IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 1:96CV01285
	)	(Judge Robertson)
DIRK KEMPTHORNE, Secretary of the Interior, et al.,	)	
	)	
Defendants.	)	
	)	

INTERIOR DEFENDANTS' REPLY BRIEF IN SUPPORT OF MOTION FOR ORDER THAT THE OFFICE OF THE SOLICITOR INFORMATION TECHNOLOGY SYSTEM MAY BE RECONNECTED TO THE INTERNET

I. Plaintiffs' Opposition to Interior Defendants' Motion Wholly Disregards the Substantial Changes in the Law Governing Federal Information Technology Security Assessments Since Entry of the Consent Order

The Government commenced the process to vacate the Consent Order that prevents Interior from reconnecting certain Information Technology ("IT") systems to the Internet when it filed Defendants' Motion to Vacate Consent Order Regarding Information Technology Security (Dkt. No. 3299) (Mar. 19, 2007) ("Motion to Vacate Consent Order"). See Interior Defendants' Motion for Order That the Office of the Solicitor Information Technology System May Be Reconnected to the Internet (Dkt. No. 3450) (Nov. 9, 2007) ("Motion to Reconnect Solicitor's IT System") at 2. In the Motion to Vacate Consent Order, we described the substantial changes in the federal law governing oversight of IT security since issuance of the Consent Order, see Motion to Vacate Consent Order at 14-19 (discussing, among other things, FISMA, the enhanced role of NIST, and Cobell XVIII).

As we further explained, this Court denied the Government's motion to vacate the Consent Order without prejudice, Tr. 41:9-10 (May 14, 2007), and in doing so, expressly noted that the legal landscape was different from the time when the Consent Order was entered and described the additional information to be provided by the Government:

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

Tr. 40:12-18 (May 14, 2007), quoted in Motion to Reconnect Solicitor's IT System at 2. The Court continued:

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

Tr. 41:10-14 (May 14, 2007), quoted in Motion to Reconnect Solicitor's IT System at 2.

As we further explain below, Interior Defendants' Motion to Reconnect Solicitor's IT System provides the Court with the remaining element described by the Court during the May 14, 2007 hearing.[1] In their opposition, however, Plaintiffs' principal arguments ask this Court to

[1] Plaintiffs' arguments about the sufficiency of the jurat on the declarations, Plaintiffs' Opposition to Defendants' Motion for Order That the Office of the Solicitor Information Technology System May Be Reconnected to the Internet (Dkt. No. 3472) (Dec. 14, 2007) at 2 and n. 4, 10-11, are incorrect. Interior Defendants believe the declarations attached to the original motion are sufficient to demonstrate that the Solicitor's IT system has security in place and that a decision to reconnect has been made, consistent with FISMA's requirements. There is a distinction between providing sworn declarations for the Court's consideration as evidence (for which a jurat is required by the local rule) and providing documents that serve as substantive evidence that Interior has complied with the requirements of federal IT security law. Indeed, for purposes of this motion, Interior Defendants arguably could have provided the required information by attaching internal memoranda, rather than documents denominated as

make judgments about the adequacy of Interior's overall IT security, rather than address the question posed by this Court, i.e., whether the Solicitor's IT systems have implemented security measures since entry of the Consent Order. See Plaintiffs' Opposition to Defendants' Motion for Order That the Office of the Solicitor Information Technology System May Be Reconnected to the Internet (Dkt. No. 3472) (Dec. 14, 2007) ("Opp.") at 6-10 (discussing overall assessments of Interior IT systems by Congress, GAO, auditors, and Interior's Inspector General).[2]

In this regard, Plaintiffs' principal attack wholly ignores the changes in the law since entry of the Consent Order. As we explained in both our initial motion to vacate the Consent Order and the current motion, FISMA expresses Congress' determination that the head of the agency bears responsibility for "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency." 44 U.S.C. § 3544(a)(1)(A)(i). The D.C. Circuit recognized the import of Congress' intent in Cobell XVIII, when it reviewed the extensive findings developed by this Court during

---

"declarations." Nevertheless, in order to moot Plaintiffs' contentions, we have attached identical declarations bearing a jurat that conforms to the court's analysis in Cobell v. Norton, 391 F.3d 251, 260 (D.C. Cir. 2004).

