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 AN ORDER (1) AUTHORIZING THE RECONNECTION TO THE INTERNET OF INFORMATION TECHNOLOGY SYSTEMS OF THE BUREAU OF INDIAN AFFAIRS, THE OFFICE OF HEARING AND APPEALS, AND THE OFFICE OF THE SPECIAL TRUSTEE, (2) CONFIRMING THAT THE OFFICE OF HISTORICAL TRUST ACCOUNTING MAY CONNECT ITS INFORMATION TECHNOLOGY SYSTEM TO THE INTERNET, AND (3) VACATING THE DECEMBER 17, 2001 CONSENT ORDER REGARDING INFORMATION TECHNOLOGY SECURITY

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 to reconnect was to be supported by "appropriate documentation."

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

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 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. 19, 2007) (Dkt. No. 3299).[2] The Court denied the motion without prejudice on May 14, 2007. In doing so, 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

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

> 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.

In accordance with these directions and for the reasons set forth below, Interior Defendants respectfully request that the Court issue an Order providing as follows:

(1) that the IT system networks of the Bureau of Indian Affairs ("BIA"), the Office of Hearings and Appeals ("OHA"), and the Office of the Special Trustee ("OST") may be reconnected to the Internet, based upon the attached documentation, which demonstrates that Interior has determined that adequate security for the data housed or accessed by these networks will be provided and that they are 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");

(2) that the OLE network of the Office of Historical Trust Accounting ("OHTA") may be connected to the Internet,[3] based upon the attached documentation, which demonstrates that Interior has determined that adequate security for the data housed or accessed by this network will be provided and that it is in compliance with the applicable standards found in information security guidance issued by OMB and NIST; and

(3) that the Consent Order is vacated because, if the Court grants the relief sought in paragraph (1), above, and in the similar motion previously filed with regard to the IT system network of the Office of the Solicitor, 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 SOLNet"), there will be no Interior IT systems remaining disconnected pursuant to the Consent Order and, therefore, the Consent Order will serve no further purpose.

---

[3] "OLE" is an acronym comprised of some of the letters within the network's name, the OHTA Local Area Network Infrastructure Environment. See Exhibit 9 (Declaration of Carl Huls, CIO of OHTA), ¶ 1 (attached to this motion). Unlike the networks for BIA, OHA, and OST, OHTA's OLE network was not in existence at the time of the Consent Order and, accordingly, was not disconnected as a result of the Consent Order. Accordingly, while the Consent Order does not prevent the connection of the OHTA network, Interior Defendants seek an Order confirming that the connection of this IT system is permissible for reasons comparable to those justifying reconnection of the BIA, OHA, and OST networks.

Defendants' counsel conferred with Plaintiffs' counsel on February 11, 2008, and Plaintiffs' counsel stated this motion would be opposed.

DISCUSSION

This motion addresses four IT system networks currently disconnected from Internet access. Three of the systems – BIA's network, OHA's network (referred to as "OHANet"), and OST's network (referred to as "OSTNet") – have been operating without access to the Internet or to any Interior IT systems with access to the Internet since the entry of the Consent Order on December 17, 2001. The fourth system – OHTA's OLE network – became operational after entry of the Consent Order, and while the OLE network was not disconnected from the Internet as a result of the Consent Order (which predated its existence), the OLE network has never been operated with access to the Internet or to any Interior IT systems with access to the Internet.

I. Interior's Architecture and Operation of IT Systems Has Changed Since Entry of the Consent Order, and Interior Now Has a Uniform Process to Review All Decisions Seeking to Establish Internet Connectivity for an IT System

Since entry of the Consent Order on 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 Interior's Enterprise Services Network ("ESN"), managed at the departmental level and controlled by a state-of-the-art command center in the Washington, D.C. 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); Interior Status Report to the Court Number Thirty-One, at 41-42 (Feb. 1, 2008) (Dkt. No. 3506) (discussing "Computer Security" and ESN

perimeter security controls).

Interior has in place a Connection Approval Process ("CAP"), which provides a uniform process for bureaus and offices to follow in seeking to establish an Internet connection through Interior's ESN.[4] 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. Exhibit 1 (Declaration of Michael Howell, Chief Information Officer ("CIO") for Interior), ¶¶ 1-2.[5] 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; 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., ¶ 3.

II. The Chief Information Officers of the Department of the Interior and BIA Have Evaluated BIA's Network and Found It To Be Adequately Secure, and BIA's Director – the Designated Representative of the Authorizing Official Under FISMA – Has Determined That the Proposed BIA Network Interconnection Is Adequately Secure

The CAP has been satisfactorily completed with regard to BIA's network. Consistent with the requirements of the CAP, both BIA's CIO and the Departmental CIO reviewed BIA's reconnection proposal and concluded that the security controls in place for the BIA network are

---

[4] The CAP was previously described in Interior Defendants' Motion to Reconnect SOLNet at 3-4 and is described again, below.

