003 Congressional Subcommittee report. IT Contempt Motion at 2, n.4.

Pursuant to the terms of the Consent Order, Interior, upon notice to and acquiescence of the Special Master, reconnected to the internet IT systems which did not house or did not provide access to IITD.[3] Interior also reconnected to the internet several systems which did house or provide access to IITD in accordance with the provisions of the Consent Order. The reconnected systems housing or providing access to IITD included the Minerals Management Service ("MMS"), the Office of the Inspector General ("OIG"), the Bureau of Land Management ("BLM") and the National Business Center ("NBC") (collectively, the "Reconnected Systems"). Other systems housing or providing access to IITD, including the Bureau of Indian Affairs ("BIA") and the Office of Special Trustee, remained offline.[4]

A dispute developed between Interior and the Special Master concerning the implementation and operation of a proposal negotiated to accommodate the Special Master's plan to conduct "penetration" and "exploitation" testing of systems reconnected pursuant to the terms of the Consent Order. The Interior Defendants took the position that the Consent Order did not authorize penetration testing, and, in any event, penetration testing without the consent of

---

[3] The Fourteenth Quarterly Report noted that "[a]fter approximately 18 months of reviewing Interior's IT systems to identify where IITD is housed, it has become apparent that a relatively small part of Interior's combined IT systems house IITD." IT Contempt Motion, Exhibit 4 at 11. Plaintiffs do not challenge this statement. Plaintiffs also have not challenged the statements in the Eleventh Quarterly Report that only six per cent of Interior's IT Systems contain IITD data, and most of those systems are not connected to the internet. IT Contempt Motion, Exhibit 1 at 8.

[4] The Bureau of Reclamation and the Bureau of Fish and Wildlife found limited amounts of IITD on their systems. The IITD were isolated onto physically secure computers not connected to the internet or to the bureaus' networks. The Special Master was apprized of this arrangement. Because the IITD found at the Bureau of Reclamation and the Fish and Wildlife Service remained offline, these bureaus filed certifications with the Court pursuant to the preliminary injunction stating that their systems have no IITD.

Interior would violate 18 U.S.C. § 1030. Consequently, the Interior Defendants drafted and proposed to the Special Master "Rules of Engagement" to govern penetration testing.

When the draft "Rules of Engagement" process broke down, Plaintiffs moved for a temporary restraining order. The Court granted the temporary restraining order on June 27, 2003. The order directed Interior Defendants immediately to disconnect from the internet all IT systems which housed or provided access to IITD until the Special Master determined that all IITD was properly secured, and disconnect from the internet all computers that housed or provided access to IIM trust data until the Special Master determined that IITD was properly secured.[5]

On July 28, 2003, the Court replaced the temporary restraining order with the preliminary injunction, which provided, in substantive part:

> 1. The Interior defendants shall immediately disconnect from the Internet all Information Technology Systems within the custody or control of the U.S. Department of the Interior, and its employees, agents, and contractors, that House or Access Individual Indian Trust Data, until such time as the Court approves their reconnection to the Internet, with the following two exceptions:
>
> (a) Immediate disconnection shall not be required for each specifically identified Information Technology System and computer that the Interior defendants certify, within ten (10) days of the date of entry of this Order, to be essential for protection against fires or other threats to life or property, and provide a specific justification in support thereof, in accordance with Rule 11 of the Federal Rules of Civil Procedure.
>
> (b) Immediate disconnection shall not be required for each specifically identified Reconnected System that the Interior defendants certify, within fifteen (15) days of the date of entry of this Order, and in accordance with Rule 11 of the Federal Rules of Civil Procedure, that the Interior Department currently believes either (1) does not House or Access to Individual Indian Trust Data, and provide a specific justification thereof, or (2) is secure from Internet access

[5] The order exempted systems essential for protection against fire and other threats to life or property.

by unauthorized users, and provide a specific justification in support thereof, stating in specific terms the security measures that are presently in place to protect unauthorized Internet access to the Individual Indian Trust Data that the Information Technology System Houses or provides Access to.

2. Within thirty (30) days of the date of entry of this Order, plaintiffs may file with the Court their response to the representations made in the certifications described in section B.1(b).

3. Within thirty (30) days of the date of entry of this Order, the Interior defendants shall file with the Court a proposal setting forth a method of approving individual reconnections of disconnected Interior computer systems, and of determining whether the Reconnected Systems should stay reconnected. The proposal should demonstrate a method of providing to the Court adequate evidence that the Reconnected Systems and the Information Technology Systems disconnected pursuant to this Order are secure against Internet access by unauthorized users, and provide a means to verify the representation that the Reconnected Systems and the Information Technology Systems disconnected pursuant to this Order are secure against Internet access by unauthorized users.

4. Within ten (10) days thereafter, plaintiffs may comment on the Interior defendants' proposed procedures.

5. The Court will decide on the record before it whether a Reconnected System shall remain connected to the Internet, and will decide all future applications for reconnection.

The Court also stayed the December 17, 2001 Consent Order.

Interior Defendants filed the submissions required by paragraphs 1(a) and 1(b) regarding systems which Interior Defendants believed were essential for protection against fire or other threats to life or property, or systems which did not house or provide access to IITD or which were secure from Internet access by unauthorized users on August 11, 2003. In accordance with paragraph 3 of the preliminary injunction, Interior Defendants filed a proposal setting forth a method of approving individual reconnections of disconnected Interior computer systems, and of determining whether the Reconnected Systems should stay reconnected. Plaintiffs filed

responses to the Interior Defendants' submissions within the times set forth in paragraphs 2 and 4 of the preliminary injunction.

ARGUMENT

I. Plaintiffs Misunderstand and Misrepresent the Four Reports on which Their Motion Relies

Plaintiffs' motion for an order to show cause is based on four government reports which Plaintiffs wrongly interpret as contradicting statements made by the Interior Defendants in quarterly status reports or as undermining the certifications filed in accordance with the preliminary injunction. None of these four government reports addresses directly the very specific issue of whether the MMS, BLM, OIG and NBC IT systems, the reconnected IT systems that house or access IITD, are secure from internet access by unauthorized users. Rather, each of these reports addresses in general terms the broader issues of IT systems and security throughout Interior, including systems that do not house or access IITD.

Although these four government reports are inapplicable, Plaintiffs selectively misread and misapply language contained in the reports as somehow rendering the statements made in the quarterly status reports and the certifications untruthful. Plaintiffs' failure to provide a factual basis for their incrimination is fatal to their attack. Moreover, Plaintiffs' request for an order to show cause why the Named Individuals should be held in civil and criminal contempt is without legal support. Plaintiffs' motion should be summarily denied.

A. The Financial Management Status Report

The Financial Management Status report (the "FMS Report") reported on Interior's financial management accomplishments for FY2003, its adherence to the requirements of the Federal Financial Management Improvement Act, and its plan for FY2004. The FMS Report did

not concern the risk of internet access by unauthorized users to systems housing or having access to IITD.

Plaintiffs assert that the FMS Report supports the conclusion that Interior and Department of Justice counsel have "covered-up debilitating weaknesses in IT Systems that they reconnected - or left connected - to the Internet." IT Contempt Motion at 3. Plaintiffs base their claim upon a paragraph in the report that stated:

> [i]n some instances, the Department has not established access controls that limit or detect inappropriate access to information technology systems and related resources, thereby increasing the risk of unauthorized modification, loss, or disclosure of sensitive or confidential data.

FMS Report at 31. Plaintiffs presumably infer "some instances" to refer to systems housing or accessing IITD. The paragraph cited by Plaintiffs does not support their inference nor their broad charge that there are "debilitating weaknesses" in the Reconnected Systems.

Plaintiffs rely upon the same faulty inference when they cite the following text:

> Key departmental financial management systems that are critical to the sound management of Interior's diverse, geographically diffuse operations and programs are in urgent need of replacement. Many systems in Interior's eight major bureaus are not integrated, which makes it difficult to maintain the quality of financial information. The systems do not have the necessary security capabilities to facilitate more open access via the Internet.

IT Contempt Motion at 14-15 (citing FMS Report at 5) (underlining added showing language omitted by Plaintiffs). Again, there is no basis for assuming that this text refers to the MMS, BLM, OIG and/or NBC IT systems. Indeed, the implication of this text is that Interior is being prudent in not connecting the old financial management programs via the internet because of security concerns and will adopt a new more robust program in FY 2004 - Financial and Business Management System (FBMS) - to permit the greater access. See FMS Report at 5.