[2] Although Plaintiffs place great emphasis upon the 2007 reports from Interior's Inspector General and from Congress, neither of these documents undermines Interior's motion to reconnect. As Plaintiffs readily concede, the Seventh Report Card on Computer Security at Federal Departments and Agencies, April 12, 2007, does not address specifically the IT systems of the Office of the Solicitor. Opp. at 6-7, n.13. Moreover, it does not present a mandate that any of the federal departments or agencies should be disconnected from the Internet because of the grade received. No one, not even Plaintiffs, has suggested that the Department of Defense or the Department of State, agencies that address the very security of the United States and which received the same grade as Interior, should be disconnected from the Internet because of the grades they received.

the 59-day Preliminary Injunction hearing in 2005 and confirmed that while FISMA "includes a role for OMB, the Department of Commerce, the NIST, the Comptroller General, Congress, the public, and multiple officials within each agency subject to the statute[,] [n]otably absent from FISMA is a role for the judicial branch." Cobell v. Kempthorne, 455 F.3d 301, 314 (D.C. Cir. 2006).

Plaintiffs' opposition seeks to reinsert this Court into the process of making determinations about the adequacy of the Solicitor's IT system security measures. As we have already explained, however, in the years that have passed since entry of the Consent Order, Congress and the D.C. Circuit have confirmed that the judiciary does not properly serve a role in determining how much security is required for IT systems or assessing the risk or magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of an agency's data. Accordingly, even to the extent Plaintiffs accurately characterize the Consent Order reconnection process in their brief,[3] Opp. at 2-5, their arguments

[3] Plaintiffs do not accurately describe the Consent Order process. While Plaintiffs suggest that the Consent Order process commenced with the provision of notice to Plaintiffs, a review of the reconnection proposals from 2002 will confirm that the process was conducted entirely by exchanges among Interior officials, Justice Department counsel, and the Special Master and his experts. Plaintiffs were provided copies of Interior reconnection proposals, but their role was limited to observing, a role they declined to accept given their repeated rejection of the Consent Order's process. See, e.g., Opp. at 4-5 and 5 n.10. Plaintiffs' characterization of the process is flawed in other respects, such as their unsubstantiated assertion that the Consent Order process was the Government's preference of the Consent Order to discovery and litigation because of a "good working relationship with the master." Id. at 4 n.9.

This Court does not need to resolve whether Plaintiffs have accurately described the Consent Order process, however. As described by Plaintiffs in their opposing brief, the Consent Order empowered the Special Master and this Court to make substantive decisions about how much and what types of security were required to be deemed "adequate" for purposes of protecting data. E.g., Opp. at 4 ("The *Consent Order* reconnection process . . . was no rubber stamp process; rather, the order conferred on the master broad authority . . . .") (italics in

are misplaced because that process is no longer authorized by law.

II. The Motion to Reconnect the Solicitor's IT System Demonstrates That Security Exists to Protect Data and That Interior Has Complied With the Requirements of FISMA

During the May 14, 2007 hearing, this Court declined to grant the Government's motion to vacate the Consent Order because Interior had not "made the requisite showing that [it had] any security." Tr. 40 :17-18 (May 14, 2007). The Court denied the Government's motion without prejudice, however, and advised the Government:

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

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

Interior Defendants' Motion to Reconnect Solicitor's IT System is accompanied by four statements of Interior officials confirming both the existence of IT security measures for the Solicitor's IT network, known as "SOLNET," and Interior's compliance with FISMA requirements. The following are among the matters demonstrated by the attached statements:

- In the declaration of Mike Howell, Interior's Chief Information Officer ("CIO") confirms, among other things, that Interior has established a uniform process for bureaus and offices to follow when seeking interconnections with other Interior IT systems. The process is known as the "Department of the Interior Connection Approval Process" ("CAP"), and it was prepared in conformity with NIST and Interior requirements and guidelines. The Solicitor's proposal to establish an interconnection between SOLNET and Interior's Enterprise Service Network ("ESN") would provide SOLNET with network services, including Internet connectivity. The Solicitor's proposal and related documentation has been reviewed by both officials within Interior's CIO's office and an independent contractor hired by Interior's CIO. Mr. Howell considered the results of the

---

original). For the reasons described in our Motion to Vacate Consent Order and the current motion, such powers are simply beyond the federal law that has evolved since 2001.

reviews, plans for further reviews and testing, and other materials, e.g., open vulnerabilities identified in the SOLNET Plan of Action and Milestones, and advised the Associate Deputy Secretary "that the SOLNET-ESN interconnection has, to the best of [his] knowledge, adequate security controls in place commensurate with the potential risks" and that he "recommend[ed] that the interconnection be approved."