[5] "Exhibit" refers to an exhibit attached to this motion.

adequate and commensurate with the risks to which the system is exposed. Exhibit 1, ¶¶ 4-12; Exhibit 3 (Declaration of Sanjeev Bhagowalia, CIO for BIA).

In addition to the review by BIA's CIO, BIA has considered the findings of SeNet International Corporation ("SeNet"), the independent contractor that evaluated BIA's network as part of the system's Certification and Accreditation ("C&A") process. Exhibit 3, ¶ 8. In August 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. Exhibit 3, ¶ 8. SeNet also reviewed and verified the system accreditation boundary. Id. SeNet further conducted an assessment of management, operational, and technical security controls for the BIA network based on NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Rev. 1, December 2006, by performing the following steps:

- Conducting Security Testing and Evaluation;[6]

---

[6] NIST SP 800-42 describes Security Testing 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.

- Performing a Risk Assessment;[7]
- Updating the System Security Plan[8] with the results of the Security Testing and Evaluation; and
- Documenting security control deficiencies.

Exhibit 3, ¶ 8.

SeNet's report identified eleven high-risk system vulnerabilities and recommended that BIA's network be fully authorized to operate, subject to remediation of these high risk vulnerabilities. Exhibit 3, ¶ 9. Since the issuance of SeNet's report, all of the high-risk vulnerabilities have been mitigated. Id.

As was previously explained in Interior Defendants' Motion to Reconnect SOLNet at 6, the statute which prescribes the standards for IT security at federal agences, 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

---

Section 2.1.1, p. 2-2 (http://csrc.nist.gov/publications/PubsSPs.html).

[7] "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.

[8] 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.

agency or other organization on behalf of an agency; . . . .

44 U.S.C. § 3544(a)(1)(A); see Cobell v. Kempthorne, 455 F.3d 301, 313 (D.C. Cir. 2006). The Director of BIA is the Authorizing Official Designated Representative[9] who must assess the level of security protections necessary for BIA's network, after considering the potential risks and the magnitude of harm. Exhibit 4 (Declaration of Jerry Gidner, Director of BIA), ¶¶ 1-2. As described in his declaration, BIA's Director has made this assessment. Id., ¶¶ 3-4.

Finally, as explained in Interior Defendants' Motion to Reconnect SOLNet at 6 note 8, while not mandated by FISMA, 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. Mr. Cason reviewed the BIA network proposal and, based on satisfactory completion of the CAP with respect to the proposed BIA network interconnection and the determination of BIA's Director that the level of security necessary for that system has been achieved, he has authorized interconnection of BIA's network, subject to action by this Court. Exhibit 2 (Declaration of James E. Cason).

III. The Chief Information Officers of the Department of the Interior and OHA Have Evaluated OHANet and Found It To Be Adequately Secure, and OHA's Designated Representative of the Authorizing Official Under FISMA Has Determined That the Proposed OHANet Interconnection Is Adequately Secure

The CAP has been satisfactorily completed with regard to OHA's network, OHANet.

---

[9] 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." Id.

Consistent with the requirements of the CAP, both OHA's CIO and the Departmental CIO reviewed OHA's reconnection proposal and concluded that the security controls in place for OHANet are adequate and commensurate with the risks to which the system is exposed. Exhibit 1, ¶¶ 4-12; Exhibit 5 (Declaration of Charles E. Breece, CIO for OHA).

In addition to the review by OHA's CIO, OHA has considered the findings of G&B Solutions, Inc. ("G&B"), the independent contractor that evaluated OHANet as part of the system's June 2006 re-accreditation. Exhibit 5, ¶ 8. In December 2005, G&B 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. Exhibit 5, ¶ 8. SeNet also reviewed and verified the system accreditation boundary. Id. G&B further conducted an assessment of management, operational, and technical security controls for OHANet based on NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Rev. 1, December 2006, by performing the following steps:

- Conducting Security Testing and Evaluation;
- Performing a Risk Assessment;
- Updating the System Security Plan with the results of the Security Testing and Evaluation; and
- Documenting security control deficiencies.

Exhibit 5, ¶ 8.

G&B's report identified two high-risk system vulnerabilities and recommended that

OHANet be fully authorized to operate, subject to remediation of these high risk vulnerabilities. Exhibit 5, ¶ 9. Since the issuance of G&B's report, one of the two high-risk vulnerabilities has been eliminated and the other has been mitigated. Id.

The Deputy Assistant Secretary for Human Capital, Performance, and Partnerships is the Authorizing Official Designated Representative who must assess the level of security protections necessary for OHANet, after considering the potential risks and the magnitude of harm. Exhibit 6 (Declaration of Paul Hoffman, Deputy Assistant Secretary for Human Capital, Performance, and Partnerships), ¶¶ 1-2. As described in his declaration, the Deputy Assistant Secretary for Human Capital, Performance, and Partnerships has made this assessment. Id., ¶¶ 3-4.

