

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.)
)
 Plaintiffs,)
)
 v.)
)
 DIRK KEMPTHORNE, Secretary of the)
 Interior, et al.)
)
 Defendants.)

Case No. 1:96CV01285
(Judge Robertson)

**INTERIOR DEFENDANTS’ MOTION FOR ORDER THAT
THE OFFICE OF THE SOLICITOR INFORMATION TECHNOLOGY
SYSTEM MAY BE RECONNECTED TO THE INTERNET**

The Consent Order Regarding Information Technology Security (“the Consent Order”) entered on December 17, 2001 (Dkt. No. 1063) provided a procedure for the reconnection to the Internet of Department of the Interior (“Interior”) Information Technology (“IT”) systems which house or provide access to individual Indian trust data (“IITD”) based upon a determination that the system adequately secures the data contained therein.¹ Consent Order at 7.

The Consent Order required Interior to provide seventy-two hours notice to the Special Master and Plaintiffs of its intent to reconnect to the Internet an IT system housing or providing access to IITD and its plan was to be supported by “appropriate documentation.” Consent Order at 7. Under the Consent Order procedure, the Special Master could “object” to the plan and the reconnection would not be permitted unless the “objections” were resolved. *Id.* If Interior and the Special Master could not resolve the “objections,” the Consent Order also provided for the

¹ The Consent Order has other provisions for systems not housing or accessing IITD and for temporary connections for testing and other purposes.

resolution of “objections” by the Court. Id.

Defendants moved to vacate the Consent Order on March 19, 2007, asserting that “substantial changes in the law and the undisputed facts since entry of the Consent Order render it no longer appropriate or justified, as a matter of law.” Defendants’ Motion to Vacate Consent Order Regarding Information Technology Security at 1 (Mar. 29, 2007) (Dkt. No. 3299).² The Court denied the motion without prejudice on May 14, 2007. However, the Court stated:

I think we have kind of a chicken/egg situation here. I don't quite understand the argument that you can't even prepare to connect something while the consent order is in place. I think there's a good deal of merit to the government's position that the consent order is no longer justified, and certainly doesn't work the way it was intended to work. But I don't see why Interior can't go ahead with its plans to connect these bureaus, and when you're ready, come to me and say, "I want to connect the bureau." And I'm probably going to say yes, because I'm going to look at Cobell XVIII and say, "I don't really have the -- the Court of Appeals doesn't want me to tinker around with this." But you haven't shown me -- you haven't made the requisite showing that you have any security. You haven't filed the IT reports, you haven't -- you say, "Oh, yeah, we have security," but you tell me that you're not even ready to connect the bureaus to the Internet. All this consent decree really does is to stop you at the last step of connecting to the IT. There's nothing in this consent decree, is there, that says that you can't prepare to connect.

Transcript, May 14, 2007, page 40. The Court concluded:

Well, if we were working on a clean slate, you could just go ahead and do it. But we're not. We have a consent decree. So I'm going to deny the motion to vacate, but without prejudice. And when 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.

Id. at 41.

² Plaintiffs opposed the motion. Memorandum in Opposition to Motion to Vacate Consent Order Regarding Information Technology Security (May 7, 2007) (Dkt. No. 3319).

In accordance with these directions and for the reasons set forth below, Interior Defendants respectfully request that the Court issue an order that the IT system for the Office of the Solicitor (known as “SOLNET”) may be reconnected to the Internet. The attached documentation demonstrates that Interior has determined that adequate security for the data housed or accessed by SOLNET will be provided and that it is in compliance with the applicable standards found in information security guidance issued by the Office of Management and Budget (“OMB”) and the National Institute of Standards and Technology (“NIST”). Defendants’ counsel conferred with Plaintiffs’ counsel on November 9, 2007, and Plaintiffs’ counsel stated this motion will be opposed.