- In the declaration of Craig Littlejohn, the Solicitor's CIO confirms, among other things, that the Solicitor's Office has followed the CAP protocol and has developed an Interconnection Security Agreement for the proposed SOLNET-ESN connection which defines the technical security requirements and further describes security controls in place to protect SOLNET, including Intrusion Prevention System appliances, the deployment of a secure software image on workstations, internal vulnerability scanning software and processes, server event logging processes, automated deployment of software updates and patches, current antivirus/spyware software, and host firewalls on all workstations. The Solicitor hired an independent contractor (different from the contractor hired by Interior's CIO) to evaluate SOLNET, and the contractor conducted its review in April 2007. Mr. Littlejohn submitted CAP documentation and the most recent SOLNET Certification and Accreditation ("C&A") documentation to Interior's CIO, and he further confirmed that "regular security compliance reviews will be conducted to evaluate SOLNET and report on vulnerabilities and corrective actions." Mr. Littlejohn advised the Solicitor, who is the FISMA "Designated Approving Authority" regarding security controls for SOLNET, which Mr. Littlejohn concluded "have been implemented correctly and are effective." Mr. Littlejohn advised that, in his opinion, "the security of SOLNET is adequate to protect the information associate with that system, commensurate with the risks to which it is exposed."

- In the declaration of David L. Bernhardt, the Solicitor confirms that under FISMA, he is "the agency official responsible for proper assessment of the level of security protection necessary for [SOLNET]." Mr. Bernhardt confirmed that after considering potential risks and the magnitude of harm and briefings by the CIOs for Interior and the Solicitor, he has made the determination "that the security controls and plans in place for SOLNET provide adequate security, commensurate with the risks and magnitude of the harm resulting from potential unauthorized access, to protect the information associated with the system."

- In the declaration of James E. Cason, the Associate Deputy Secretary confirms that after review of CAP process-generated materials and consideration of the advice and recommendations of the CIOs for Interior and the Solicitor, he has made the determination "that the security controls and plans in place for SOLNET and ESN provide adequate security, commensurate with the risk and magnitude of the harm resulting from potential unauthorized access, to protect the information

> associated with those systems." Accordingly, Mr. Cason stated his intention "to authorize the proposed interconnection between SOLNET and ESN, subject to approval by the District Court."

Plaintiffs' opposition to the motion devotes a scant two-and-half pages to the substance within these four declarations. Opp. at 12-14. In doing so, Plaintiffs essentially raise questions about how risks to trust data have been weighed, Opp. at 12, and reference a 2004 SOLNET Risk Assessment document which, as Plaintiffs concede, was reviewed during the 2005 IT security hearing, Opp. at 13-14. The obvious problem with Plaintiffs' challenge to the "weighing" of risks is that Congress made the agency head responsible for these determinations. 44 U.S.C. § 3544(a)(1)(A)(i). In the words of the D.C. Circuit in Cobell XVIII, "[t]his is not a FISMA compliance case, whether or not such an animal exists." 455 F.3d at 314. With regard to the 2004 SOLNET Risk Assessment document, it should be evident that, over three years later, its relevance to the current state of IT security is dubious.[4]

---

[4] The state of IT security is constantly changing, as agencies are called upon to address changes in data requirements, new hardware and software, and new risks to data. See, e.g., NIST Special Publication 800-37, ch. 2.1 at 9 (Guide for the Security Certification and Accreditation of Federal Information Systems) (May 2004) ("Security accreditation is part of a dynamic, ongoing risk management process.") (quoted in Cobell v. Norton, 394 F. Supp. 2d 164, 176 (D.D.C. 2005), vacated on other grounds, Cobell v. Kempthorne, 455 F.3d 301 (D.C. Cir. 2006) ("Cobell XVIII"). A copy of Special Publication 800-37 is accessible at http://csrc.nist.gov/groups/SMA/fisma/CnA.html). NIST's guidance further provides, in part:

> The monitoring of security controls in the information system continues throughout the system development life cycle. Reaccreditation occurs when there are significant changes to the information system affecting the security of the system or when a specified time period has elapsed in accordance with federal or agency policy.