Finally, Interior's additional review by the Associate Deputy Secretary, James Cason, has been performed. Mr. Cason reviewed the OHANet proposal and, based on satisfactory completion of the CAP with respect to the proposed OHANet interconnection and the determination of the Deputy Assistant Secretary for Human Capital, Performance, and Partnerships that the level of security necessary for that system has been achieved, authorized interconnection of OHANet subject to action by this Court. Exhibit 2.

IV. The Chief Information Officers of the Department of the Interior and OST Have Evaluated OSTNet and Found It To Be Adequately Secure, and OST's Designated Representative of the Authorizing Official Under FISMA Has Determined That the Proposed OSTNet Interconnection Is Adequately Secure

The CAP has been satisfactorily completed with regard to OST's network, OSTNet. Consistent with the requirements of the CAP, both OST's CIO and the Departmental CIO reviewed OST's reconnection proposal and concluded that the security controls in place for OSTNet are adequate and commensurate with the risks to which the system is exposed.

Exhibit 1, ¶¶ 4-12; Exhibit 7 (Declaration of Robert C. McKenna, CIO for OST).

In addition to the review by OST's CIO, OST has considered the findings of SeNet, the independent contractor that evaluated OSTNet as part of the system's C&A process. Exhibit 7, ¶ 8. In August 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. Exhibit 7, ¶ 8. SeNet also reviewed and verified the system accreditation boundary. Id. SeNet further conducted an assessment of management, operational, and technical security controls for the BIA network based on NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Rev. 1, December 2006, by performing the following steps:

- Conducting Security Testing and Evaluation;
- Performing a Risk Assessment;
- Updating the System Security Plan with the results of the Security Testing and Evaluation; and
- Documenting security control deficiencies.

Exhibit 7, ¶ 8.

SeNet's report identified no high-risk system vulnerabilities and recommended that OSTNet be fully authorized to operate. Exhibit 7, ¶ 9

The Special Trustee for American Indians (the "Special Trustee") is the Authorizing Official Designated Representative who must assess the level of security protections necessary for OSTNet, after considering the potential risks and the magnitude of harm. Exhibit 8 (Declaration

of Ross O. Swimmer, Special Trustee for American Indians), ¶¶ 1-2. As described in his declaration, the Special Trustee has made this assessment. Id., ¶¶ 3-4.

Finally, Interior's additional review by the Associate Deputy Secretary, James Cason, has been performed. Mr. Cason reviewed the OSTNet proposal and, based on satisfactory completion of the CAP with respect to the proposed OSTNet interconnection and the determination of the Special Trustee that the level of security necessary for that system has been achieved, authorized interconnection of OSTNet subject to action by this Court. Exhibit 2.

V. The Chief Information Officers of the Department of the Interior and OHTA Have Evaluated OHTA's Local Area Network, Known as "OLE," and Found It To Be Adequately Secure, and OHTA's Designated Representative of the Authorizing Official Under FISMA Has Determined That the Proposed OLE Interconnection Is Adequately Secure

The CAP has been satisfactorily completed with regard to OHTA's network, OLE. Consistent with the requirements of the CAP, both OHTA's CIO and the Departmental CIO reviewed OHTA's reconnection proposal and concluded that the security controls in place for OLE are adequate and commensurate with the risks to which the system is exposed. Exhibit 1, ¶¶ 4-12; Exhibit 7 (Declaration of Carl Huls, CIO for OHTA).

In addition to the review by OHTA's CIO, OHTA has considered the findings of Rollout Systems, Inc. ("Rollout Systems"), the independent contractor that evaluated OLE as part of the system's C&A process. Exhibit 8, ¶ 8. In August 2007, Rollout Systems 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.

Exhibit 9, ¶ 8. Rollout Systems also reviewed and verified the system accreditation boundary. Id. Rollout Systems further conducted an assessment of management, operational, and technical security controls for the BIA network based on NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Rev. 1, December 2006, by performing the following steps:

- Conducting Security Testing and Evaluation;
- Performing a Risk Assessment;
- Updating the System Security Plan with the results of the Security Testing and Evaluation; and
- Documenting security control deficiencies.

Exhibit 9, ¶ 8.

Rollout Systems's report identified two high-risk system vulnerabilities and recommended that OHANet be fully authorized to operate, subject to remediation of these high risk vulnerabilities. Exhibit 9, ¶ 9. Since the issuance of G&B's report, both of the high-risk vulnerabilities has been eliminated. Id.

