

**THE PROPRIETY OF THE TAXPAYER-FUNDED
WHITE HOUSE DATA BASE**

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL ECONOMIC GROWTH,
NATURAL RESOURCES, AND REGULATORY AFFAIRS
OF THE

COMMITTEE ON GOVERNMENT
REFORM AND OVERSIGHT
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

SECOND SESSION

SEPTEMBER 10, 1996

Printed for the use of the Committee on Government Reform and Oversight



U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 1997

38-236 CC

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-054186-7

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

WILLIAM F. CLINGER, JR., Pennsylvania, *Chairman*

BENJAMIN A. GILMAN, New York	CARDISS COLLINS, Illinois
DAN BURTON, Indiana	HENRY A. WAXMAN, California
J. DENNIS HASTERT, Illinois	TOM LANTOS, California
CONSTANCE A. MORELLA, Maryland	ROBERT E. WISE, JR., West Virginia
CHRISTOPHER SHAYS, Connecticut	MAJOR R. OWENS, New York
STEVEN SCHIFF, New Mexico	EDOLPHUS TOWNS, New York
ILEANA ROS-LEHTINEN, Florida	JOHN M. SPRATT, JR., South Carolina
WILLIAM H. ZELIFF, JR., New Hampshire	LOUISE MCINTOSH SLAUGHTER, New York
JOHN M. MCHUGH, New York	PAUL E. KANJORSKI, Pennsylvania
STEPHEN HORN, California	GARY A. CONDIT, California
JOHN L. MICA, Florida	COLLIN C. PETERSON, Minnesota
PETER BLUTE, Massachusetts	KAREN L. THURMAN, Florida
THOMAS M. DAVIS, Virginia	CAROLYN B. MALONEY, New York
DAVID M. MCINTOSH, Indiana	THOMAS M. BARRETT, Wisconsin
RANDY TATE, Washington	BARBARA-ROSE COLLINS, Michigan
DICK CHRYSLER, Michigan	ELEANOR HOLMES NORTON, District of Columbia
GIL GUTKNECHT, Minnesota	JAMES P. MORAN, Virginia
MARK E. SOUDER, Indiana	GENE GREEN, Texas
WILLIAM J. MARTINI, New Jersey	CARRIE P. MEEK, Florida
JOE SCARBOROUGH, Florida	CHAKA FATTAH, Pennsylvania
JOHN B. SHADEGG, Arizona	BILL BREWSTER, Oklahoma
MICHAEL PATRICK FLANAGAN, Illinois	TIM HOLDEN, Pennsylvania
CHARLES F. BASS, New Hampshire	ELIJAH CUMMINGS, Maryland
STEVEN C. LATOURETTE, Ohio	
MARSHALL "MARK" SANFORD, South Carolina	BERNARD SANDERS, Vermont (Independent)
ROBERT L. EHRlich, JR., Maryland	
SCOTT L. KLUG, Wisconsin	

JAMES L. CLARKE, *Staff Director*
KEVIN SABO, *General Counsel*
JUDITH MCCOY, *Chief Clerk*
BUD MYERS, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL ECONOMIC GROWTH, NATURAL RESOURCES, AND REGULATORY AFFAIRS

DAVID M. MCINTOSH, Indiana, *Chairman*

J. DENNIS HASTERT, Illinois	COLLIN C. PETERSON, Minnesota
JOHN M. MCHUGH, New York	HENRY A. WAXMAN, California
RANDY TATE, Washington	JOHN M. SPRATT, JR., South Carolina
GIL GUTKNECHT, Minnesota	LOUISE MCINTOSH SLAUGHTER, New York
JOE SCARBOROUGH, Florida	PAUL E. KANJORSKI, Pennsylvania
JOHN B. SHADEGG, Arizona	GARY A. CONDIT, California
ROBERT L. EHRlich, JR., Maryland	CARRIE P. MEEK, Florida

EX OFFICIO

WILLIAM F. CLINGER, JR., Pennsylvania	CARDISS COLLINS, Illinois
MILDRED WEBBER, <i>Staff Director</i>	
KAREN BARNES, <i>Professional Staff Member</i>	
CINDI STAMM, <i>Clerk</i>	
LIZA MIENTUS, <i>Minority Professional Staff</i>	