Next, Plaintiffs cite comments in the FMS Report that acknowledged that Interior continues to address the challenges of resolving FMFIA (Federal Managers Financial Integrity Act) material weaknesses, including "challenges in managing Indian Trust Funds and inadequate computer security." IT Contempt Motion at 15.[6] None of the material quoted by the Plaintiffs from the FMS Report implicated the Reconnected Systems or contradicted the quarterly reports or the PI certifications regarding whether the MMS, BLM, OIG and NBC IT systems are secure from internet access by unauthorized users.

Interior recognized, in the FMS Report, that its financial management programs needed to improve and critically pointed out to OMB the areas of weakness and the plans for remediation.[7] However, nowhere in the FMS Report did Interior state that the IITD on the MMS, BLM, OIG and NBC IT systems was not secure from internet access by unauthorized users.[8] Nor is the omission of such conclusions unexpected because the purpose of the report is financial management, not IT security, and because such a statement would not be accurate.

---

[6] Plaintiffs also cite material from the FY 2002 Audited Financial Statements Material Weaknesses Remediation Status Report (FMS Report at 24, Exhibit 3-2) that "Inadequate Controls Over Trust Funds" was a material weakness carried over from the FY 2001 audit and has a target resolution date of September 30, 2005. Similarly, the Plaintiffs cite material from a chart listing FMFIA Material Weaknesses as of September 30, 2002 (FMS Report at 33, Exhibit 3-4). However, the material cited, see IT Contempt Motion at 15, simply restated the obvious - the increasing growth in electronic commerce and the growing vulnerabilities of information systems to unauthorized access demands comprehensive improvement in IT security.

[7] Exhibit 3-1 of the FMS Report showed that MMS and BLM received "unqualified audit opinions" for at least the last four fiscal years (FY1999 to FY2002). FMS Report at 22.

[8] The FMS Report did report on the "Computer Security Improvement Project" but did not directly address the security of any particular IT system from internet access by unauthorized users. FMS Report at 65-68.

B. The GAO Investment Report

The GAO report, entitled "Information Technology: Departmental Leadership Crucial to Success of Investment Reforms at Interior" (the "GAO Investment Report"), was issued on September 12, 2003, and is available to the public on the GAO website.[9] As the title of the report states, this report focused not on IT security at Interior but rather on the effective management of the investment of government funds on information technology and the need for effective leadership. The GAO was asked to evaluate (1) Interior's capabilities for managing the agency's IT investments and (2) Interior's actions and plans to improve these capabilities. GAO September 12, 2003, letter to The Honorable Charles H. Taylor, Chairman, Subcommittee on Interior and Related Agencies, Committee on Appropriations, House of Representatives, GAO Investment Report at 1. The GAO Investment Report concluded that Interior had limited capability to manage its IT investments. Id.

The Plaintiffs quote liberally from the GAO Investment Report, IT Contempt Motion at 19-21, yet even a cursory review of those quotes reveal that the GAO Investment Report focused on Interior's management of its IT investments. Plaintiffs have unjustifiably leapt from the actual text and stated purpose of the report to the conclusion that Interior's shortcomings in ensuring that its "mix of IT investments best meets the agency's mission and business priorities GAO

---

[9] Plaintiffs assert that the Interior Defendants suppressed the publicly available GAO Investment Report and that Secretary Norton "**concurred unequivocally** in the concealed draft" GAO findings, but "**insisted** that the GAO 'remove[] **all** description of . . . [the] Trust." IT Contempt Motion at 18 (emphasis in original). The genesis of this false assertion is the request from the Office of the Associate Deputy Secretary dated August 27, 2003, that "Interior requests deletion in the final report of any description of national critical infrastructure or Trust systems, as this could potentially cause security concerns." GAO Investment Report at 45. Her expressed concerns for security were certainly appropriate.

Investment Report at 36" impact the security of IITD. Id. at 20-21. The Plaintiffs' conclusion that the GAO investment management report is evidence that the Reconnected Systems are at risk for internet access by unauthorized users simply has no logical or factual basis.

C. The Scorecard

Plaintiffs cite to what they incorrectly call "Interior's self-appraised 'scorecard'" as evidence that Interior's IT security is poor. IT Contempt Motion at 12. Plaintiffs actually are relying upon a computer security grade assigned by Congress and reported in the December 9, 2003 Congressional Subcommittee report ("the Scorecard"). The computer security grades assigned to each agency were based on information contained in agencies' and Inspectors General's Federal Information Security Management Act reports to OMB for fiscal year 2003. Scorecard, Attachment "How Grades Were Assigned" at 1. The Subcommittee analyzed the agency and IG responses and derived a numerical score. Scorecard, Attachment "How Grades Were Assigned" at 2. Plaintiffs attempt to compare the numerical score of 43 derived by the Subcommittee for Interior with Interior's IT security performance measurement of 81.9% for BIA in September 2003. IT Contempt Motion at 13.

Plaintiffs' comparison, and argument based thereon, are unsupported because they are based upon the incorrect assumption that the two scores are based upon the same criteria. They are not. The Subcommittee's method of deriving the numerical scores is described at Attachment 1 of the Subcommittee's report; Interior's method of measuring IT security performance is described in its September 17, 2003 FISMA report at 3. Appendix B of the FISMA report shows Interior's overall score as of August 31, 2003 as 69.7%.

D. The OIG Annual Evaluation

Plaintiffs contend that Interior suppressed information that IITD are in "imminent risk." IT Contempt Motion at 26-30. Plaintiffs cite to the Office of Inspector General Annual Evaluation of the Information Security Program of the Department of the Interior (the "OIG Report") as support for their claim. Plaintiffs' argument reflects a misunderstanding of the report.

The OIG Report is required by the Federal Information Security Management Act of 2002 ("FISMA"), which pertains to information and information systems security in general – it is not limited to protecting information systems from Internet access by unauthorized users. The OIG Report was based upon an analysis of various reviews and reports as identified in Appendix 1 of the OIG Report. In addition, the OIG tested information system security controls at U.S. Geological Survey (GS), National Park Service (NPS), Bureau of Reclamation (BOR), and DOI Web sites. OIG Report at 1-2. Most of the subjects addressed in the portion of the OIG Report quoted by Plaintiffs, see IT Contempt Motion at 28-30, pertained to bureaus that do not house or provide access to IITD. OIG Report at 1-2.

Plaintiffs also rely upon the OIG Report to argue that "IT Systems are no more secure than they had been two-and-one-half years ago." IT Contempt Motion at 30-31. Plaintiffs' argument has absolutely no factual support. The cover letter from the Department of the Interior's Inspector General to the Secretary of the Interior states:

> We found that the Department continues to make significant progress to improve the security over its information systems. However, its overall security program does not yet adequately protect all information systems supporting the operations and assets of the Department and therefore remains a material weakness.

Letter from Mr. Earl R. Devaney, Inspector General to Secretary Gale Norton, dated September 22, 2003 (included in the OIG Report filed with the Court). The OIG "found that [Interior]

continues to improve the security of its information and information systems," OIG Report at 2, and stated that "[i]mprovements in information security related to Indian trust information and systems were also made." Id. at 11. The OIG Report, in the "Evaluation Results" section, concludes that "[d]uring the past 2 years much has been accomplished and the list of tasks remaining to be completed has become shorter." Id. The IG concluded that "until bureaus and offices fully implement security policies and procedures, effectively assess risks, and fully integrate corrective action plans with the capital planning and investment control process, [Interior] should continue to report to the Congress the lack of an adequate information security program as a material weakness. Id. at 2-3. The improvement in IT security is documented by the testing, evaluation and reporting on IT systems by the Special Master's experts from January 2002 until June 2003.

Thus, Plaintiffs' assertion, see IT Contempt Motion at 31, that all competent evidence supports their view that IT security is worse than in 2001 fails for three reasons. First, they have cited no competent objective evidence that the MMS, BLM, OIG and NBC IT systems are not secure from internet access by unauthorized users. Second, the results of testing, scanning and system improvements and upgrades, as described in the PI certifications that are properly attested to under applicable rules, demonstrate conclusively that the IT systems housing or accessing IITD are more secure than in 2001 and adequately protect that data from internet access by unauthorized users. Finally, the independent judgment of the Inspector General is that IT security is better.