The Special Trustee is the Authorizing Official Designated Representative who must assess the level of security protections necessary for OLE, after considering the potential risks and the magnitude of harm. Exhibit 10 (Declaration of Ross O. Swimmer, Special Trustee for American Indians), ¶¶ 1-2. As described in his declaration, the Special Trustee has made this assessment. Id., ¶¶ 3-4.

Finally, Interior's additional review by the Associate Deputy Secretary, James Cason, has been performed. Mr. Cason reviewed the OLE proposal and, based on satisfactory completion of the CAP with respect to the proposed OLE interconnection and the determination of the Special

Trustee that the level of security necessary for that system has been achieved, authorized interconnection of OLE subject to action by this Court. Exhibit 2.

VI. The Court Should Vacate the Consent Order

For the reasons set forth above and previously with regard to Interior Defendants' Motion to Reconnect SOLNet, the Court should allow Interior to reconnect the IT Systems of the Solicitor, BIA, OHA, and OST. Upon doing so, no Interior IT systems will remain disconnected pursuant to the Consent Order and, therefore, the Consent Order will serve no further purpose.

It is well-recognized that an injunction, such as the Consent Order, should be modified or vacated if required by changes in the underlying law or facts. As one district court has explained:

> [C]ourts have continuing jurisdiction to terminate, dissolve, vacate, or modify an injunction or an interlocutory order in the event that changed circumstances require it. The Court's power may arise from a change of law or a change of fact.

University of Hawaii Professional Assembly v. Cayetano, 125 F. Supp. 2d 1237, 1240 (D. Haw. 2000) (citing, inter alia, In re Detroit Auto Dealers Ass'n, Inc., 84 F.3d 787, 789 (6th Cir. 1996), and United States v. Oregon, 769 F.2d 1410, 1416 (9th Cir. 1985)); see also Cobell v. Norton, 274 F. Supp. 2d 111, 133 (D.D.C. 2003) ("It is certainly true that one of the grounds on which a court may modify a consent decree is that a change in controlling law renders the decree impermissible.") (citing Rufo v. Inmates of Suffolk County, 502 U.S. 367, 388 (1992)), vacated on other grounds, 391 F.3d 251 (D.C. Cir. 2004). The reconnection of all previously disconnected IT systems justifies vacating the Consent Order.[10]

[10] For a discussion about the changes in the law since entry of the Consent Order, Interior Defendants further respectfully refer the Court to the discussion in Defendants' Motion to Vacate Consent Order Regarding Information Technology Security at 14-19 (Mar. 29, 2007) (Dkt. No. 3299).

Conclusion

For the foregoing reasons, Interior Defendants respectfully request this Court to issue an Order providing (1) that the IT system networks of BIA, OHA, and OST may be reconnected to the Internet, (2) that OHTA's OLE network may be connected to the Internet, and (3) that the December 17, 2001 Consent Order is vacated because it serves no further purpose in light of the changes in facts and law since its entry.

Dated: February 11, 2008

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.
Deputy Director
(D.C. Bar No. 406635)
JOHN WARSHAWSKY
Senior Trial Counsel
(D.C. Bar No. 417170)
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 February 11, 2008 the foregoing *Interior Defendants' Motion for an Order (1) Authorizing the Reconnection to the Internet of Information Technology Systems of the Bureau of Indian Affairs, the Office of Hearing and Appeals, and the Office of the Special Trustee, (2) Confirming That the Office of Historical Trust Accounting May Connect its Information Technology System to the Internet, and (3) Vacating the December 17, 2001 Consent Order Regarding Information Technology Security* 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	)	

DECLARATION OF MICHAEL HOWELL

I, Michael Howell, to the best of my knowledge, information, and belief 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

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 individual IT systems for the Bureau of Indian Affairs, the Office of Hearings and Appeals, the Office of Historical Trust Accounting, and the Office of the Special Trustee for American Indians (collectively known as "TrustNet"), seek permission to establish an interconnection with the Department's Enterprise Service Network (ESN). ESN provides network services, including Internet access, to Interior bureaus and offices. The individual systems that comprise TrustNet provide general IT services to the respective bureau or office such as email and file sharing. ESN is the gateway through which TrustNet, as a whole, may access the Internet.

5. Consistent with the planning phase of the CAP, each TrustNet bureau submitted for my review a Memorandum of Understanding and Interconnection Security Agreement between the Department and that bureau, which documents the requirements and expectations of each bureau with regard to security and operations of ESN and that system. In addition, each TrustNet bureau submitted its most recent Certification and Accreditation (C&A) package for my review. In compliance with NIST Special Publication 800-37, each C&A package included a System Security Plan, a risk assessment report, a Security Test and Evaluation Report, and a Plan of Action and Milestones.