CONTENTS

	Page
Hearing held on September 10, 1996	1
Statement of:	
BeVier, Lillian R., Doherty professor of law and Elizabeth D. & Richard A. Merrill Research professor of law, University of Virginia School of Law; and John Harrison, professor of law, University of Virginia School of Law	121
Brock, Jack, Director, Information Management Issues, General Account- ing Office; Keith Rhodes, Technical Assistant Director, Office of the Chief Scientist, General Accounting Office; and Ron Hess, General Accounting Office	92
Letters, statements, etc., submitted for the record by:	
BeVier, Lillian R., Doherty professor of law and Elizabeth D. & Richard A. Merrill Research professor of law, University of Virginia School of Law, prepared statement of	124
Brock, Jack, Director, Information Management Issues, General Account- ing Office, prepared statement of	96
Harrison, John, professor of law, University of Virginia School of Law, prepared statement of	129
McIntosh, Hon. David M., a Representative in Congress from the State of Indiana:	
Letter dated August 12, to Jack Quinn regarding the White House Data Base audit function; Mr. Quinn's August 14, 1996 response; document provided by the White House titled "WhoDB," the White House Management Information System; and the White House Data Base printout of Mr. Arthur Coia by the White House	5
Prepared statement of	25
Peterson, Hon. Collin C., a Representative in Congress from the State of Minnesota, copy of a contract left by the Bush administration to establish a Data Base in the Bush administration	29

THE PROPRIETY OF THE TAXPAYER-FUNDED WHITE HOUSE DATA BASE

TUESDAY, SEPTEMBER 10, 1996

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL ECONOMIC GROWTH,
NATURAL RESOURCES, AND REGULATORY AFFAIRS,
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:15 a.m., in room 2154, Rayburn House Office Building, Hon. David M. McIntosh (chairman of the subcommittee) presiding.

Present: Representatives McIntosh, Hastert, Ehrlich and Peterson.

Staff present: Mildred Webber, staff director; Todd Gaziano, chief counsel; Karen Barnes, professional staff member; Cindi Stamm, clerk; Bruce Gwinn, minority senior policy analyst; and Liza Mientus, minority professional staff.

Mr. McINTOSH. Today the Subcommittee on National Economic Growth, Natural Resources, and Regulatory Affairs is holding a hearing to determine whether the White House has legally and properly spent at least a half a million dollars of taxpayer money to build and maintain a White House Data Base. The White House Data Base is a vast computer system, nicknamed by some in the White House as "big brother," that keeps personal and political information on at least 200,000 unsuspecting Americans. The existence of the White House Data Base came to light as part of Congress' investigation of the White House's improper request for FBI files.

Chairman Clinger asked this subcommittee to look into potential uses, and abuses, of this sensitive, personal and political information contained in the White House Data Base.

On June 27, 1996, I first wrote to the White House requesting information on the White House Data Base for review by this subcommittee and ultimately by the full committee. I asked the General Accounting Office to conduct a technical audit of the Data Base. We have many, many questions about this gross breach of public confidence. And sadly, the White House has continued to stonewall this committee and the American public.

As information has trickled out of the White House about the system, I have developed several very serious concerns. The White House Data Base is an unprecedented use of government resources to keep very private, personal and political information on American citizens. It is accessible to more than 100 users, including White House interns. This information includes the ethnic and reli-

gious backgrounds of individual Americans, as well as campaign contribution records and attendance at Democratic National Committee functions. For example, many of the entries show up as "1992 Top 20"; "DNC Trustee"; and "1992 Early Supporter Financial."

Mysteriously, this system identifies not only individuals who have received communications from the Clinton White House, but also those who have received mail from the DNC and the Clinton/Gore Reelection Committee. If this were done by a Member of Congress, it would be illegal.

Where did this data come from? How was it entered into the system? Who paid for it? What was the possible legitimate and legal use that the White House could have for this type of information?

I am entering into the record of this hearing a copy of the report on Arthur Coia, generated by the White House for the Crime Subcommittee here in Congress. This particular record, from which I have redacted truly personal information, shows the type of political data kept at the White House Data Base by the White House. It is absolutely astounding to me that it would have this type of political information in the White House, and I have asked the staff to distribute copies of this report to not only the Members, but all those in attendance here at this committee.

Last week I spent a few hours at the White House to get a better sense of the kind of information that we were talking about, and frankly, I was shocked and even more disturbed by what I saw. The system looked more like a campaign contribution list than an official record. This is the type of information the DNC would use, not something for which the Clinton White House should bill the taxpayers over a half a million dollars.

As I said, if any Member of this committee had this type of Data Base on their House computers, they would be violating the law and go to jail.

Congress and the American people are entitled to the whole truth about this system. Was it an illegal use of government-funded resources? Was it intended to help the President with his campaign? Did it keep track of rewards from major contributors?