DISCUSSION

As discussed below and in the attached declarations, Interior has in place a Connection Approval Process (“CAP”), which provides a uniform process for bureaus to follow in seeking to establish an Internet connection through Interior’s Enterprise Services Network (“ESN”).³ The CAP complies with the requirements and guidance in Interior’s Certification and Accreditation Guide, NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, September 2002, and IT security regulations and policies. Exh. 2,

³ The Office of the Solicitor’s IT system has been operating without access to the Internet or to Interior IT systems with access to the Internet since the entry of the Consent Order. Since December 17, 2001, substantial and significant changes have occurred in the architecture and operation of Interior IT systems. Where Internet access was provided by bureau or office systems in 2001, all Internet access for Interior IT systems is now provided by the ESN, managed at the departmental level and controlled by a state-of-the-art command center in the Washington suburbs. See Cobell v. Norton, 394 F.Supp.2d 164, 259-60 (D.D.C. 2005) (generally describing the ESN as it was being implemented at Interior); Quarterly Report 30 of Interior, at 41-42 (Aug. 1, 2007) (Dkt. No. 3364) (discussing “Computer Security” and ESN perimeter security controls).

Declaration of Michael Howell, CIO, Department of the Interior, at 1-2. The CAP requires continuous security management practice before, during, and after interconnection of one Interior IT system with another. It defines objectives and tasks and identifies responsible parties for each, and 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. Id. at 2.

I. The Chief Information Officers of the Department of the Interior and the Solicitor's Office Evaluated SOLNET and Found it to be Adequately Secure.

The CAP has been satisfactorily completed with regard to SOLNET. Consistent with the requirements of the CAP, both the Chief Information Officer ("CIO") for the Office of the Solicitor and the Departmental CIO reviewed the connection proposal and concluded that the security controls in place for SOLNET, are adequate and commensurate with the risks to which the system is exposed. See Exh. 1, Declaration of Craig Littlejohn; CIO, Office of the Solicitor; Exh. 2 at 2-5.

In addition to the review by the Solicitor CIO, the Office of the Solicitor sought independent third-party verification of the current operational safety level of SOLNET through a contract with SeNet International Corporation ("SeNet"). Exh. 1 at 5. In April 2007, SeNet reviewed and verified the system categorization based on NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004 and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004. Exh. 1 at 4. SeNet also 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;⁴
- Performing a Risk Assessment;⁵
- Updating the System Security Plan⁶ with the results of the System Test evaluation; and
- Documenting security control deficiencies.

SeNet's report identified two high-risk system vulnerabilities and recommended that SOLNET be fully authorized to operate subject to remediation of these high risk vulnerabilities. Those

⁴ NIST SP 800-42 describes Security Test and Evaluation ("ST&E") as:

[A]n examination or analysis of the protective measures that are placed on an information system once it is fully integrated and operational. The objectives of the ST&E are to:

- Uncover design, implementation and operational flaws that could allow the violation of security policy
- Determine the adequacy of security mechanisms, assurances and other properties to enforce the security policy
- Assess the degree of consistency between the system documentation and its implementation.

The scope of an ST&E plan typically addresses computer security, communications security, emanations security, physical security, personnel security, administrative security, and operations security.

Section 2.1.1, p. 2.2 (<http://csrc.nist.gov/publications/PubsSPs.html>).

⁵ "Risk Assessment" is "the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis." NIST SP 800-30, Glossary, p. E-2.

⁶ A "System Security Plan" is a "[f]ormal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements." NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Glossary, p. 56.

vulnerabilities have been fully resolved. Exh. 1 at 4.

II. The Solicitor, the Designated Representative of the Authorizing Official, Determined that the Proposed SOLNET Interconnection is Adequately Secure.