5. The FISMA Report

While not included in its list of reports that supports their claims for contempt, Plaintiffs assert that Interior's Report on the Implementation of the Federal Information Security Management Act : FY2003 ("the FISMA Report) is "false and materially misleading." IT Contempt at 27. Plaintiffs assert that the report omits "materially adverse information"[10] including "explicit concerns raised by both the GAO and the Inspector General" regarding the department's ability to manage and secure Interior's IT systems (id. at 26). The FISMA Report is focused on a different subject area than the IT investment management report from the GAO. The OIG Report was submitted to Congress as an appendix to the FISMA Report.[11] Plaintiffs cite no specific examples of false statements in the FISMA Report. Further, they cite no examples of conflicts between the PI certifications and the statements made in the FISMA Report.

II. There is No Factual Basis for a Show Cause Motion.

As this Court has noted, "the 'extraordinary nature' of the remedy of civil contempt leads courts to 'impose it with caution.'" *SEC v. Life Partners, Inc.*, 912 F. Supp. 4, 11 (D.D.C. 1996) (quoting *Joshi v. Professional Health Services, Inc.*, 817 F.2d 877, 879 n.2 (D.C. Cir. 1987)).

---

[10] The FISMA report does not omit all materially adverse material. For instance, on pages 18 and 19, the report lists the number of material weakness for FY2003, the number carried over from FY2002 and identifies and describes the material weakness.

[11] Plaintiffs also assert that the FISMA Report attacked the Court. This assertion is not correct. The comment states "Although we believe adequate defenses are in place in other Trust organizations, namely the Bureau of Indian Affairs (BIA), Office of the Special Trustee (OST), Solicitor (SOL), and the Office of Hearing and Appeals (OHA), remain offline to comply with the applicable court orders. This continues to cause tremendous hardship on these offices as it greatly inhibits their ability to efficiently serves their customers and adds costs and unnecessary risks to maintaining sound security." FISMA Report at 7.

The party seeking a contempt finding bears the burden of establishing its claim by the heightened clear and convincing evidence standard. *SEC v. Bilzerian*, 112 F. Supp. 2d 12, 16 (D.D.C. 2000); *Petties v. District of Columbia*, 897 F. Supp. 626, 629 (D.D.C. 1995). Further, in light of the severity of the contempt sanction, it should not be resorted to "if there are any grounds for doubt as to the wrongfulness of the defendants' conduct." *Life Partners*, 912 F. Supp. at 11 (citing *MAC Corp. v. Williams Patent Crusher & Pulverizer Co.*, 767 F.2d 882, 885 (Fed. Cir. 1985)). Plaintiffs have fallen far short of meeting these standards.

Standards for civil contempt have been set forth repeatedly in the contempt hearings in this case, *Cobell v. Babbitt*, 37 F. Supp. 2d 6 (D.D.C. 1999) ("*Cobell I*"), and *Cobell v. Norton*, 226 F. Supp.2d 1 (D.D.C. 2002) ("*Cobell II*"), and the elements have been described by controlling authority in other cases in this circuit. The Court of Appeals held in *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1289 (D.C. Cir. 1993):

> "There can be no question that courts have inherent power to enforce compliance with their lawful orders through civil contempt." *Shillitani v. United States*, 384 U.S. 364, 370 (1966). Nevertheless, "civil contempt will lie only if the putative contemnor has violated an order that is clear and unambiguous," *Project B.A.S.I.C. v. Kemp,* 947 F.2d 11, 16 (1st Cir. 1991), and the violation must be proved by "clear and convincing" evidence. *Washington-Baltimore Newspaper Guild, Local 35, v. Washington Post Co.*, 626 F.2d 1029, 1031 (D.C. Cir. 1980).

Plaintiffs' Motion fails as a matter of law unless it identifies actions by the Named Individuals that can be shown to have violated a "clear and unambiguous" court order. As explained in *Project B.A.S.I.C.*:

> A court order, then, must not only be specific about what is to be done or avoided, but can only compel action from those who have adequate notice that they are within the order's ambit. For a party

> to be held in contempt, it must have violated a clear and unambiguous order that left no reasonable doubt as to what behavior was expected and who was expected to behave in the indicated fashion. "In determining specificity, the party enjoined must be able to ascertain from the four corners of the order precisely what acts are forbidden."

947 F.2d at 17 (internal citation omitted). Thus, a party seeking a finding of civil contempt must initially show, by clear and convincing evidence, that (1) a court order was in effect, (2) the order clearly and unambiguously required certain conduct by the respondent, and (3) the respondent failed to comply with the court's order. *SEC v. Bilzerian*, 112 F. Supp. 2d 12, 16 (D.D.C. 2000); *Petties v. District of Columbia*, 897 F. Supp. 626, 629 (D.D.C. 1995).

Plaintiffs request findings of civil and criminal contempt for violations of orders issued in this case. Plaintiffs discuss three orders: (1) the temporary restraining order issued June 27, 2003; (2) the preliminary injunction entered July 28, 2003; and (3) the order of December 21, 1999, insofar as it required Defendants to file quarterly reports. None of these orders have been violated.[12]

---

[12] While Plaintiffs briefly discuss the consent order issued December 17, 2001, IT Contempt Motion at 8, Plaintiffs do not contend in their motion that anyone should be held in contempt for alleged violation of the Consent Order. While the Consent Order was in effect, Defendants reconnected systems to the internet only upon advance notification to the Special Master and upon providing documentation required by the Consent Order to the Special Master. Plaintiffs do not contend that Defendants reconnected any system to the internet to which the Special Master objected. Plaintiffs do not take issue with documentation submitted by Defendants in support of the reconnection of any system under the Consent Order. Moreover, the Court found, in the Memorandum Opinion supporting issuance of the preliminary injunction, that "[p]laintiffs have not demonstrated to the satisfaction of the Court that the reconnected systems are not presently secure from unauthorized Internet access." *Cobell v. Norton*, 274 F. Supp. 2d 111, 132 (D.D.C. 2003) (emphasis in original).

A. The Temporary Restraining Order and the Preliminary Injunction

1. Defendants Have Complied with the Preliminary Injunction and the TRO.

The preliminary injunction required the Interior Defendants to disconnect IT systems from the internet, with two exceptions. First, Defendants were not required to disconnect systems and computers which the Defendants certified within 10 days of entry of the order to be essential for protection against fires or other threats to life or property. Preliminary Injunction, ¶ 1(a). Second, Defendants were not required to disconnect from the internet IT systems which Defendants certified that Interior currently believed either (1) did not house or provide access to IITD, or (2) were secure from internet access by unauthorized users. Preliminary Injunction, ¶ 1(b).

Defendants fully complied with the preliminary injunction, provided extensive certifications for systems and computers which Interior believed should be connected to the internet, and provided extensive and substantial evidentiary justifications for each certification.

Paragraph 3 of the preliminary injunction required Interior Defendants to file within 30 days a proposal setting forth a method of approving individual reconnections of disconnected Interior computer systems, and of determining whether the Reconnected Systems should stay reconnected. Defendants also complied with this provision of the preliminary injunction. However, the Court has not ruled upon the proposed method of approving reconnections of systems currently disconnected from the internet. Therefore, since issuance of the preliminary injunction, the Interior Defendants have not connected any system to the internet which had not been connected during the period that the Consent Order was in effect. Consequently, since entry

of the Consent Order on December 17, 2001, the only Interior IT systems connected to the internet at any time have been systems which do not house or do not provide access to IITD, or systems housing or providing access to IITD which Interior has documented are secure from unauthorized internet access. All other systems housing or providing access to IITD have remained offline.

2. The Attestations Comply with Legal Requirements

Plaintiffs quibble with the form of the certifications submitted in compliance with paragraphs 1(a) and 1(b) of the preliminary injunction. IT Contempt Motion at 32.[13] Plaintiffs contend that all of the certifications are incompetent because the attestations for the certifications, "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information and belief" is not identical to the language which, Plaintiffs assert, "[b]oth 28 U.S.C. § 1746 and LCvR 5.1(h) require explicitly that all *jurats* for unsworn declarations contain." IT Contempt Motion at 32.

This argument, which Plaintiffs have made without success throughout this litigation, is not supported by the explicit language of the local rule and the statute. Both the rule and the statute provide that a certification meets the requirements if it is substantially in the form of the language quoted in Plaintiffs' motion. A declaration or certification "to the best of" the declarant's knowledge is sufficient under the local rule, the statute, and the more stringent requirements of Federal Rules of Civil Procedure 56(e). See *United States v. Roberts*, 308 F.3d

[13] Plaintiffs also assert in passing that Defendants were required to submit certifications before reconnecting IT systems to the internet. IT Contempt Motion at 32. This contention is inconsistent with the clear and unambiguous language of paragraph 1 of the preliminary injunction.