I am particularly troubled about potential uses and abuses of the information in the system since the White House does not maintain an audit trail to identify who used the system and what information was used or changed. Now, despite repeated requests, the audit function on the system was never turned on. First, the White House claimed that they did not have an audit function, and it wasn't originally installed into the system. And more recently, they are changing their story to claim that it would result in serious, "performance problems."

Now, because of the unprecedented scope of the White House Data Base, keeping vast amounts of political and personal data on hundreds of thousands of innocent Americans, I have insisted that the White House provide this subcommittee with a copy of the entire Data Base and an alphabetical list of the names of the individuals who are on it. At the rate I was allowed to manually review the individual records, it would take me 4 years just to see all the records on the system.

The subcommittee must have the Data Base itself and historical copies to conduct a thorough examination of the potential and actual uses of the data. I am deeply concerned about the limited access to the Data Base and other documents and materials that the White House has given not only this subcommittee, but the General Accounting Office.

On October 2, the subcommittee wrote to the President and advised him we would seek a subpoena if we could not reach an agreement on the information and access that the White House would provide for the subcommittee. We continue to seek the White House's voluntary cooperation in this investigation, and, sadly, the President has failed to comply.

The lack of White House cooperation is particularly troubling to me because they have been unable to truthfully and completely answer our questions thus far. For example, we need to know who authorized the White House Data Base. Now, we were originally told that Marsha Scott was solely responsible for initiating and approving the Data Base project. Now, apart from the question of whether someone of Ms. Scott's rank had the authority to spend half a million dollars, we later found out that this statement was at worst untrue and at best incomplete.

A White House document, which we are also intending to enter into the record, clearly states that the Data Base was created at the direction of the President and the First Lady; and I repeat, at the direction of the President and the First Lady.

Today we will hear from two panels of witnesses. First we will hear from the General Accounting Office about the progress of this audit. Mr. Jack Brock, GAO's Director of Information Management Issues, has brought with him two of GAO's technical experts, Keith Rhodes and Ron Hess, who have examined the Data Base. They will describe the system and tell us what it can and cannot do. They will also tell us which of their requests the White House has met and where they have continued to stonewall this nonpartisan watchdog of the American taxpayer.

Our second panel will consist of Professor John Harrison and Professor Lillian BeVier, both professors at the University of Virginia Law School. Professor Harrison will address the legality or illegality of the use of taxpayer funds for official and political purposes, and Professor BeVier will address the potential legal and policy implications of the White House keeping and using personal records on a single Data Base within the White House.

This is the first hearing of the White House Data Base that will allow us to get an initial understanding for the design of the system and the legal principles that apply to its use. This subcommittee will continue to examine every aspect about this, bring forward the troubling facts and continue to raise questions during the course of this investigation. And we will continue to take action pursuant to our letter to the President of August 15th.

At this point, I would ask unanimous consent to insert several documents into the record, specifically my August 12th letter to White House counsel Jack Quinn regarding the White House Data Base audit function; Mr. Quinn's August 14, 1996 response to my letter regarding the White House Data Base audit function; a document provided to the subcommittee by the White House titled

“WhoDB,” the White House Management Information System; and the White House Data Base printout of Mr. Arthur Coia that was provided to the House Crime Subcommittee by the White House.

Without objection, it is so ordered.

[The information referred to follows:]

**Congress of the United States
Committee on Government Reform and Oversight
House of Representatives**

August 12, 1996

BY FACSIMILE

The Honorable John M. Quinn
Counsel to the President
The White House
Washington, DC 20500

Dear Mr. Quinn:

I have repeatedly asked you to secure all versions of the White House Database (WhoDB) and to provide access logs to the Subcommittee that would indicate who accessed the WhoDB. Although you have indicated that you have done everything you can to secure different versions of the WhoDB, your answers regarding whether you can provide access logs have been inconsistent at times or completely nonresponsive.

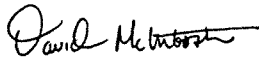
I recently have been informed by the GAO officials conducting the technical audit of the WhoDB that the automatic audit function for the WhoDB was not turned on, and that GAO was told that it was never turned on. GAO has informed me that such an audit function is a safeguard built into the computer system so that this type of access information can be automatically stored.

For your own security reasons alone, I do not understand why you would deliberately disable this basic safeguard that the White House had built into the system.

Given that the Privacy Act requires you to maintain the type of information that the audit function would have stored and that I have repeatedly asked you to secure the information for our investigation, it is troubling to learn that you have not done so. Please inform me by 5:00 on Tuesday, August 13, 1996 whether you have turned on the WhoDB audit function.

Thank you for your attention to this matter.