Special Publication 800-37, ch. 2.7, at 24. The evolving state of IT security within Interior was described in detail by this Court and the D.C. Circuit in the opinions cited above, and given the constantly changing nature of IT security, the 2004 Risk Assessment document cannot be relied

III. Plaintiffs' Claims Of Irreparable Harm And "Catastrophic Loss" Are Wholly Insupportable and Groundless

Plaintiffs repeatedly make bald assertions such as their claim that "reconnection to the Internet would further expose plaintiffs' trust assets to catastrophic loss" or "catastrophic risk," and that they would suffer "irreparable harm" as "a result of the government's continuing breach of trust." Opp. at 5, 15. The D.C. Circuit rejected such assertions in Cobell XVIII,[5] and no evidentiary basis exists for the Court to entertain them now. Plaintiffs present nothing which supports an assertion of "catastrophic loss" related to the reconnection of SOLNET to the Internet.[6] See also Tr. 35:20-36:15 (May 14, 2007) (Plaintiffs' counsel provides no

---

upon to provide information about SOLNET in December 2007.

[5] Following the 59-day hearing in 2005, in which Plaintiffs obtained no less than five million pages of documents, Opp. at 10 ("Interior defendants, having filed over five million pages of documentation in connection with the 2005 IT evidentiary hearing . . . ."), the Court of Appeals concluded:

> The class members have pointed to no evidence showing that anyone has already altered IITD [individual Indian Trust data] by taking advantage of Interior's security flaws, nor that such actions are imminent. Even if someone did penetrate Interior's systems and alter IITD, we have been shown no reason to believe that the effects would likely be so extensive as to prevent the class members from receiving the accounting to which they are entitled.
> . . . .
>
> While the class members may face some risk of harm if IITD housed on Interior's computers were compromised, we have not been shown that this possibility is likely, nor that it would substantially harm the class members' ability to receive an accounting.

Cobell XVIII, 455 F.3d at 315, 317.

[6] Plaintiffs' assertion that "defendants do not want to protect trust data," Opp. at 2, is inflammatory and baseless. Interior's expenditure of more than $100 million dollars and utilization of extensive manpower to improve its IT security reveals how important the protection of trust data is to Interior. See Cobell v. Norton, 394 F. Supp. 2d 164, 267-68 (D.D.C. 2005), vacated on other grounds, Cobell v. Kempthorne, 455 F.3d 301 (D.C. Cir. 2006). Even

substantiation for Plaintiffs' "belief" that beneficiaries have not received payments because of IT system security issues).

IV. This Court Should Reject Plaintiffs' Request to Conduct Discovery and to Schedule Either an Evidentiary Hearing Regarding IT Security or a Trial on Alternative Equitable Remedies

Plaintiffs finally ask this Court to "authorize plaintiffs' discovery on the posture of security on SOLNET as well as any other Interior system that defendants seek to reconnect to the Internet." Opp. at 15. Plaintiffs further "suggest that such discovery should be conducted in preparation for an evidentiary hearing so that this Court may 'resolve the state of Interior's IT systems security." Id. Plaintiffs further seek to delay the Court's consideration of the current motion by asking "that any IT security evidentiary hearing be held in abeyance until such time as a trial on alternative equitable remedies has been completed and a judgment rendered." Id.

The motivation behind these requests must be transparent. Over the years, Plaintiffs have had numerous opportunities to obtain information about Interior's IT systems, and this culminated in the 59-day Preliminary Injunction hearing at which, by Plaintiffs' own account, the Government produced over five million pages of materials. Opp. at 10. At the end of this process, the D.C. Circuit rejected any claim that Plaintiffs had demonstrated entitlement to injunctive relief, particularly in light of the legal developments since the Consent Order was entered. This Court's orders regarding discovery during 2007 have reflected an appreciation for the limited role of discovery in this matter, particularly where Plaintiffs have shown no need to

---

this Court recognized in 2005 that "[i]t is also undeniable that Interior has made strides in the IT security arena. The Court is aware that, when IT security became an issue in this litigation some years ago, Interior was forced to begin from square one. Many of the individuals who testified in this evidentiary hearing are competent, conscientious, and well-intentioned. Interior's progress in a period of five years is laudable." 394 F. Supp. 2d at 272.

conduct discovery.