6. In implementing the CAP process, my staff in the OCIO conducted an analysis of the above documentation and concluded that each TrustNet bureau had (a) properly completed the CAP and C&A efforts; (b) adequately planned for and documented the proposed interconnection terms and requirements; (c) eliminated 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 also developed and approved a plan for testing the security of the TrustNet-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 each bureau's Interconnection Security Agreement. The test procedures included network port scans, automated vulnerability scans, password discovery/cracking, network sniffing, evaluation of intrusion detection

evaluation of the configurations of the firewalls, routers, and other network security devices implemented to protect the interconnections.

8. In October 2007, the OCIO hired Valador, 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. None of the vulnerabilities identified were considered to be "high-risk."

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 individual TrustNet bureaus, and by the independent contractor relative to the evaluations conducted during the Connection Approval Process. I determined that the existing security controls for TrustNet and ESN are adequate, commensurate with the potential risks to which the systems 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 each TrustNet bureau's Plan of Action and Milestones, and reviewed 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 the security of each TrustNet system and ESN, and report on vulnerabilities and corrective actions. Automated port and vulnerability scans designed to discover new vulnerabilities, or to validate closure of

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 reports that categorize their criticality as "High," "Medium," or "Low;" and the applicable system's Plan of Action and Milestones will be updated accordingly. A comprehensive security test designed to validate the effectiveness of the security controls documented within each TrustNet system's Interconnection Security Agreement will be conducted at least annually.

12. Based on my review of the documentation of the completion of the CAP by each TrustNet bureau, I have advised the Associate Deputy Secretary of the Interior that the TrustNet-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.

12/21/07
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.	)	

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 Bureau of Indian Affairs (BIA), Office of Hearings and Appeals (OHA), Office of Historical Trust Accounting (OHTA), and Office of the Special Trustee for American Indians (OST) propose interconnection of their information technology systems, known

collectively as TrustNet, with the Department's Enterprise Network System (ESN). ESN provides network services to Department bureaus and offices, and will be the gateway through which TrustNet as a whole may access the Internet. The Chief Information Officers of BIA, OHA, OHTA, and OST, as well as the Chief Information Officer of the Department, with the assistance of their staffs and contractors, undertook to accomplish the requirements of the CAP with regard to the proposed interconnection of TrustNet with ESN.

4. After careful review of documentation submitted to me by those Officers for the proposed TrustNet-ESN interconnection, and based upon their advice and recommendations, I have determined that the security controls and plans in place for TrustNet 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 TrustNet and ESN, subject to approval by the District Court.

12/21/07
Date

James E Cason
James E. Cason
Associate Deputy Secretary

EXHIBIT 2
Defendants' Motion to Reconnect DoI's
BIA, OHA & OST to the Internet; Allow DoI's
OHTA's OLE to Connect to the Internet; and
Vacate the Dec. 17, 2001 I-T Security Consent Order

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 SANJEEV BHAGOWALIA

I, Sanjeev Bhagowalia, declare that the following is true and correct to the best of my knowledge, information and belief:

1. I am the Chief Information Officer (CIO) for the Bureau of Indian Affairs (BIA), United States Department of the Interior (the Department). My staff of 320 federal and contractor information technology professionals provides support services for the hardware and software for the four (4) Local Area Network (LAN) zones [Northern Zone, Southern Zone, Western Zone, and Eastern Zone] that together comprise the BIA network.
2. The BIA network provides general IT services such as office automation, file sharing, and printer sharing to over 5,000 BIA employees. As CIO, my responsibilities for the BIA network 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 BIA has proposed that its network 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 for the BIA network 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 Certification & Accreditation (C&A) process was completed for each LAN zone; and (3) providing a recommendation on whether to grant approval for the interconnection for the network.

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

6. I also developed an Interconnection Security Agreement for the proposed BIA network interconnection with ESN which defined the technical security requirements and further identified and described the defense-in-depth security controls employed to protect all data in the BIA environment including Individual Trust Data. These security controls include:

    i. an Access Control List on the perimeter access device that strictly controls both inbound and outbound network traffic;

ii. Network-based Intrusion Detection Systems placed throughout the network inspecting both inbound and outbound network traffic;

iii. a stateful inspection firewall stack strictly controlling both inbound and outbound network traffic;

iv. Intrusion Prevention Systems on the core network segment that are capable of identifying viruses, unauthorized equipment and user access, and network traffic anomalies;

v. a security information management system providing collection, collation, and archival of events generated by the servers and security devices for each LAN, as well as provide near real time identification and alerting of malicious, suspicious or anomalous activity;

vi. secure software image deployed on all workstations based on the Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG);

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

viii. automated deployment of system software updates and patches via Microsoft Windows Server Update Service;

ix. current anti-malware software and centralized scheduled updates of signature files;

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 interconnection between ESN and the BIA network. This agreement was signed by both parties.