Sincerely,



David M. McIntosh
Chairman
Subcommittee on National Economic Growth,
Natural Resources, and Regulatory Affairs

THE WHITE HOUSE
WASHINGTON
August 14, 1996

The Honorable David McIntosh, Chairman
Subcommittee on National Economic Growth,
Natural Resources and Regulatory Affairs
Committee on Government Reform and Oversight
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, D.C. 20515-6143

Dear Congressman McIntosh:

I am writing in response to your August 2, 1996, letter to the President as well as your recent inquiry about the audit function capability of the White House database. As you know from our earlier responses to you and our work with the GAO, we are prepared to do all we can to accommodate your legitimate oversight needs regarding the database. In that vein, I would like to meet with you and Congressman Peterson to work through the process of providing you with the information to meet these needs. I recognize that you have other matters to attend to this week, but I am ready to meet any day next week other than Friday, the 23rd.

I think a meeting of this kind is important. It is apparent from our exchanges to date that some of the practical implications of meeting all of your requests have not been brought home fully to you. I accept responsibility for that and want to remedy it as soon as possible. I want, for example, to ensure that you are fully apprised of all the costs, privacy expectations and work involved in these requests. I also want to renew my outstanding offer to you to review every aspect of the data in the system personally. This review likely would, as I previously stated, obviate the need for many of your other requests.

As an initial matter, the investment of time and costs by technical personnel -- excluding all the other related equipment and other resource costs -- who would have to be reassigned from serving the daily computer needs and projects of the Executive Office of the President and, in the instance of one particular project, our congressional appropriations committee, is quite significant.

By way of example, you requested that we "turn on" an audit function on the database and suggested in your August 12, 1996, letter that it was "disabled." As we have indicated, this feature was never installed in the White House Database system. To add this feature for you will require, at a minimum, three to five weeks of full-time work by a couple of computer programmers,

Prepared for Chairman David M. McIntosh, Subcommittee on National Economic Growth,
Natural Resources and Regulatory Affairs.

Chairman McIntosh
August 14, 1996
Page Two

excluding other technical costs. This estimate has been confirmed by Sybase, the system's software developer. You also have requested an alphabetized list of the names in the database -- something that certainly would be of value to the White House but because of time and costs reasons, we have never created. Designing and printing such a report would require at least three to five days of software development and about 240 hours -- 10 around-the-clock days -- of processing and printing time. These are just some of the issues associated with only two of the requests you have made; it does not begin to factor in the limits of our staff and other on-going projects that affect personnel availability. I hope that after we meet to discuss these types of considerations, you may be better able to assess your oversight needs in the context of the costs to the taxpayers.

Independent of the obvious resource and cost issues associated with your requests, there are more paramount privacy expectations that we intend to honor for persons who have elected to provide the White House with contact information, including unlisted home telephone numbers, social security numbers, and private mailing addresses. I know that ensuring the reasonable privacy expectations of these Americans is also important to you; we therefore need to work out a responsible way to meet their expectations. We believe providing you and Congressman Peterson with an opportunity to review any and every entry in the database at your own convenience did so; since you have declined to review the system personally to date, we need to work out another method that accomplishes this same level of privacy protection.

I am happy to meet with you, as I have with the Chairman in the past, to work through all of these matters. My goal is to meet your legislative needs while minimizing the costs to taxpayers, prioritizing and setting reasonable time projections, protecting the privacy of Americans in our system, and ensuring that all of the information is used for appropriate oversight functions, and not for any unofficial or impermissible purposes. I look forward to meeting with you and Congressman Peterson as early next week as possible.

Sincerely,



Jack Quinn
Counsel to the President

cc: Representative Collin Peterson
Chairman William Clinger, Jr.
Representative Cardiss Collins

Prepared for Chairman David M. McIntosh, Subcommittee on National Economic Growth, Natural Resources and Regulatory Affairs.

I. Executive Summary

The President and the First Lady have requested from Marsha Scott that a resource database containing relevant information about all White House events and contacts be designed and implemented. This database will be used and accessed by key White House Office personnel in the OEOB and East and West Wings of the White House. Currently, there is no central repository for this information that can be quickly and easily accessed as most offices use proprietary and dedicated systems that, in most cases, do not allow for the sharing of information between offices. This closed environment has resulted in redundant information, islands of information, duplication of effort, difficult support and a lack of synergy between offices.