1147, 1155 (11th Cir. 2002), *cert. denied*, 123 S. Ct. 2232 (2003) (holding that a false statement attested to as "correct and true to the best of my knowledge and belief" was substantially in the form provided by § 1746)); *Colon v. Coughlin*, 58 F.3d 865, 872 (2d Cir. 1995) (reversing summary judgment against plaintiff because the verified complaint "attesting under the penalty of perjury that the statements in the complaint were true to the best of his knowledge" was sufficient under Rule 56(e) assuming that the other requirements of the rule are met); *Williams v. Sielaff*, 914 F.2d 250 (4th Cir. 1990) (unpublished table decision) (reversing summary judgment because declaration "made under penalty of perjury and that it was true and correct to the best of his knowledge" was sufficient under Rule 56(e) and 28 U.S.C. § 1746 to qualify as an affidavit). Moreover, even if Plaintiffs' contention had any merit, which it does not, the proper remedy is a motion to strike the certifications. Plaintiffs apparent contention that thirteen people should be convicted of a crime over the form of the certifications is ludicrous.

3. The Rossman Declaration is Not False

Plaintiffs attack the declaration submitted by Hart Rossman which was included among the justifications for the certifications. Plaintiffs' attack on the Rossman declaration is wholly unsupported by the facts. Without quotes taken out of context and assumptions that are without factual basis, there could be no attack at all. Plaintiffs focus on two straightforward, factually based, unassailable paragraphs that conclude Mr. Rossman's declaration. Plaintiffs attack paragraph 8 of Mr. Rossman's affidavit by intentionally omitting critical language and contorting the remaining language into a broad statement of legal compliance, which it is not.

Paragraph 8 provides, in its entirety, as follows:

> Interior, consistent with existing Federal guidance, has directed the Bureau heads and CIOs, **through policy and memorandum,** to use risk management methodologies that conform with NIST guidance to determine the threat to Interior information technology systems, the vulnerability of those systems to identified threats, and the subsequent impact of harm to those systems. **These assessments are used in determining the appropriate level of security to apply to their systems.**

(Rossman Declaration at ¶ 8, emphasis added showing language omitted by the Plaintiffs). Plaintiffs ignore the plain meaning of the first sentence of this paragraph, which states nothing more than that Interior directed Bureau heads through policy and memorandum. Leaving out "through policy and memorandum," Plaintiffs applied their own twisted and self-serving interpretation that Mr. Rossman was in some way representing that Interior was in compliance "with existing Federal guidelines," a phrase that does not even appear in Mr. Rossman's declaration, or with "IT industry best practices." Mr. Rossman said nothing of the sort. There is simply no evidence that the statements made by Mr. Rossman in paragraph 8 are not true.

Plaintiffs also attack paragraph 9 of Mr. Rossman's declaration, [14] which reads:

> Interior, consistent with the guidance laid forth by the OMB **M-**02-09 and IT industry best practices as set forth by the SANS (SysAdmin, Audit, Network, Security) Institute, have instituted a Department-wide program to assess the technical vulnerability of IT systems facing the Internet. **This is done by scanning their Internet perimeter monthly against a superset of the SANS/FBI "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus" list, a list of the 20 major categories of vulnerabilities. The scan results are produced and distributed monthly to stakeholders and they are responsible for the remediation and mitigation of identified vulnerabilities. This process, to date, has reduced the overall presence of Interior's Internet visible IT systems and** reduced significantly the number of vulnerable hosts.

---

[14] Plaintiffs appear to cite to the last sentence of this paragraph 9 as paragraph 10. Mr. Rossman's declaration contains 9 numbered paragraphs and the language cited by the Plaintiffs as appearing in paragraph 10 actually appears in paragraph 9.

(Rossman Declaration at ¶ 9, emphasis added showing language omitted by the Plaintiffs). By highlighting "consistent with the guidance laid forth by the OMB **M-**02-09 and IT industry best practices," and reading this phrase in the context of the arguments made by the Plaintiffs, it appears Plaintiffs again misinterpret Mr. Rossman's statements in paragraph 9 as some sort of broad representation regarding Interior's entire IT System being in compliance "with existing Federal guidelines," or "IT industry best practices." Such an interpretation is unsupported by the context and plain language of paragraph 9 in which Mr. Rossman simply represents that Interior's act of instituting "a Department-wide program to assess the technical vulnerability of IT systems facing the internet" was itself "consistent with the guidance laid forth by the OMB **M-**02-09 and IT industry best practices." Again, there is simply no evidence that this is not a true and accurate statement.

Finally, Plaintiffs' suggestion that paragraph 9 somehow constitutes a representation that "security was adequate" is also misplaced. Plaintiffs reach this interpretation by improperly isolating the last 7 words of the paragraph: "reduced significantly the number of vulnerable hosts." Alone, these words cannot be ascribed the meaning assigned by the Plaintiffs. Reading these words in the context of the rest of paragraph 9, however, shows a very specific factual assertion for which there is no contradictory evidence.

Mr. Rossman's declaration is not false because it does not purport to make the representations imagined by the Plaintiffs. Moreover, Plaintiffs' attack against Mr. Rossman is based on the unsupported and incorrect assumption that Mr. Rossman either conducted or participated in the 2002 department-wide review that was referenced in the GAO Investment

Report cited by Plaintiffs. The fact is Mr. Rossman was not involved in the 2002 department-wide review which was conducted by a completely separate group within SAIC, nor is there any evidence that Mr. Rossman was aware of the results of that review or of the discussion cited in the GAO Investment Report. Troubling is the fact that Plaintiffs boldly misrepresent Mr. Rossman's involvement in the 2002 department-wide review while wholly failing to present or even suggest any evidence to support their wild but serious allegations as to either Mr. Rossman's involvement in this review process or what Mr. Rossman knew at the time he submitted his declaration in August 2003.

Moreover, the findings by persons other than Mr. Rossman do not provide the contradictory facts that would make even Plaintiffs' strained interpretation of Mr. Rossman's declaration false. First, the review and report predate Mr. Rossman's declaration by over a year. There is no evidence whatsoever that any shortcomings expressed in the report existed or were known to Mr. Rossman in August 2003. Second, as is the case with the four government reports that spurred the filing of Plaintiffs' motion, the matters addressed in the GAO Investment Report do not address the very specific representations made by Mr. Rossman in his declaration. The portion of the GAO Investment Report quoted by the Plaintiffs discusses Interior's lines of authority and control of resources and was not specific to any particular bureaus. There is simply nothing in the language quoted by the Plaintiffs to support an argument that the very specific statements of fact set forth in Mr. Rossman's declaration regarding the narrow issues discussed in that declaration were in any way inaccurate, or worse, false.

4. Defendants Complied with the Preliminary Injunction in Regard to Contractor Operated IT Systems.

Plaintiffs contend that Defendants violated the TRO and the preliminary injunction in regard to contractor-operated IT systems. Plaintiffs assert that Interior Defendants have "presented **no** evidence that the connected contractor IT Systems are secure." IT Contempt Motion at 36 (emphasis in original). Relying on what they claim are statements in the OIG Report, Plaintiffs assert that Secretary Norton "and her senior managers admit that they do not know the status of IT Systems operated by contractors, including Tribes," id. at 37; and that Secretary Norton "and her senior managers admit that the contracts let to such contractors are inadequate to insure the security of Trust Data and Trust Assets." Id. Plaintiffs assert that the "malfeasance and bad faith of Norton and her senior managers and counsel here are palpable." Id. at 37-38.

If anyone has acted in bad faith on the issue of contracted IT systems, it is the Plaintiffs. First, the certifications did discuss contractor-operated systems when those systems housed or accessed IITD.[15] Consequently, the charge that the Interior Defendants presented no evidence concerning the security of contractor-operated systems is patently false.

Second, the contention that Interior Defendants did not know the status of contractor-operated systems connected to the internet is nonsense. The certifications themselves discuss the status of contractor-operated systems. Moreover, each contractor-operated IT system that contained IITD and that was connected to the internet under the preliminary injunction had been

[15] For example, the MMS certification provides seventeen pages detailing the security controls in place at each contractor site. MMS Certification at 59-76.

connected under the Consent Order, with the participation of the Special Master, after the Interior Defendants had provided documentation concerning the system.