8. As part of the C&A process for each LAN zone, BIA contracted with SeNet International Corporation (SeNet) to evaluate the BIA network and provide a report of its findings. In August 2007, SeNet reviewed and verified the system categorization for each LAN zone 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 the BIA network 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 11 high risk system vulnerabilities and recommended that the system be fully authorized to operate subject to their remediation. All 11 vulnerabilities identified by SeNet have been mitigated.

10. I submitted to the Chief Information Officer of the Department of the Interior the CAP documentation relative to the BIA network, and the most recent C&A documentation for each LAN zone. 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) the BIA network 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 are conducted to evaluate the BIA network 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, are conducted monthly. Vulnerabilities and weaknesses are recorded in a report that categorizes the risks as "High Risk", "Medium Risk", or "Low Risk" and the Plan of Actions and Milestones are updated accordingly. A comprehensive security test designed to validate the effectiveness of the security controls documented within the BIA network Interconnection Security Agreement will be conducted annually.

12. I have advised the Director of the Bureau of Indian Affairs, as the Designated Approving Authority for the BIA network, that security controls for each LAN zone

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 the BIA network is adequate to protect the information associated with that network, 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 the BIA network and ESN.

12-21-2007
Date

Sanjeev Bhagowalia
Chief Information Officer
Bureau of Indian Affairs

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 JERRY GIDNER

I, Jerry Gidner, to the best of my knowledge, information, and belief declare as follows:

1. I am the Director, Bureau of Indian Affairs (BIA) for the United States Department of the Interior.
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 BIA information technology network, after considering potential risks and the magnitude of harm.
3. I have been briefed by the Chief Information Officer for the BIA with regard to the security measures in place for the BIA network and have been advised that the security controls for the BIA network have been assessed using appropriate verification and validation techniques and procedures; and that security controls have been implemented correctly and are effective.

4. Based on the advice and recommendations of the Chief Information Officer for the BIA, I have determined that the security controls and plans in place for the BIA network provide adequate security, commensurate with the risks and magnitude of the harm resulting from potential unauthorized access, to protect the information associated with the network.

12/21/2007
Date

Jerry Gidner
Director, Bureau of Indian Affairs

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 CHARLES E. BREECE

I, Charles E. Breece, declare that the following is true and correct to the best of my knowledge, information and belief:

1. I am the Chief Information Officer (CIO) for the Office of Hearings and Appeals, United States Department of the Interior (the Department). My staff of three (3) federal and contractor information technology professionals in the Office of Hearings and Appeals provide support services for the hardware and software that comprise the Office of Hearing and Appeals network environment (hereinafter "OHANet").
2. OHANet provides general IT services such as electronic messaging, file sharing, and printer sharing to over 120 Office of Hearings and Appeals employees. As CIO, my responsibilities for OHANet 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 Hearings and Appeals seeks permission for OHANet to 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 Hearings and Appeals 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 OHANet 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 OHANet interconnection and defined the roles, responsibilities, terms, conditions, and expectations of the Department and of the Office of Hearings and Appeals for security and operation of ESN and OHANet. The agreement was signed by both parties.

6. I also developed an Interconnection Security Agreement for the proposed OHANet interconnection which defined the technical security requirements. By implementing the following security controls, OHA uses a defense-in-depth strategy that protects all the data in OHANet including Individual Indian Trust Data. These security controls include:

    i. an access Control List on the perimeter access device that strictly controls both inbound and outbound network traffic;

ii. Intrusion Detection System appliances on each local area network segment, which are capable of identifying unauthorized equipment and user access, and network traffic anomalies;

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

iv. host firewalls on all workstations;

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

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

vii. an automated deployment of system software updates and patches via Microsoft Windows Server Update Services and System Management Server; and

viii. current anti-virus/spyware software and centralized scheduled updates of signature files.

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 OHANet-ESN interconnection. This agreement was signed by both parties.

8. OHA completed the C&A process for OHANet in July 2004. Because OHA changed the OHANet operating system environment in FY 2005, the system was re-accredited in June 2006. As part of the re-accreditation process for OHANet, the Office of Hearings and Appeals contracted with G&B Solutions, Inc. to evaluate OHANet and provide a report of its findings. In December 2005, G&B Solutions, Inc. 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. G&B Solutions, Inc. conducted an assessment of management, operational, and technical security controls for OHANet based on NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems, February 2005*, 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. G&B Solutions, Inc. produced a report that identified two high risk system vulnerabilities and recommended that the system be fully authorized to operate subject to their remediation. Of the two high-risk vulnerabilities identified by G&B Solutions, Inc., one has been eliminated and the other has been mitigated.

10. I submitted the CAP documentation relative to OHANet and the most recent OHANet 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) OHANet 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 are conducted to evaluate OHANet 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, are conducted monthly. Vulnerabilities and weaknesses are recorded in a report that categorizes the risks as "High Risk", "Medium Risk", or "Low Risk" and the Plan of Actions and Milestones are updated accordingly. A comprehensive security test designed to validate the effectiveness of the security controls documented within the OHANet System Security Plan (SSP) will be conducted annually.