The mission of the Database Team, consisting of Marsha Scott, Erich Vaden, Laura Tayman, Mark Bartholomew and Jerry Carlsen, was to eliminate the many existing White House databases and merge them into one cohesive and user oriented system that will meet the following objectives:

- Provide the President and First Lady with a database that tracks all contacts with individuals and organizations who are important to the Presidency.
- Provide select White House staffers a tool for recording contacts and planning future events and meetings.
- Eliminate duplication and confusion among White House staffers as to where and how to find critical contact information.
- Promote cooperation and coordination amongst White House Offices and staffers.

The Database Team began planning the strategy for accomplishing this mission in December and an approximate timeline was established. After initial introductory meetings between Marsha Scott, Erich Vaden, Laura Tayman and the selected White House offices had taken place, technical interviews commenced in January and continued through February. Concurrently several meetings were held with Cheryl Mills, White House General Counsel's Office to address the following issues:

- From what sources can the White House obtain information for the database?

Answer: Any source provided the information is helpful to the President in an "official" capacity.

Source: The White House, WhoDB: The White House Management Information Systems, WhoDB Requirements Report (undated)

WinDB - Individual's Phone Numbers

File Edit Report Data Admin Help

Mr. **Arthur** A. **COIT**
 First Name Middle Name Last Name
 Social Security # Date of Birth Waves / Other / Other State / ZIP / Other

Home Address(es)
 C/P Id Ind Street Street2 City State Zip Add Address Delete

C/P	Id	Ind	Street	Street2	City	State	Zip	Add Address	Delete

Telecommunication Addresses

Index	Type	Telecommunication	Last Modified By
Business/Organization	4	Voice	2002
Business/Organization	4	Fax	2002

Delete Add Phone Add

Business Address(es)
 C/P Id Ind O/B Business

C/P	Id	Ind	O/B	Business
X	X	4		LABORERS

Basic Info Hierarchical Info Categories Business Associations

List of Individual's phone numbers : Double Click on a phone number to view details

Who00 - Comments

File Edit Report Data Admin Help

Mr. Arthur A. Cole

Prof. Name Middle Name Last Name Suffix

Joanne Cole

WAVES / Comments Type

Public Group User Add Clear

Comments	Owner	Comments
1	SYSADM	DNC HJkes
1	POSTER R	ATTENDED - S0080394

Basic Info Biographical Info Categories

Who08 - Categories: Region

File Edit Report Data Admin Help

Mr. Arthur A. Cole

Religion: [] Political Party: [] Social Security: [] Date of Birth: [] WAGES: [] Social Security: []

Region: [] Congressional Dist: [] (Basic Participants)

Home State: [] Home Country: []

Media Market(s): []

92 Early Supporter - Political
92 Early Supporter - Top Twenty
KC Trustee

SOCIAL OFFICE AE
Organizing Office

680721
Organizing List

Demographic

Outreach

Basic Info | Demographic Info | Categories | Issues/Outreach

The media market in which the candidate lives works

WhoDB - Categories: Industry/Professional

File Edit Report Data Admin Help

Mr. Arthur A. Coia

First Name Last Name Social Security Number

Out of P.T. AA/VS /Classification Type Special FBI Name

Categories:

Position: Add Clear

Category Position Detail

Category	Position	Detail
Government	Federal	Executive Political Appointee
Labor/Union		President

Basic Info Information Categories Issues Settings

List of the primary P. Jobs and Categories: Double click on a category to edit/remove

WhoDR - Categories: Demographic

File Edit Report Data Admin Help

Mr. Arthur A. Cole
Prof. First Name Middle Name Last Name
Social Security # Date of Birth WIVES / Divorces Type Spouse Full Name

General Consideration(s):
Ethnicities: Caucasian-European Descent Italian
Veteran Status(es):
Religious Affiliation:
Close

Basic Info Demographic Categories Assistance/Options

WhoDB - Categories: Outreach

File Edit Report Data Admin Help

Mr. Arthur A. Cola

Code: [] First Name: [] Initials: [] Last Name: []

Special Category: [] Color of Emblem: [] Way/ES / Clearance: []

Joanne Cola

1985 Holiday Card
1985 Holiday Card - CNC
1995 Holiday Card - Re-elect
California Republican Party Finance Office

Region: [] Industry/Profession: []

Basic Info | **Biographical Info** | Categories: []

OK Cancel

WhoDB - Contact Manager Information

File Edit Report Data Admin Help

Mr. Artixur A. Coia
 Betty First Name Middle Name Last Name Suffix
 Social Security # Date of Birth WAVES / Clearance Type Spouse Full Name