Plaintiffs further confuse issues by an apparent misreading of Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004) ("Cobell XII"). Opp. at 15. Contrary to Plaintiffs' suggestion that the D.C. Circuit required a hearing on any matters regarding IT security, the Cobell XII holding simply concluded that this Court's entry of a preliminary injunction against Interior in March 2004, without a hearing, was improper when material facts were in dispute, "[p]articularly when a court must make credibility determinations to resolve key factual disputes in favor of the moving party." 391 F.3d at 261 (citation omitted). In this case, there can be no serious dispute that Interior has made the determinations described in the motion to reconnect SOLNET. The only serious dispute raised by Plaintiffs regards the risk-management assessments by Interior's officials, but, again, both Congress and Cobell XVIII confirm that such assessments are not properly within the province of the judiciary.

Finally, putting aside the facially dubious nature of Plaintiffs' repeated requests for "a trial on alternative equitable remedies," there simply is no justification for requiring the Solicitor's Office to continue to operate in a pre-Internet environment. Interior has complied with the requirements imposed by Congress to operate SOLNET in an environment with Internet connectivity, and Interior Defendants' motion to reconnect the Solicitor's IT system provides the Court with the information missing from the original motion to vacate the Consent Order, i.e., IT security is in place and Interior has complied with the risk-assessment provisions of FISMA.

CONCLUSION

For the reasons set forth in Interior Defendants' Motion to Reconnect Solicitor's IT System and the foregoing reasons, Interior Defendants respectfully request that the Court issue

an Order that Interior Defendants may proceed to reconnect SOLNET to the Internet.

Dated: December 21, 2007

Respectfully submitted,

JEFFREY S. BUCHOLTZ
Acting Assistant Attorney General

MICHAEL F. HERTZ
Deputy Assistant Attorney General

J. CHRISTOPHER KOHN
Director

/s/ Robert E. Kirschman, Jr.
ROBERT E. KIRSCHMAN, JR. (D.C. Bar No. 406635)
Deputy Director
JOHN WARSHAWSKY (D.C. Bar No. 417170)
Senior Trial Counsel
GLENN GILLETT
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 616-0328
Facsimile: (202) 514-9163

CERTIFICATE OF SERVICE

I hereby certify that, on December 21, 2007 the foregoing *Interior Defendants' Reply Brief in Support of Motion for Order That the Office of the Solicitor Information Technology System May Be Reconnected to the Internet* 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,	)	
	)	Case No. 1: 96CV01285
v.	)	
	)	(Judge Robertson)
DIRK KEMPTHORNE,	)	
Secretary of the Interior, et al.,	)	
	)	
Defendants.	)	

REVISED DECLARATION OF CRAIG LITTLEJOHN

I, Craig Littlejohn, declare as follows:

1. I am the Chief Information Officer (CIO) for the Office of the Solicitor, United States Department of the Interior (the Department). I have held this position for approximately 3 years. I am certified by the International Information Systems Security Consortium, Inc. as a Certified Information System Security Professional. My staff of 10 federal and contractor information technology professionals in the Office of the Solicitor, Division of Administration, provide support services for the hardware and software that comprise the Office of the Solicitor network environment (hereinafter "SOLNET").
2. SOLNET provides general IT services such as electronic messages, file sharing, and printer sharing to over 400 employees of the Office of the Solicitor. As CIO, my responsibilities for SOLNET include system development and maintenance, and implementation of applicable information technology policies, directives, and guidelines. It is also my responsibility to execute certain tasks required by the *Department of the*

Interior Connection Approval Process (CAP), which is the policy establishing a uniform process for Department bureaus and offices to utilize when seeking interconnections between IT systems.

3. The Office of the Solicitor has proposed that SOLNET be connected to the Internet through the Department Enterprise Service Network (ESN) in accordance with the CAP policy.

4. The primary tasks which needed to be accomplished by the Office of the Solicitor in order to comply with the CAP were (1) establishing a Memorandum of Understanding and an Interconnection Security Agreement with the Department for the interconnection through ESN; (2) validating that the SOLNET Certification & Accreditation (C&A) process was completed; and (3) providing a recommendation on whether to grant approval for the interconnection.