Third, Plaintiffs argument relies upon a misquotation of the OIG Report which could hardly be inadvertent. According to Plaintiffs, the OIG Report at 18 states:

> DOI has been focusing on security [sic] DOI-operated systems **not those operated or maintained by contractors [including Tribes]** and other agencies.

IT Contempt Motion at 37 (emphasis in original). The term "[including Tribes]" is not part of the OIG Report - it is a misrepresentation by Plaintiffs. See IT Contempt Motion, Exhibit 6, Appendix 2 at 18. In any event, the TRO and the preliminary injunction do not on their face apply to IT systems operated by Tribes. The TRO and the preliminary injunction cover IT systems "within the custody and control" of Interior, including systems operated by other entities ("employees, agents and contractors") over whom Interior can exercise direct control. Native American tribes, as sovereigns, are not in that category. Congress has limited the direct control Interior can exercise over Native American Tribes, even when they are acting in accordance with a compact or agreement with the Department.[16] Therefore, the TRO and the preliminary injunction do not apply to the Tribes, at least not "clearly and unambiguously," and therefore the status of any Tribal IT systems cannot be a basis for civil or criminal contempt. If Plaintiffs really want to deprive one or more Tribes of internet access, Plaintiffs should file an appropriate motion, directed to the Tribes.

---

[16] The Department is authorized to create contracts and compacts with Tribes under the Indian Self-Determination and Education Assistance Act. The Act authorizes Tribes to assume the administration and operation of federal programs, services and functions that were previously managed by the federal government. 25 U.S.C. §§ 450 & 450a (1994).

Fourth, the actual statement in the OIG Report says nothing about the security of contractor- operated IT Systems to prevent unauthorized access to IITD data by third parties through internet connections - the subject of the TRO and the preliminary injunction, and, for that matter, the Consent Order. The sentence of the OIG Report which Plaintiffs misquote addresses whether the contracts between Interior bureaus and IT service providers adequately address issues concerning employees used by the service providers, such as identifying sensitive positions and background clearances for those employees. Finally, the statement in the OIG Report which Plaintiffs misquote is the assessment of the IG's office, not, as Plaintiffs represent, the assessment of Secretary Norton and her senior managers.

5. The DOJ Attorneys Undertook Reasonable Inquiry

Finally, Plaintiffs assert that Department of Justice attorneys Robert McCallum, Jr., Peter Keisler, Stuart Schiffer, Christopher Kohn, Sandra Spooner, John Stemplewicz, Glenn Gillett, and John Warshawsky should be held to have violated the preliminary injunction because their names appeared in the signature blocks on papers transmitting one or more of the certifications.[17] Plaintiffs contend that the attorneys failed to conduct the "reasonable inquiry" mandated by Federal Rule of Civil Procedure 11. The "reasonable inquiry" standard of Rule 11 is less stringent that the standards necessary to support civil or criminal contempt. Nonetheless, Plaintiffs do not make a colorable showing that the certifications arguably failed to comply with the reasonable inquiry standard.

---

[17] Plaintiffs also assert that the attorneys' names appeared on papers transmitting quarterly reports "and other materially misleading information to this Court." IT Contempt Motion at 32, n.89. However, Plaintiffs only discuss the conduct of the attorneys in relation to the certifications under the preliminary injunction and do not even attempt to support their allegations against the attorneys regarding any other filings.

Rule 11 provides in pertinent part that by presenting a paper to the court an attorney is certifying

> that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances, -
>
> . . .
>
> (2) the claims, defenses, and other legal contentions therein are warranted by existing law. . . .
>
> (3) the allegations and other factual contentions have evidentiary support . . . .

Fed. R. Civ. P. 11(b).[18] The only legal issue Plaintiffs have raised about the certifications is the form of the attestation, and, as discussed above, the form used in the certifications is warranted by existing law.

The factual allegations or contentions in each certification were that the IT system addressed in the certification either did not house or provide access to IITD or was secure from internet access by unauthorized users. The lengthy "justifications" submitted in support of each certification furnished the evidentiary support for the factual allegations and contentions. The OIG, MMS, BLM, and NBC submitted justifications that their IT systems met the requirements of paragraph B.1.(b)(2) of the preliminary injunction (secure from internet access by unauthorized users). The other bureaus and offices certified that their IT systems did not house

[18] Plaintiffs purport to quote the text of Rule 11 as providing that an attorney's signature is a certification that the paper presented to the court "is well grounded in fact." This language is not in the text of the rule. To the extent that there is a difference between a certification that a pleading filed with the court is well grounded in fact and a certification that factual contentions in a pleading have evidentiary support, Plaintiffs are basing their argument on an incorrect standard.

or provide access to Individual Indian Trust Data as the term is defined in the preliminary injunction.

The Director of MMS signed the certification for MMS and stated:

> I certify that I believe that the information (including IITD) on the MMS's systems is secure from Internet access by unauthorized users and that the security measures now in place protect the IITD on the IT systems from unauthorized Internet access, for purposes of justifying Internet connectivity.

This declaration was made under the penalty of perjury and stated that it "is true and correct to the best of my knowledge, information and belief." Attached to the declaration were 92 pages of factual material upon which the declaration is based.

The Deputy Director for Operations of BLM and the Director of NBC signed certifications for BLM and NBC respectively, which were identical except for identification of the agencies. The BLM certification was supported by almost 100 pages of factual material, as was the NBC declaration.[19]

Of the hundreds of pages of evidentiary material filed in support of the certifications, Plaintiffs have only challenged a three-page declaration by Mr. Rossman. As discussed above, Plaintiffs' contentions about the Rossman declaration are without merit.

Plaintiffs also argue that the existence of the OMB, GAO and OIG reports should be considered in determining whether the attorneys acted reasonably. As discussed at length in part I, those reports are not inconsistent with the certifications, or, for that matter, with the quarterly reports. However, even if the reports were inconsistent with a certification, which they are not, the reports would only create a contested issue of fact. Rule 11 requires that factual assertions

---

[19] The OIG certification was also filed the same day, with supporting evidence. Plaintiffs do not identify any issues with the OIG certification.

have evidentiary support, not that factual allegations be uncontested. If the latter were the standard, any attorney filing an unsuccessful motion for summary judgment would necessarily violate Rule 11.

Besides requesting contempt sanctions against the Department of Justice attorneys, Plaintiffs propose in their draft order that the attorneys be referred to the Disciplinary Panel of the United States District Court for the District of Columbia. The defense attorneys fully complied with all professional obligations, and the requested referral therefore is totally unwarranted.

C. Quarterly Reports

1. The Quarterly Reports Do Not Contain Misrepresentations.

Plaintiffs contend that the 11th through the 15th Quarterly Reports contain material misrepresentations, affirmatively and by omission, regarding IT Security. IT Contempt Motion at 10-12, 25. Plaintiffs cite to statements that the "relative security and integrity of [Interior's] computer systems is gradually improving" (11th Quarterly Report at 8), or "slowly improving" (12th Quarterly Report at 10), or that "Interior's computer security efforts are showing significant progress" (14th Quarterly Report at 10).

Plaintiffs rely upon the 2003 Federal Computer Security Score Card (the "Scorecard") as evidence that there has been no improvement, apparently comparing Interior's scores over the years, as assigned by the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. IT Contempt Motion at 13. As described above, the Scorecard is based upon a variety of factors, not operational security, that is, it does not focus on whether a system is susceptible to unauthorized access from the internet. Accordingly, the numerical score,

albeit low, is not a reliable method for determining whether, in fact, Interior made gradual, slow, or significant progress in its security efforts.[20]

2. The Quarterly Reports Are Not Inconsistent with Subsequent Government Reports

Plaintiffs also attack the quarterly reports as inconsistent with findings in the GAO Investment Report. IT Contempt Motion at 21-25. As discussed in Part I.B, above, the GAO Investment Report addresses management of the investment of government funds on information technology, not IT security. As discussed in greater detail below, Plaintiffs' allegations are unsupported.

a. The Eleventh Quarterly Report and the GAO Investment Report Are Not Inconsistent

The Plaintiffs contend that the GAO Investment Report contradicts the Eleventh Quarterly Report's statements regarding capital asset planning:

> IT Security and Capital Asset Planning:
>
> - The budget justifications (Exhibit 300's) for IT systems were reviewed from an IT security perspective for the first time this quarter in connection with the FY 2004 budget. The review focused on IT security components relevant to the stage of the system lifecycle (planning, design, development, testing, implementation, steady state, or expiration). This year, for the first time, **DOI's new capital planning executive review boards met to assess major investments for IT systems. All aspects of system functionality and requirements analysis along with IT security were reviewed to assure proper controls and funding were being addressed.**

---

[20] It should be noted that the improvement in security is corroborated by the OIG Report, which Plaintiffs rely upon to argue that Defendants should be held in contempt. The OIG "found that [Interior] continues to improve the security of its information and information systems." OIG Report at 2. The OIG further stated that "[i]mprovements in information security related to Indian trust information and systems were also made" and cited examples. OIG Report at 11.