Contacts	Staff Member	Out/In	Response	Date	Time	Contact Type	Description
WHO	KIM WIDDESS	Out	Regretted	04/02/1996	19:30	State/Official Dinner	Italy State Dinner
WHO	KIM WIDDESS	Out	Regretted	01/25/1996	12:00	Luncheon	DNC Finance Lunch
WHO	KIM WIDDESS	Out	Invited	12/06/1995	18:30	Reception	DELETE THIS EVENT
WHO	KIM WIDDESS	Out	Attended	12/06/1995	18:30	Reception	Holiday Reception (Pageant of Pa...
WHO	KIM WIDDESS	Out	Accepted	09/11/1995	17:00	Reception	DNC BLF Reception
SOFF	System Admin	Out	Regretted	05/26/1995	13:30	Meeting	
SOFF	System Admin	Out	Regretted	02/21/1995	18:30	Dinner	DNC Dinner
SOFF	System Admin	Out	Attended	11/10/1994	18:30	Reception	Health Care Reception
SOFF	System Admin	Out	Attended	11/08/1994	17:00	Reception	Election Day Reception
SOFF	System Admin	Out	Attended	10/20/1994	19:30	Dinner	Dinner (DNC)
SOFF	System Admin	Out	Attended	09/03/1994	08:00	Breakfast	Breakfast (DNC Labor Council)
SOFF	System Admin	Out	Attended	08/03/1994	10:30	Ceremony	Health Care Express Bus Arriva
SOFF	System Admin	Out	Attended	06/28/1994	07:00	Breakfast	Breakfast

List of contacts with this individual. Double click on a contact to view...

WhoDB - Contact Manager Information

File Edit Report Data Admin Help

Mr.

First Name Middle Name Last Name Suffix

Social Security # Date of Birth WAVES / Clearance Type Special Full Name

Sort by:

Office	Staff Member	Date	Response	Date	Time	Contact Type	Description
SOFF	System Admins/Out	06/28/1994	Attended	06/28/1994	00:00	Breakfast	Breakfast
SOFF	System Admins/Out	05/12/1994	Attended	05/12/1994	10:30	Reception	Coffee (Founders of the National C
SOFF	System Admins/Out	05/10/1994	Attended	05/10/1994	12:00	Meeting	AFL-CIO Meeting
SOFF	System Admins/Out	05/04/1994	Attended	05/04/1994	00:00	Ceremony	School-to-Work Bill Signing Cerem
SOFF	System Admins/Out	04/19/1994	Attended	04/19/1994	18:30	Presidential Dinner	Reception (DNC Trustees)
SOFF	System Admins/Out	03/05/1994	Attended	03/05/1994	14:00	Ceremony	Announcement (Reemployment Ad
SOFF	System Admins/Out	12/06/1993	Attended	12/06/1993	18:30	Presidential Dinner	holiday Reception
SOFF	System Admins/Out	12/01/1993	Attended	12/01/1993	19:30	Presidential Dinner	Dinner (DNC Managing Trustees)
SOFF	System Admins/Out	10/14/1993	Regretted	10/14/1993	17:30	Reception	DNC Reception
SOFF	System Admins/Out	09/01/1993	Attended	09/01/1993	10:00	Reception	Labor Day Reception
SOFF	System Admins/Out	08/01/1993	Attended	08/01/1993	19:30	Presidential Dinner	Private Dinner
SOFF	System Admins/Out	05/04/1993	Attended	05/04/1993	15:00	Meeting	AFL-CIO MEETING

Basic Info

List of contacts with this individual. Double click on a contact to view/edit.

WhoDB - Issues/Positions Information

File Edit Report Data Admin Help

Mr. Arthur A. Cois

Joanna Cois

Sort by: Data Issue Position Public Release Private Release Add Issue

Issue	Sub-Issue	Position	Date	Release	Ext Modified By

Basic Info **Biographical Info** Categories Issues Positions

Issues and positions listed on these issues.

Mr. MCINTOSH. At this point, let me turn to the ranking member of the subcommittee, Mr. Peterson, for an opening statement. And we will confine opening statements to the two of us, and then other committee members, if they arrive, will have an opportunity to question panel members during the hearing.

[The prepared statement of Mr. McIntosh follows.]

OPENING STATEMENT OF REP. DAVID M. MCINTOSH

*Chairman, Subcommittee on National Economic Growth,
Natural Resources, and Regulatory Affairs*

Hearing on the White House Database

September 10, 1996

Today, the Subcommittee on National Economic Growth, Natural Resources, and Regulatory Affairs is holding a hearing to determine whether the White House legally and properly spent at least a half a million tax dollars to build and maintain the White House Database. The White House database is a vast computer system that keeps personal and political information on at least 200,000 unsuspecting Americans. The existence of the White House database came to light as part of the Congress' investigation of the White House's improper requests for FBI files. Chairman Clinger asked this Subcommittee to look into the potential uses and abuses of the sensitive personal and political information contained in the White House database.