12. I have advised the Deputy Assistant Secretary – Human Capital, Performance, and Partnerships, as the Designated Approving Authority for OHANet, that security controls for OHANet 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 OHANet 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 OHANet and ESN.

12/21/07
Date

Charles E. Breece
Charles E. Breece
Chief Information Officer
Office of Hearings and Appeals

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 PAUL HOFFMAN

I, Paul Hoffman, to the best of my knowledge, information, and belief declare as follows:

1. I am the Deputy Assistant Secretary for Human Capital, Performance, and Partnerships of the United States Department of the Interior.
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 of the Office of Hearings and Appeals known as OHANET, after considering potential risks and the magnitude of harm.
3. I have been briefed by the Chief Information Officer for the Office of Hearings and Appeals with regard to the security measures in place for OHANET and have been advised that the security controls for OHANET have been assessed using appropriate verification and validation techniques and procedures; and that security controls have been implemented correctly and are effective.
4. Based on the advice and recommendations of the Chief Information Officer for the Office of Hearings and Appeals, I have determined that the security controls and

plans in place for OHANET 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.

12/21/07
Date

Paul Hoffman
Deputy Assistant Secretary for Human Capital, Performance, and Partnerships

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 ROBERT C. MCKENNA

I, Robert C. McKenna, declare that the following is true and correct to the best of my knowledge, information, and belief:

1. I am the Chief Information Officer (CIO) for the Office of the Special Trustee for American Indians, United States Department of the Interior (the Department). My staff of 27 federal and contractor information technology professionals in the Office of the Special Trustee, Office of the Chief Information Officer, provides support services for the hardware and software that comprise the Office of the Special Trustee network environment (hereinafter "OSTNET").
2. OSTNET provides general IT services such as electronic messages, file sharing, and printer sharing to over 700 employees of the Office of the Special Trustee. As CIO, my responsibilities for OSTNET 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 Special Trustee has proposed that OSTNET 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 Special Trustee 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 OSTNET Certification & Accreditation (C&A) process was completed; and (3) providing a recommendation on whether to grant approval for the interconnection.

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

6. I also executed an Interconnection Security Agreement for the proposed OSTNET interconnection which defined the technical security requirements and further identified and described the defense-in-depth security controls employed to protect all the data in OSTNET including Individual Indian Trust Data. These security controls include:

    i. an access Control List on the perimeter access device that strictly controls both inbound and outbound network traffic;

ii. network based Intrusion Detection Systems strategically placed throughout the network inspecting both inbound and outbound network traffic;

iii. a statefull inspection firewall stack strictly controlling both inbound and outbound network traffic;

iv. an intrusion prevention system on the core network segment, which is capable of identifying viruses, unauthorized equipment and user access, and network traffic anomalies;

v. a security information management system providing collection, collation, and archival of events generated by servers and security devices throughout OSTNET as well as provide near real time identification and alerting of malicious, suspicious or anomalous activity;

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

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

viii. an automated deployment of system software updates and patches via Microsoft Windows Security Update Services and Systems Management Service;

ix. current anti-malware software and centralized scheduled updates of signature files;

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 OSTNET-ESN interconnection. This agreement was signed by both parties.

8. As part of the C&A process for OSTNET, and to obtain independent verification of its current operational safety level, the Office of the Special Trustee contracted with SeNet International Corporation (SeNet) to evaluate OSTNET and provide a report of its findings. In August 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 OSTNET 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 no high-risk system vulnerabilities and recommended that the system be fully authorized to operate.

10. I submitted the CAP documentation relative to OSTNET and the most recent OSTNET 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) OSTNET 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 OSTNET 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 OSTNET Interconnection Security Agreement will be conducted at least annually.

12. I have advised the Special Trustee, as the Designated Approving Authority for OSTNET, that security controls for OSTNET 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 OSTNET 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 OSTNET and ESN.

12/19/07
Date

Robert C. McKenna
Chief Information Officer
Office of the Special Trustee

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 ROSS O. SWIMMER

I, Ross O. Swimmer, to the best of my knowledge, information, and belief declare as follows:

1. I am the Special Trustee for American Indians of the United States Department of the Interior.
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 at Office of the Special Trustee known as OSTNET, after considering potential risks and the magnitude of harm.
3. I have been briefed by the Chief Information Officer for the Office of the Special Trustee with regard to the security measures in place for OSTNET and have been advised that the security controls for OSTNET have been assessed using appropriate verification and validation techniques and procedures; and that security controls have been implemented correctly and are effective.

4. Based on the advice and recommendations of the Chief Information Officer for the Office of the Special Trustee, I have determined that the security controls and plans in place for OSTNET 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.