5. I developed and finalized a Memorandum of Understanding which described the background and purpose for the SOLNET interconnection and defined the roles, responsibilities, terms, conditions, and expectations of the Department and of the Office of the Solicitor for security and operation of ESN and SOLNET. The agreement was signed by both parties.

6. I also developed an Interconnection Security Agreement for the proposed SOLNET interconnection which defined the technical security requirements and further identified and described the security controls in place to protect SOLNET. These security controls include:

    i. Intrusion Prevention System appliances on each local area network segment, which are capable of identifying viruses,

unauthorized equipment and user access, and network traffic anomalies;

ii. secure software image deployed on all workstations based on the National Institute of Standards and Technology (NIST) Security Technical Implementation Guide;

iii. internal vulnerability scanning software and processes for assessment and mitigation of vulnerabilities;

iv. server event log collection, management, and reporting;

v. automated deployment of system software updates and patches via Microsoft Systems Management Service;

vi. current anitvirus/spyware software and centralized scheduled updates of signature files;

vii. host firewalls on all workstations.

7. The Interconnection Security Agreement defines the maintenance and monitoring requirements and responsibilities including the provision for regular vulnerability assessment and security evaluation of the interconnection. It further defines the guidelines for the emergency system disconnection in the event of a significant security compromise, virus incident, or security threat. In addition, it includes a topological drawing displaying the network architecture configuration of the routers, firewalls, servers, and application platforms for the SOLNET-ESN interconnection. This agreement was signed by both parties

8. As part of the C&A process for SOLNET, and to obtain independent verification of its current operational safety level, the Office of the Solicitor contracted with SeNet

International Corporation (SeNet) to evaluate SOLNET and provide a report of its findings. SeNet reviewed and verified the system categorization based on guidance from NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004* and Federal Information Processing Standards199, *Standards for Security Categorization of Federal Information and Information Systems, 2004 February*; and reviewed and verified the system accreditation boundary. SeNet conducted an assessment of management, operational, and technical security controls for SOLNET based on NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems, Rev. 1, December 2006*, by performing the following steps:

- conducting a System Test & Evaluation ;
- performing a Risk Assessment;
- updating the System Security Plan with the results of the System Test & Evaluation; and
- documenting security control deficiencies.

9. SeNet produced a report that identified two system vulnerabilities and recommended that the system be fully authorized to operate subject to their remediation. Both vulnerabilities identified by SeNet have been fully resolved.

10. I submitted the CAP documentation relative to SOLNET and the most recent SOLNET C&A documentation to the Chief Information Officer of the Department of the Interior. Upon review, the Chief Information Officer of the Department found that (a) the CAP and C&A efforts were complete; (b) the proposed interconnection terms and requirements were adequately planned and documented; (c) SOLNET did not have open

any high risk vulnerabilities; (d) adequate corrective plans were developed to reduce or eliminate open lower-risk vulnerabilities.

11. In order to comply with the maintenance and monitoring requirements of the CAP, regular security compliance reviews will be conducted to evaluate SOLNET and report on vulnerabilities and corrective actions. Automated port and vulnerability scans designed to discover new vulnerabilities, or to validate closure of previously discovered vulnerabilities, will be conducted at least monthly. Vulnerabilities and weaknesses will be recorded in a report that categorizes the risks as "High Risk", Medium Risk", or "Low Risk" and the Plan of Actions and Milestones will be updated accordingly. A comprehensive security test designed to validate the effectiveness of the security controls documented within the SOLNET Interconnection Security Agreement will be conducted at least annually.

12. I have advised the Solicitor, as the Designated approving Authority for SOLNET, that security controls for SOLNET have been assessed using appropriate verification and validation techniques and procedures; and that the security controls have been implemented correctly and are effective.

13. It is my opinion that the security of SOLNET is adequate to protect the information associated with that system, commensurate with the risks to which it is exposed. Accordingly, I recommend that the Chief Information Officer of the Department of the Interior give his approval for interconnection between SOLNET and ESN.

I declare that the foregoing is true and accurate, to the best of my knowledge, information, and belief.