On June 27, 1996, I first wrote the White House requesting information on the White House database for review by the Subcommittee. I also asked the General Accounting Office to conduct a technical audit of the White House database. We have many questions about this gross breach of public confidence. And sadly, the White House has continued to stonewall the American public.

As information has trickled out of the White House about this system, I have developed very serious concerns. The White House database is an unprecedented use of government resources to keep very private, personal and political information on American citizens. It is accessible to more than a hundred users, including White House interns. This information includes the ethnic and religious backgrounds of individual Americans as well as campaign contribution records and attendance at Democratic National Committee events. For example, it identified individuals as "1992 Top Twenty," "DNC Trustee," and "1992 Early Supporter -- Financial."

Mysteriously, the system identifies not only individuals who have received communications from the Clinton White House, but also those who received mail from the DNC and Clinton/Gore reelection committee. If this were done by members of Congress it would be illegal. Where did this data come from? How was it entered in the system? Who paid for it? What possible legitimate and legal use could the White House have for this information?

I am entering into the record of this hearing a copy of the report on Arthur Coia generated by the White House for the Crime Subcommittee. This particular record, from which I have redacted truly personal information, shows the types of political data kept on the White House database by the White House. It is absolutely astounding to me that the American taxpayers are funding this blatantly political database.

Last week, I spent a few hours at the White House to get a better sense of what kind of database we were talking about. Frankly, I was shocked and disturbed by what I saw. The system looked more like a campaign contributor list than an official record. This is the type of information that the DNC would use -- not something for which the Clinton White House should bill the taxpayers \$550,000. As I said, if any member of this Committee had this data on their House computers, they would be violating the law and go to jail. Congress and the American public are entitled the whole truth about this system. Was it an illegal use of government funded resources to help the President in his campaign? Did it keep track of rewards for major contributors?

I am particularly troubled about potential uses and abuses of the information in the system since the White House does not maintain an audit trail to identify who used the system and what information they used or changed. Despite repeated requests to activate the audit function of the system, the White House has refused -- first claiming that no audit function was originally installed on the system and more recently changing their story to claim that activating the audit function would result in a serious "performance" problem.

Because of the unprecedented scope of the White House database -- keeping vast amounts of political and personal data on hundreds of thousands of innocent Americans -- I have insisted that the White House provide the Subcommittee with a copy of the database and an alphabetical list of the names of the individuals kept on it. At the rate that I was allowed to manually review individual records at the White House, it would take me four years just to see all of the records in the system. The Subcommittee must have the database itself and historical copies to conduct a thorough examination of the potential and actual uses of the data.

I am deeply concerned about the limited access to the database and other documents and materials that the White House has given to the Subcommittee and GAO. On August 2, the Subcommittee wrote the President and advised him that we would seek a subpoena if we could not reach an agreement on the information and access that the White House would provide to the Subcommittee. We continue to seek the White House's voluntary cooperation in this investigation. Sadly to date, the President has failed to comply.

The lack of White House cooperation is particularly troubling to me because we have been unable to get truthful and complete answers to our questions so far. For example, we need to know who authorized the White House database.

We were originally told that Marsha Scott was solely responsible for initiating and approving the database project. Apart from the question of whether someone of Ms. Scott's rank has the authority to spend half a million dollars on her own, we later found this statement to be at worst untrue or at best incomplete.

A White House document produced to the Subcommittee clearly states in the first sentence that the database was created at the direction of the President and First Lady.

Today we will hear from two panels of witnesses. First, we will hear from the General Accounting Office about the progress of its audit. Mr. Jack Brock, GAO's Director of Information Management Issues, has brought with him two of GAO's technical experts, Keith Rhodes and Ron Hess, who have examined the database. They will describe the system and tell us what it can and cannot do. They will also tell us which of their requests the White House has met and where they have continued to stonewall this non-partisan watchdog of taxpayer money.

Our second panel will consist of John Harrison and Lillian BeVier, professors at the University of Virginia School of Law. Professor Harrison will address the legality or illegality of the use of taxpayer funds for unofficial and political purposes. Professor BeVier will address the potential legal and policy implications of the White House keeping and using personal and political information on a single database within the White House.

This first hearing on the White House database will allow us to get an initial feel for the design of the system and the legal principles that apply to its use. This Subcommittee will continue to examine all of the troubling facts that continue to arise in the course of this investigation.