The Federal Information Management Security Act (“FISMA”) provides that the head of an agency:

shall...be responsible for...providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of –

information collected or maintained by or on behalf of an agency; and

information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

44 U.S.C. § 3544(a)(1)(A)(emphasis added); see Cobell v. Kempthorne, 455 F.3d 301, 313 (D.C. Cir. 2006). The Solicitor is the Authorizing Official Designated Representative⁷ who must assess the level of security protections necessary for SOLNET, after considering the potential risks and the magnitude of harm. The Solicitor has made those determinations. Exh. 3, Declaration of David Bernhardt.⁸

⁷ The “Authorizing Official” is the “Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.” NIST SP 800-37 at 51. The “Authorizing Official Designated Representative” is the “Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.”

⁸ Solely because of this litigation, Interior requires additional review of reconnection proposals not required for other IT-related issues. This review is provided by the Associate Deputy Secretary, James Cason. He reviewed the SOLNET proposal and, based on satisfactory completion of the CAP with respect to the proposed SOLNET interconnection and the determination of the Solicitor that the level of security necessary for that system has been achieved, he authorized interconnection of SOLNET subject to action by this Court. Exh. 4, Declaration of James E. Cason.

CONCLUSION

For the foregoing reasons, Interior Defendants request that the Court issue an order that Interior Defendants may proceed to reconnect SOLNET to the Internet.

Dated: November 9, 2007

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

MICHAEL F. HERTZ
Deputy Assistant Attorney General

J. CHRISTOPHER KOHN
Director

/s/ Robert E. Kirschman, Jr.
ROBERT E. KIRSCHMAN, JR.
Deputy Director
(D.C. Bar No. 406635)
JOHN WARSHAWSKY
Senior Trial Counsel
(D.C. Bar No. 417170)
GLENN D. GILLET
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 616-0238
Facsimile: (202) 514-9163

CERTIFICATE OF SERVICE

I hereby certify that, on November 9, 2007 the foregoing *Interior Defendants' 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,)
)
 v.)
)
 DIRK KEMPTHORNE,)
 Secretary of the Interior, et al.,)
)
 Defendants.)

Case No. 1: 96CV01285

(Judge Robertson)

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 antivirus/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. In April 2007, 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 Standards 199, *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.

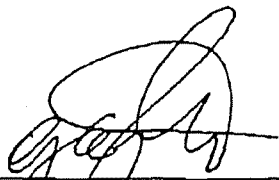
9. SeNet produced a report that identified two high risk system vulnerabilities and recommended that the system be fully authorized to operate subject to their remediation. Both vulnerabilities identified by SeNet have been fully resolved.
10. I submitted the CAP documentation relative to SOLNET and 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.

Date

11/7/2007



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)	

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.

11/7/07
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,)

v.)

DIRK KEMPTHORNE,)

Secretary of the Interior, et al.,)

Defendants.)

Case No. 1: 96CV01285

(Judge Robertson)

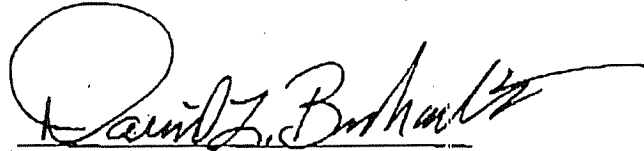
DECLARATION OF DAVID L. BERNHARDT

I, David L. Bernhardt, 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.

11/7/2007
Date


David L. Bernhardt
David L. Bernhardt, Solicitor

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.)

DECLARATION OF JAMES E. CASON

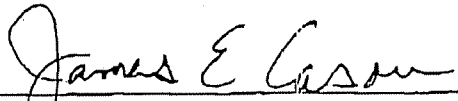
I, James E. Cason, declare as follows:

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.

11/7/07
Date


James E. Cason
Associate Deputy Secretary
United States Department of the Interior

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

ORDER

This matter comes before the Court on *Interior Defendants' Motion for Order That the Office of the Solicitor Information Technology System May Be Reconnected to the Internet.*

[_____] Upon consideration of the Defendants' Motion, Plaintiffs' Opposition, and any Reply thereto, and the entire record of this case, it is hereby

ORDERED that the Motion is, GRANTED.

SO ORDERED

Hon. James Robertson
UNITED STATES DISTRICT JUDGE

Date: _____