12/20/2007
Date

Craig Littlejohn
Chief Information Officer
Office of the Solicitor

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL et al.,	)	
	)	
Plaintiffs,	)	Case No. 1: 96CV01285
	)	
v.	)	(Judge Robertson)
	)	
DIRK KEMPTHORNE,	)	
Secretary of the Interior, et al.,	)	
	)	
Defendants	)	

REVISED DECLARATION OF MICHAEL HOWELL

I, Michael Howell, declare as follows:

1. I am the Chief Information Officer of the United States Department of the Interior (the Department). My responsibilities in this position include managing the Office of the Chief Information Officer (OCIO), setting Departmental policies and guidance for information resources and information technology (IT) management, and overseeing the implementation of those functions. It is also my responsibility to ensure proper execution of the policy outlined in the *Department of the Interior Connection Approval Process* (CAP), which establishes a uniform procedure for bureaus and offices to utilize when seeking interconnections between Department IT systems.

2. The CAP, in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-47 *Security Guide for Interconnecting Information Technology Systems*, is the standardized policy of the Department for requesting and granting

authorization to establish interconnections between Department IT systems. The CAP is based upon and complies with the requirements and guidance in the Department *Certification and Accreditation Guide*; the Department Office of Chief Information Officer Bulletin *Interconnecting Department of the Interior Information Technology Systems with External Entities*; and other applicable IT security regulations and policies.

3. The CAP provides for continuous security management practice in four distinct phases: planning, implementation, maintenance and monitoring, and termination. Each phase includes defined objectives and tasks and identifies a responsible party for each of them. The CAP defines measures of performance to assure that adequate IT system security controls are implemented and tested, that risks are properly assessed, that reasonable corrective actions are documented, and that security plans are maintained and appropriately updated.

4. The Office of the Solicitor proposed that its IT system known as SOLNET be permitted to establish an interconnection with the Department's Enterprise Service Network (ESN), which provides network services, including Internet access, to Interior bureaus and offices. SOLNET provides general IT services to the Office of the Solicitor such as email and file sharing. ESN is the gateway through which Department bureaus and offices may access the Internet.

5. Consistent with the planning phase of the CAP, the Office of the Solicitor submitted for my review a Memorandum of Understanding and Interconnection Security Agreement between the Department and the Office of the Solicitor that document the requirements and expectations of each with regard to security and operations of ESN and SOLNET, as

well as the most recent Certification and Accreditation (C&A) package for SOLNET. In compliance with NIST Special Publication 800-37, the C&A package included a System Security Plan, risk assessment reports, a Security Test and Evaluation Report, and a Plan of Action and Milestones.

6. In implementation of the CAP process, my staff in the OCIO conducted an analysis of the above documentation and concluded that the Office of the Solicitor had (a) properly completed the CAP and C&A efforts; (b) adequately planned for and documented the proposed SOLNET interconnection terms and requirements; (c) resolved any open, high risk vulnerabilities; (d) established adequate corrective plans to reduce to an acceptable level or eliminate any open lower-risk vulnerabilities; and (e) appropriately documented the open vulnerabilities.

7. The OCIO office also developed and approved a plan for testing the security of the SOLNET-ESN interconnection. The test plan included procedures designed to identify any technical vulnerabilities in the proposed interconnection and to validate the effectiveness of the security controls documented in the SOLNET Interconnection Security Agreement. The test procedures included network port scans, automated vulnerability scans, password discovery/cracking, network sniffing, evaluation of intrusion detection system capabilities, and virus protection validation. The test plan also included manual evaluation of the configurations of the firewalls, routers, and other network security devices implemented to protect the SOLNET ESN interconnection.

8. In October 2007, the OCIO hired Valador Information Architects, an independent contractor, to implement the test plan described in Paragraph 7. The testing confirmed

the adequacy of the security of the proposed interconnection. Subsequent to its testing, the contractor prepared a Security Test Report that documented each vulnerability found, described the potential impact of each vulnerability, and suggested corrective actions. The two high risk vulnerabilities identified have been mitigated; and the remaining lower risk vulnerabilities are being addressed.

9. As the final step in the implementation phase of the CAP, I reviewed the reports and other materials generated by my staff in the OCIO, by the Office of the Solicitor, and by independent contractors relative to the evaluations conducted during the connection approval process. I determined that the existing security controls for both SOLNET and the ESN are adequate, commensurate with the potential risks to which they are exposed, to protect the information associated with those systems; and that they meet Department C&A and CAP requirements.

10. I also reviewed all of the open vulnerabilities documented in the SOLNET Plan of Action and Milestones and their corrective action status and determined that the risk associated with those vulnerabilities was at an acceptable level.