IT Contempt Motion at 21, citing 11th Quarterly Report at 10 (emphasis added by Plaintiffs).

Plaintiffs evidently equate a review to assure that issues are being addressed with a representation that the issues have been successfully resolved. Plaintiffs then cite to the GAO Investment Report at pages 12-13 to argue that, in fact, proper controls and funding are not in place. Contrary to Plaintiffs' rhetoric that "the GAO found **nothing** had been accomplished," IT Contempt Motion at 22, emphasis in original, in the very passage quoted by Plaintiffs from the GAO Investment Report at 12, the GAO stated that "a number of initiatives have been undertaken . . . ." The GAO noted, however, that reform has not moved forward as specified in the implementing memoranda.

The Plaintiffs characterize GAO's findings with regard to Interior's "capital planning review boards" as "ineffective and lack[ing] 'core competencies in using the IT investment approach.'" IT Contempt Motion at 22. Rather, what GAO found was that "executives cannot be adequately assured that decisions made by the boards are being well supported and carried out . . . ." GAO Investment Report at 17. Thus, the GAO did not find that the boards' decisions were not being implemented, but that there was no way to consistently know if the boards' decisions were being carried out.

The Plaintiffs also take Interior's statements about Exhibit 300s out of context. In its Eleventh Quarterly Report, Interior stated that it was reviewing Exhibit 300s from an IT security perspective. Plaintiffs contend this was impossible because: (a) there were no formal policies and procedures in place for the completion and review of the Exhibit 300s; (b) they are not required for non-major IT investments; and (c) the Management Council cannot demonstrate that identified users participated in project management. IT Contempt Motion at 22-23.

The GAO Investment Report stated that "written policies and procedures for identifying **business needs** have not been formally approved . . . ." GAO Investment Report at 26 (emphasis added). The GAO further found, however, that "[s]ince individuals responsible for identifying business needs and preparing Exhibit 300 reports work in departmental and bureau offices that sponsor IT investments, their work experience gives them sufficient knowledge regarding the business needs of those units. In addition, the department has provided supplemental training in business needs identification for major projects." Id.

Plaintiffs' complaint regarding the lack of Exhibit 300s for non-major investments does not establish a contradiction with Interior's statement that it reviewed Exhibit 300s. Plaintiffs' citation of the GAO's statement that "the department was also unable to demonstrate that identified users participated in project management throughout a project's life cycle" to challenge Interior's statement that it reviewed Exhibit 300s is also unavailing as the GAO statement does not relate to Exhibit 300s. IT Contempt Motion at 23 (citing GAO Investment Report at 25).

b. Plaintiffs Misread the Twelfth Quarterly Report.

In its Twelfth Quarterly Report, Interior reported that it was continuing to review Exhibit 300s, which "provides assurance that these investments are linked to mission needs . . . ." Twelfth Quarterly Report at 12. Plaintiffs contend this is a misrepresentation by Interior. IT Contempt Motion at 23. Plaintiffs rely upon GAO's finding that Interior does not have sufficient information regarding its IT inventory to "ensure that duplication among existing and proposed IT investments is eliminated." GAO Investment Report at 20. It appears that Plaintiffs are reading the term "mission needs" as used by Interior in the Twelfth Quarterly Report not to refer to whether the investment will fulfill mission goals, but rather whether there is or is not a need

for the investment because of duplication. Plaintiffs' parsing of the language in the Twelfth Quarterly Report does not comport with the GAO's discussion of the Exhibit 300s and their use in connection with assuring that the investments meet business needs of the users. See, e.g., GAO Investment Report at 26. Accordingly, Plaintiffs' contention that Interior made a misrepresentation in its Twelfth Quarterly Report is wrong.

c. Plaintiffs Misunderstand the Thirteenth Quarterly Report.

In its Thirteenth Quarterly Report, Interior reports that the IT Security Office completed the IT Security Asset Valuation Guide, Version 2.0. Thirteenth Quarterly Report at 10. Plaintiffs take issue with Interior's explanation that the "process provides a means for . . . establishing and validating IT security requirements based upon an IT system's overall importance." Id. Plaintiffs apparently interpret the explanation to mean that there is a "compliance system in place to ensure the adequacy of IT security requirements." IT Contempt Motion at 24. Plaintiffs rely upon the GAO Investment Report to refute their interpretation of what was stated in the Thirteenth Quarterly Report. However, the passage in the GAO Investment Report quoted by Plaintiffs does not refer to IT security requirements. Rather, the focus of the GAO's concerns is that "under performing projects will not be reported to the appropriate IT investment board. In the absence of effective board oversight, Interior executives do not have adequate assurance that projects are being developed on schedule and within budget." GAO Investment Report at 22. Thus, even assuming that Plaintiffs' interpretation of Interior's statement is correct, which Defendants do not concede, Plaintiffs' purported authority for disproving the statement is not on point.[21]

[21] Plaintiffs make similar allegations with regard to the Fourteenth Quarterly Report. IT (continued...)

III. Plaintiffs' Motion Has No Legal Basis.

A. Plaintiffs Have Failed to Establish a Legally Sufficient Basis for Civil Contempt Sanctions Against the Named Individuals.

1. The Standards for Civil Contempt Have Not Been Met.

The Court of Appeals for the D.C. Circuit recently clarified the distinction between civil and criminal contempt. The Court explained:

> Civil contempt is ordinarily used to compel compliance with an order of the court, [*Int'l Union, United Mine Workers v.*] *Bagwell*, 512 U.S. [821,] at 828 [(1994)], although in some circumstances a civil contempt sanction may be designed to "compensate[] the complainant for losses sustained." *Id.* at 829. By contrast, criminal contempt is used to punish, that is, to "vindicate the authority of the court" following a transgression rather than to compel future compliance or to aid the plaintiff. *Id.* at 828.

Cobell v. Norton, 334 F.3d 1128, 1145 (D.C. Cir. 2003). Plaintiffs purport to seek both civil and criminal sanctions in the current motion, but their motive is transparently punitive. Plaintiffs in fact acknowledge that they are alleging past failure of the Named Individuals to comply with Court orders, and that the appropriate remedy for such past violations is criminal, not civil, contempt. IT Contempt Motion at 44. The remedial purpose of a contempt order cannot be served where the allegedly violative act cannot be corrected. *See In re Sealed Case*, 250 F.3d 764, 770 (D.C. Cir. 2001) ("Because the Government could not undo the July 18 disclosure [of grand jury material], holding the Government in civil contempt would serve no useful purpose. . . ."). As explained in Part B, below, plaintiffs have fallen far short of establishing a basis for criminal contempt, and in any event, plaintiffs cannot prosecute a criminal contempt action, nor

---

[21](...continued)
Contempt Motion at 24, n.68. For the same reasons noted above, however, Plaintiffs' allegations are equally unsupported.

can they circumvent the Named Individuals' constitutional rights by filing a show cause motion. Although plaintiffs have failed to articulate a cogent factual basis for the Court even to consider an order to show cause for civil contempt, we address the legal strictures that would apply to civil contempt proceedings.

As stated above at page 14, a party seeking a finding of civil contempt must initially show, by clear and convincing evidence, that (1) a court order was in effect, (2) the order clearly and unambiguously required certain conduct by the respondent, and (3) the respondent failed to comply with the court's order. *SEC v. Bilzerian*, 112 F. Supp. 2d 12, 16 (D.D.C. 2000); *Petties v. District of Columbia*, 897 F. Supp. 626, 629 (D.D.C. 1995).