12/21/07
Date

Ross O. Swimmer
Special Trustee for American Indians

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 CARL HULS

I, Carl Huls, declare that the following is true and correct to the best of my knowledge, information and belief:

1. I am the Chief Information Officer (CIO) for the Office of Historical Trust Accounting, United States Department of the Interior (the Department). I have held this position for approximately 3 years. I am certified by the Project Management Institute (PMI®) as a Project Management Professional (PMP®), and certified by the International Information Systems Security Consortium, Inc. as a Certification and Accreditation Professional (CAP). My staff of fourteen (14) contractor information technology professionals provide support services for the hardware and software that comprise the Office of the Office of Historical Trust Accounting local area network infrastructure environment (hereinafter "OLE").
2. OLE provides users access to a read-only copy of the Account Reconciliation Tool (ART), and general IT services such as office automation, file sharing, and printer

sharing to over 32 employees of the Office of Historical Trust Accounting. As CIO, my responsibilities for OLE 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 Historical Trust Accounting seeks permission for OLE to 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 Historical Trust Accounting, 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 OLE 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 OLE interconnection and defined the roles, responsibilities, terms, conditions, and expectations of the Department and of the Office of Historical Trust Accounting for security and operation of ESN and OLE. The agreement was signed by both parties.

6. I also developed an Interconnection Security Agreement for the proposed OLE interconnection which defined the technical security requirements and further identified

the security controls employed to protect all the data in OLE including Individual Indian Trust Data. These security controls include:

i. Intrusion Detection System appliances on each local area network segment, which are capable of identifying, unauthorized equipment and user access, and network traffic anomalies;

ii. secure software image deployed on all workstations based on the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG);

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 Windows Server Update Service;

vi. current anti-virus/spyware software and centralized scheduled updates of signature files;

vii. host-based intrusion detection system for database security;

viii. 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 OLE-ESN interconnection. This agreement was signed by both parties.

8. As part of the C&A process for OLE, the Office of Historical Trust Accounting, contracted with Rollout Systems, LLC to perform an independent verification of OLE and provide a report of its findings. In June 2007, Rollout Systems 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. Rollout Systems conducted an assessment of management, operational, and technical security controls for OLE 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. Rollout Systems 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 Rollout Systems have been eliminated.

10. I submitted the CAP documentation relative to OLE and the most recent OLE 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) OLE 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 are conducted to evaluate OLE 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, are conducted monthly. Vulnerabilities and weaknesses are recorded in a report that categorizes the risks as "High Risk", "Medium Risk", or "Low Risk" and the Plan of Actions and Milestones are updated accordingly. A comprehensive security test designed to validate the effectiveness of the security controls documented within the OLE System Security Plan (SSP) will be conducted annually.

12. I have advised the Special Trustee for American Indians, as the Designated Approving Authority for OLE, that security controls for OLE 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 OLE 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 OLE and ESN.

12/21/2007
Date

Carl Huls
Chief Information Officer
Office of Historical Trust Accounting

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 ROSS O. SWIMMER

I, Ross O. Swimmer, to the best of my knowledge, information, and belief declare as follows:

1. I am the Special Trustee for American Indians of the United States Department of the Interior.
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 of the Office of Historical Trust Accounting known as OLE, after considering potential risks and the magnitude of harm.
3. I have been briefed by the Chief Information Officer for the Office of Historical Trust Accounting with regard to the security measures in place for OLE and have been advised that the security controls for OLE have been assessed using appropriate verification and validation techniques and procedures; and that security controls have been implemented correctly and are effective.

4. Based on the advice and recommendations of the Chief Information Officer for the Office of Historical Trust Accounting, I have determined that the security controls and plans in place for OLE 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.

10/21/07
Date

Ross O. Swimmer
Special Trustee for American Indians

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.	

ORDER

This matter comes before the Court on *Interior Defendants' Motion for an Order (1) Authorizing the Reconnection to the Internet of Information Technology Systems of the Bureau of Indian Affairs, the Office of Hearing and Appeals, and the Office of the Special Trustee, (2) Confirming That the Office of Historical Trust Accounting May Connect its Information Technology System to the Internet, and (3) Vacating the December 17, 2001 Consent Order Regarding Information Technology Security*. [_____] 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 December 17, 2001 *Consent Order Regarding Information Technology Security* (Dkt. No. 1063) is VACATED;

AND IT IS FURTHER ORDERED that the IT system networks of the Department of Interior's Bureau of Indian Affairs, the Office of Hearings and Appeals, and the Office of the Special Trustee may be reconnected to the Internet at the department's earliest convenience. The OLE network of the Department of Interior's Office of Historical Trust Accounting OLE

network may be connected to the Internet at the Department of Interior's earliest convenience.

SO ORDERED

Hon. James Robertson
UNITED STATES DISTRICT JUDGE

Date:_____