11. Consistent with the maintenance and monitoring phase of the CAP, regular security compliance reviews will be conducted to evaluate SOLNET and ESN security and report on vulnerabilities and corrective actions. Automated port and vulnerability scans designed to discover new vulnerabilities, or to validate closure of previously discovered vulnerabilities, will be conducted at least monthly. Vulnerabilities and weaknesses will be recorded in a report that categorizes their criticality as "High", "Medium," or "Low;" and the SOLNET Plan of Action and Milestones will be updated accordingly. A

comprehensive security test designed to validate the effectiveness of the security controls documented within the SOLNET Interconnection Security Agreement will be conducted at least annually.

12. Based on my review of the documentation of the completion of the CAP by the Office of the Solicitor with regard to SOLNET, I have advised the Associate Deputy Secretary of the Interior that the SOLNET-ESN interconnection has, to the best of my knowledge, adequate security controls in place commensurate with the potential risks; and I recommend that the interconnection be approved.

I declare that the foregoing is true and accurate, to the best of my knowledge, information, and belief.

12/20/07
Date

Michael Howell
Michael Howell
Chief Information Officer
Department of the Interior

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL et al.,	)	
	)	
Plaintiffs,	)	
	)	Case No. 1: 96CV01285
v.	)	
	)	(Judge Robertson)
DIRK KEMPTHORNE,	)	
Secretary of the Interior, et al.,	)	
	)	
Defendants.	)	

REVISED DECLARATION OF DAVID L. BERNHARDT

I, David L. Bernhardt, to the best of my knowledge, information, and belief, declare as follows:

1. I am the Solicitor of the United States Department of the Interior (the Department).
2. Under the Federal Information Management Security Act, I am the agency official responsible for proper assessment of the level of security protection necessary for the information technology system known as SOLNET, after considering potential risks and the magnitude of harm.
3. I have been briefed by the Chief Information Officer for the Department and by the Chief Information Officer for the Office of the Solicitor with regard to the security measures in place for SOLNET. These Officers advised me that the security controls for SOLNET have been assessed using appropriate verification and validation techniques and procedures; and that the security controls have been implemented correctly and are effective.

4. Based on the advice and recommendations of these two Officers, I have determined that the security controls and plans in place for SOLNET provide adequate security, commensurate with the risks and magnitude of the harm resulting from potential unauthorized access, to protect the information associated with the system.

12/20/2007
Date

David L. Bernhardt, Solicitor

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL et al.,	)	
	)	
Plaintiffs,	)	
	)	Case No. 1: 96CV01285
v.	)	
	)	(Judge Robertson)
DIRK KEMPTHORNE,	)	
Secretary of the Interior, et al.,	)	
	)	
Defendants.	)	

REVISED DECLARATION OF JAMES E. CASON

I, James E. Cason, to the best of my knowledge, information, and belief, declare as follows:

1. I am the Associate Deputy Secretary of the United States Department of the Interior (Department).
2. The Department of the Interior has established a Connection Approval Process (CAP) which provides a uniform process through which a Department bureau or office may seek approval for interconnection between information technology (IT) systems. The CAP is the standardized policy of the Department for requesting and granting authorization to establish such interconnections. It requires specific procedures for thorough analysis and testing of the risks and security measures of any IT system proposed for interconnection, and results in extensive documentation of the implementation and completion of those procedures.
3. The Office of the Solicitor proposed interconnection of its information technology system, known as SOLNET, to the Internet through the Department's Enterprise Network System (ESN). The Chief Information Officer of the Office of the Solicitor and the Chief

Information Officer for the Department of the Interior, with the assistance of their staffs and contractors, undertook to accomplish the requirements of the CAP with regard to the proposed interconnection of SOLNET.

4. After careful review of documentation submitted to me by those Officers for the proposed SOLNET-ESN interconnection, and based upon their advice and recommendations, I have determined that the security controls and plans in place for SOLNET and ESN provide adequate security, commensurate with the risk and magnitude of the harm resulting from potential unauthorized access, to protect the information associated with those systems. Accordingly, I intend to authorize the proposed interconnection between SOLNET and ESN, subject to approval by the District Court.

12/20/07
Date

James E. Cason
James E. Cason
Associate Deputy Secretary