The Court of Appeals has ruled that a civil contempt order should be imposed, if at all, only at the conclusion of a three-stage proceeding involving "(1) issuance of an order; (2) following disobedience of that order, issuance of a conditional order finding the recalcitrant party in contempt and threatening to impose a specified penalty unless the recalcitrant party purges itself of contempt by complying with prescribed purgation conditions; and (3) exaction of the threatened penalty if the purgation conditions are not fulfilled." *NLRB v. Blevins Popcorn Co.*, 659 F.2d at 1184-85 (citing *Oil, Chem. & Atomic Workers Int'l Union v. NLRB*, 547 F.2d 575, 581 (D.C. Cir. 1976)); *see also SEC v. Bilzerian*, 112 F. Supp. 2d 12, 16 (D.D.C. 2000) (penalty should be imposed only after recalcitrant party has been given an opportunity to purge itself of contempt by complying with prescribed purgation conditions).

Plaintiffs have failed even to make out a prima facie case that Interior has violated any clear and unambiguous provision of the preliminary injunction. The preliminary injunction required Interior defendants to file certifications, and they did so. While plaintiffs have attacked

the certifications filed by Interior defendants pursuant the preliminary injunction, plaintiffs do not request an order directing the defendants to file revised certifications. In any event, the preliminary injunction itself established a procedure for plaintiffs to address the certifications, and plaintiffs have filed "comments" pursuant to those procedures. The comments remain pending before the Court. Thus, the Court should not even reach the first stage of the *Blevins Popcorn* proceeding.

If, upon consideration of the certifications and Plaintiffs' comments the Court ordered disconnection of a particular Reconnected System and Interior did not do so, the Court would have occasion to consider, after an appropriate hearing, whether Interior had not fully complied with the Court's order. Even if those hypothetical circumstances were to occur, the Court should, in accordance with *Blevins Popcorn*, establish purgation conditions so that Interior would have the opportunity to correct any deficiencies. A fundamental concept of civil contempt is that the contemnor "carries the keys of his prison in his own pocket." *Gompers v. Bucks Stove & Range Co.*, 221 U.S. 418, 442 (1911) (*cited in International Union, United Mine Workers of America v. Bagwell*, 512 U.S. 821, 828 (1994)). Thus, the individual found in civil contempt must be afforded the opportunity to purge the contempt. *See Bagwell*, 512 U.S. at 829 ("Where a fine is not compensatory, it is civil only if the contemnor is afforded an opportunity to purge."). It is simply not appropriate for the Court to proceed directly from a finding that an order has been violated to the imposition of civil contempt sanctions, as the Plaintiffs urge.

2. The Named Individuals Acted In the Course and Scope of Their Official Duties and Therefore Are Not Liable in Their Personal Capacities for Civil Contempt.

Plaintiffs request that the Named Individuals be held in civil contempt for alleged violations of the quarterly reporting violations of the December 21, 1999 Order, the TRO, and the preliminary injunction. Those rulings were directed to **Defendants.** Gale Norton is the only Named Individual who is a defendant, and she is a defendant only in her official capacity. Plaintiffs have made no allegations, nor supplied any evidence, that any Named Individual violated a court order directed to him or her personally or while acting in his or her personal capacity. While injunctive orders entered against the government are binding upon government employees acting as such, Fed. R. Civ. P. 65(d), an order against the government does not apply to government employees in their individual or personal capacities. *Hernandez v. O'Malley*, 98 F.3d 293, 294 (7th Cir. 1996) ("Fed. R. Civ. P. 65(d), which makes an injunction effective against successors in office, does not create personal (as opposed to official) liability."). As explained in *Dobbs, Law of Remedies 2d* § 2.8(5) (2d ed. 1993), an agent who is acting in his own interest and not in the interest of his principal or employer would not be in violation of an injunction directed to his principal or liable for contempt. Thus, the Named Individuals, acting in their personal capacities, were not "within the order's ambit," *see Project B.A.S.I.C.*, 947 F.2d at 17, and they cannot be held liable in their personal capacities for any violations of the December 21, 1999 ruling, the TRO, or the preliminary injunction.

Plaintiffs' claims against the Named Individuals concern solely actions taken in their official capacities. Any claim in this proceeding against the Named Individuals in their official capacities is a claim against the government. As the Supreme Court has explained:

> Official-capacity suits, in contrast, "generally represent only another way of pleading an action against an entity of which an officer is an agent." *Monell v. New York City Dept. of Social Services*, 436 U.S. 658, 690, n.55 (1978). As long as the government entity receives notice and an opportunity to respond, an official-capacity suit is, in all respects other than name, to be treated as a suit against the entity.

Kentucky v. Graham, 473 U.S. 159, 165-66 (1985); *see also Wyoming v. United States*, 279 F.3d 1214, 1225 (10th Cir. 2002), and cases cited therein. Gale Norton is a defendant in her representative capacity, and any civil contempt relief to which Plaintiffs could conceivably be entitled against the government would be fulfilled by a finding against her in her official capacity. Plaintiffs' motion that twelve Named Individuals who are not parties to this case show cause why they should not be held in civil contempt, as well as the torrent of personal abuse directed to Secretary Norton and the non-party Named Individuals, serve no legitimate litigation purpose.

3. Plaintiffs Fail to Identify Any Form of Relief They Could Obtain From Contempt Sanctions, And There Are None.

Civil contempt sanctions are used either to obtain compliance with a court order or to compensate for damages sustained as a result of noncompliance. *Food Lion, Inc. v. United Food & Commercial Workers Int'l Union*, 103 F.3d 1007, 1016 (D.C. Cir. 1997). Therefore, the party seeking a civil contempt finding must articulate some legally available form of relief for the injury it claims to have suffered as a result of the alleged contumacy.

Plaintiffs ask the Court to hold Named Individuals in civil contempt without specifying any relief they could possibly obtain from a civil contempt finding. This failure, too, is fatal to their motion. The goal of a civil contempt order is not to punish, but to exert only so much of the court's authority as is required to assure compliance. *Petties*, 897 F. Supp. at 629. "Civil

contempt does not exist to punish the contemnor or to vindicate the court's integrity." *Morgan v. Barry*, 596 F. Supp. 897, 899 (D.D.C. 1984)) (citing *National Labor Relations Board v. Blevins Popcorn Co.*, 659 F.2d 1173 (D.C. Cir. 1981)). Plaintiffs do not attempt to identify either coercive or compensatory sanctions that would be appropriate to redress the alleged violations of the orders.

Further, Plaintiffs' counsel have failed in their motion to identify any damages suffered by members of the plaintiff class as a result of the alleged violations.[22] In any event, the doctrine of sovereign immunity bars the imposition of fines, penalties or monetary damages against the government, except to the extent that the United States has explicitly consented to such sanctions. The doctrine of sovereign immunity "stands as an obstacle to virtually all direct assaults against the public fisc, save only those incursions from time to time authorized by Congress." *United States v. Horn*, 29 F.3d 754, 761 (1st Cir. 1994). A waiver of sovereign immunity must be definitively and unequivocally expressed and must appear in the text of the statute itself. *Id.* at 762 (citing *United States v. Mitchell*, 445 U.S. 535, 538 (1980), and *United*

---

[22] Plaintiffs' counsel once again urge the Court to award them their fees and costs associated with bringing this motion. However, the Court of Appeals ruled that such an award "cannot be considered relief for the underlying contempt. . . ." 334 F.3d at 1145. That holding is the law of the case and is binding upon this Court through the mandate rule. *Indep. Petroleum Ass'n of America v. Babbitt*, 235 F.3d 588, 597 (D.C. Cir. 2001) ("The mandate rule is a 'more powerful version' of the law-of-the-case doctrine, which prevents courts from reconsidering issues that have already been decided in the same case.") (quoting *LaShawn A. v. Barry*, 87 F.3d 1389, 1393 n.3 (D.C. Cir. 1996)). Plaintiffs attempt to persuade the Court to ignore the Court of Appeals' holding by citing a recent Supreme Court case, *Frew v. Hawkins*, 2004 WL 57266 (U.S. Jan. 14, 2004). *See Plaintiff's Notice of Supplemental Authority* (filed Jan.22, 2004) at2-3. However, the portion of *Frew* that plaintiffs rely is simply an excerpt and explication of the Court's 1978 decision in *Hutto v. Finney*, 437 U.S. 678 (1978). The Court of Appeals must be presumed to have been aware of this 25-year-old decision when it issued its 2003 ruling in the present case. Further, *Frew* and *Hutto* both involve the imposition of compensatory sanctions for civil contempt against state entities – not against a coordinate branch of the Federal government in the absence of an explicit waiver of sovereign immunity.

States v. Nordic Village, Inc., 503 U.S. 30 (1992)). The determinations in this case that sovereign immunity does not bar either Plaintiffs' claim for prospective action or their claim for retrospective relief in the form of an accounting[23] have no bearing on the separate issue of whether the government has waived sovereign immunity for money damages for civil contempt. A waiver of sovereign immunity as to one available remedy does not, by implication, waive sovereign immunity as to other remedies. *See Brown v. Secretary of the Army*, 918 F.2d 214 (D.C. Cir. 1990) (waiver of sovereign immunity as to back pay awards for discriminatory denial of promotion did not waive sovereign immunity for prejudgment interest on such back pay awards).

The United States has not waived sovereign immunity from citation for criminal contempt, nor for court-imposed fines for civil contempt. *Coleman v. Espy*, 986 F.2d 1184, 1191 (8th Cir. 1993); *United States v. Horn*, 29 F.3d at 763; *see also In re Sealed Case*, 192 F.3d 995, 999-1000 (D.C. Cir. 1999) (*per curiam*) ("[i]t is far from clear that Congress has waived federal sovereign immunity in the context of criminal contempt. . . . We know of no statutory provision expressly waiving federal sovereign immunity from criminal contempt proceedings.").[24]

---

[23] *See Cobell v. Babbitt*, 30 F. Supp. 2d. 24, 31-33, 38-42 (D.D.C. 1998) (denying defendants' motion for judgment on the pleadings); *Cobell v. Babbitt*, 52 F. Supp. 2d 11, 21 (D.D.C. 1999) (denying defendants' motion for summary judgment); *see also Cobell v. Norton,* 240 F.3d 1081, 1094-95 (D.C. Cir. 2001) (agreeing that plaintiffs' action was not barred by sovereign immunity).

[24] As the Court acknowledged in the Contempt II Order, whether a court can order the government to compensate a party for losses sustained as a result of the government's contempt has not been decided by the Court of Appeals in this Circuit. 226 F. Supp. 2d at 154 n.163. The District Court in *United States v. Waksberg*, 881 F. Supp. 36, 41 (D.D.C. 1995), *vacated and remanded*, 112 F.3d 1225 (D.C. Cir. 1997), held that sovereign immunity barred recovery of damages as compensation for the government's violation of an injunctive order. The Court of Appeals vacated and remanded with directions to withhold a ruling on the sovereign immunity (continued...)

Accordingly, to the extent that Plaintiffs are requesting any monetary remedies, sovereign immunity precludes such an award.

Because the availability of a remedy "for the benefit of the complainant" is an essential component of a civil contempt proceeding, *Bagwell*, 512 U.S. at 827 (quoting *Gompers,* 221 U.S. at 441), and Plaintiffs' Motion fails to identify any remedial measure the Court could properly order, the motion should be denied.

B. Plaintiffs Have Failed to Demonstrate a Legally Sustainable Basis for the Issuance of Show Cause Orders for Criminal Contempt.

As shown above, Plaintiffs' allegations do not meet the legal requirements for civil contempt sanctions. They certainly do not satisfy the heightened showing required for criminal contempt sanctions. Further, to the extent that Plaintiffs seek punitive sanctions (including incarceration), the Named Individuals are entitled to the full measure of due process afforded in criminal proceedings, including a trial by jury and proof beyond a reasonable doubt. *Cobell v. Norton*, 334 F.3d 1128, 1147 (D.C. Cir. 2003).

Plaintiffs do not identify the particular statutory provision upon which they base their claims of criminal contempt. Plaintiffs are requesting sanctions for violations of court orders. To convict a defendant of criminal contempt for violation of court orders, the Court must find, beyond a reasonable doubt, that the person willfully violated a "clear and reasonably specific" order of the court. *United States v. Roach*, 108 F. 3d 1477, 1481 (D.C. Cir. 1997) (citing *United States v. NYNEX Corp.,* 8 F.3d 52, 54 (D.C. Cir. 1993), and *United States v. Turner,* 812 F.2d 1552, 1563 (11th Cir. 1987)). For a violation to be "willful," the accused must have acted with

---

[24](...continued)
issue pending a determination on whether Waksberg had incurred damages. 112 F.3d at 1228.

deliberate or reckless disregard of the obligations created by the court order. *Roach*, 108 F.3d at 1481 (citing *In re Holloway*, 995 F.2d 1080, 1082 (D.C. Cir. 1993), and *United States v. Greyhound Corp.,* 508 F.2d 529 (7th Cir. 1974)).

Thus, in order to support a referral for criminal contempt, Plaintiffs must initially show that evidence exists that, if believed, could establish beyond a reasonable doubt that (1) a clear and reasonably specific court order was in effect, (2) the order required certain conduct by a Named Individual, and (3) the Named Individual willfully violated the court's order. Moreover, Plaintiffs must demonstrate Named Individual by Named Individual that the elements for a criminal referral exist. *Cobell v. Norton*, 334 F.3d 1128, 1147 (D.C. Cir. 2003).

For the same reasons that their claims fail to establish a basis for civil contempt, Plaintiffs' claims cannot meet the even more stringent criminal contempt standard. As discussed, the orders at issue did not apply to the Named Individuals in their personal capacities, and Plaintiffs have failed to demonstrate that anyone violated an order in his or her official capacity. Plaintiffs' assertions that alleged violations were willful are strictly rhetorical, unsupported by any evidence whatsoever. Finally, Plaintiffs do not even attempt to show the elements necessary to support a referral of criminal contempt for any particular Named Individual - identifying his or her conduct allegedly violating a court order and setting forth evidence showing that any such alleged violation was willful. Plaintiffs have made serious charges against the Named Individuals and have asked for serious consequences. Their failure even to attempt to support the charges individual by individual is profoundly unprincipled.

CONCLUSION

Plainly, there is neither a legal nor factual basis for Plaintiffs' Motion. For the reasons stated above, the Court should deny Plaintiffs' Motion and admonish Plaintiffs against filing such frivolous and reckless pleadings in the future.

Respectfully submitted,

ROBERT D. McCALLUM, JR.
Associate Attorney General

PETER D. KEISLER
Assistant Attorney General

STUART E. SCHIFFER
Deputy Assistant Attorney General

MICHAEL F. HERTZ
Director

/s/ Dodge Wells
Dodge Wells
D.C. Bar No. 425194
Tracy L. Hilmer
D.C. Bar No. 421219
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 261
Ben Franklin Station
Washington, D.C. 20044
(202) 307-0474

DATED: January 27, 2004

CERTIFICATE OF SERVICE

I hereby certify that, on January 27, 2004 the foregoing *Memorandum of Points and Authorities in Opposition To Plaintiffs' Motion for an Order to Show Cause Why The Department of the Interior Secretary, Gale Norton, and Her Senior Managers and Counsel Should Not Be Held in Civil And Criminal Contempt for Violating Court Orders* was served by Electronic Case Filing, and on the following who is not registered for Electronic Case Filing, by facsimile:

Earl Old Person (*Pro se*)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
Fax (406) 338-7530

/s/ Kevin P. Kingston
Kevin P. Kingston

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
Plaintiffs,	)	
v.	)	Case No. 1:96CV01285
	)	(Judge Lamberth)
GALE NORTON, Secretary of the Interior, et al.,	)	
Defendants.	)	

ORDER

This matter comes before the Court on *Plaintiffs' Motion for an Order to Show Cause Why the Department of the Interior, Interior Secretary Gale Norton, and Her Senior Managers and Counsel, Should Not Be Held in Civil and Criminal Contempt for Violating Court Orders, Including the Temporary Restraining Order and Preliminary Injunction Entered to Protect Trust Data and Assets* (Dkt. # 2441). Upon consideration of the Plaintiffs' Motion, Defendants' Opposition, any Reply thereto, and the entire record of this case, it is hereby

ORDERED that the Motion for an Order to Show Cause is DENIED.

SO ORDERED.

Hon. Royce C. Lamberth
UNITED STATES DISTRICT JUDGE
United States District Court for the
District of Columbia

Date:_____

cc:

Dodge Wells
Tracy L. Hilmer
Sandra P. Spooner
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875

Dennis M Gingold, Esq.
Mark Brown, Esq.
1275 Pennsylvania Avenue, N.W.
Ninth Floor
Washington, D.C. 20004

Keith Harper, Esq.
Richard A. Guest, Esq.
Native American Rights Fund
1712 N Street, NW
Washington, D.C. 20036-2976
Fax (202) 822-0068

Elliott Levitas, Esq.
1100 Peachtree Street, Suite 2800
Atlanta, GA 30309-4530

Earl Old Person (*Pro se*)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
Fax (406) 338-7530