Mr. PETERSON. Thank you, Mr. Chairman.

I don't know where to start here exactly. I also have gone down to the White House, I think, probably 2 or 3 weeks prior to when you did, to look at the system. And I will have to say that I think some of your comments are a little bit overblown, at least from what I have been able to determine at this point.

I would also like to point out that the White House was not invited to testify here today, which I think is somewhat curious.

But I too would have something I would like to make part of the record, if you wouldn't mind, and that is a copy of a contract that was left by the Bush administration to establish exactly the same kind of Data Base in the Bush administration that you are talking about here. And without objection, I would like that made part of the record.

Mr. MCINTOSH. I haven't had a chance to observe that, but I will be glad to make it part of the record and work on the comparison.

[The information referred to follows:]

AWARD/CONTRACT		1 THIS CONTRACT IS A RAFLD ORDER UNDER DPAS (15 CFR 350)	RATING	PAGE OF PAGE 1 59			
2. CONTRACT (Proc. Inst. Ident.) NO. OA1C03		3. EFFECTIVE DATE NOV 13, 1999	4. REQUISITION/PURCHASE REQUEST/PROJECT NO. RZZ1830 RZZ1760 RZZ1855				
5. ISSUED BY EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF ADMINISTRATION; PROCUREMENT BRANCH; NEOB, RM. 5001, 725 17TH STREET, NW; WASHINGTON, DC 20503; (202) 395-3314		6. ADMINISTERED BY (If other than Item 5) CODE					
7. NAME AND ADDRESS OF CONTRACTOR (No., street, city, county, State and ZIP Code) U.S. SMALL BUSINESS ADMINISTRATION WASHINGTON DISTRICT OFFICE 1111 18TH STREET, N.W. 6TH FLOOR WASHINGTON, DC 20036		8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> OTHER (Rev. 6-74)					
9. DISCOUNT FOR PROMPT PAYMENT NET 30		10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN: SEE SECTION: G.5					
11. SHIP TO OFFICE OF ADMINISTRATION/IRMD 725 17TH STREET, N.W. WASHINGTON, DC 20503 ATTN: DAVID L. STONEHILL		12. PAYMENT WILL BE MADE BY EXECUTIVE OFFICE OF THE PRESIDENT; OFFICE OF ADMINISTRATION; FINANCIAL MGMT DIVISION RM. 4005, 725 17TH ST., NW; WASH. DC 20503					
13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C. 2304(c)(1) <input checked="" type="checkbox"/> 41 U.S.C. 253(c)(1) 5		14. ACCOUNTING AND APPROPRIATION DATA 1110038 DIV 107 OC 72: 34970.32, DIV 107 OC 75: 122029.68					
15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT		
00	THE CONTRACTOR SHALL PROVIDE SERVICES AS FURTHER DEFINED HEREIN.						
01	TASK I. (FIRM FIXED PRICE)	1	LOT	34470.32	\$34470.32		
02	TASK II (OBLIGATE INCREMENTAL FUNDING)	1	LOT	122029.68	122029.68		
03	LOCAL TRAVEL (NOT TO EXCEED)	1	LOT	500.00	500.00		
15G. TOTAL AMOUNT OF CONTRACT					\$ 157000.00		
16. TABLE OF CONTENTS							
VI	SEC.	DESCRIPTION	PAGE(S)	VI	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	52-53
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2-4	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH			
X	C	DESCRIPTION/SPECS./WORK STATEMENT	5-37	X	J	LIST OF ATTACHMENTS	
X	D	PACKAGING AND MARKING	38	PART IV - REPRESENTATIONS AND INSTRUCTIONS			
X	E	INSPECTION AND ACCEPTANCE	38	X	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	54-55
X	F	DELIVERIES OR PERFORMANCE	39	X	L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	G	CONTRACT ADMINISTRATION DATA	40-44	X	M	EVALUATION FACTORS FOR AWARD	
X	H	SPECIAL CONTRACT REQUIREMENTS	45-51				
CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE							
17. <input checked="" type="checkbox"/> CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 4 copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)				18. <input type="checkbox"/> AWARD (Contractor is not required to sign this document.) Offer on Solicitation Number _____ including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and offer, and (b) this award/contract, no further contractual document is necessary.			
19A. NAME AND TITLE OF SIGNER (Type or print) WARREN C. JOHNSON ADVISORY CONTRACTING OFFICER				20A. NAME OF CONTRACTING OFFICER /s/ DALE HELMS			
19B. NAME OF CONTRACTOR		19C. DATE SIGNED		20B. UNITED STATES OF AMERICA		20C. DATE SIGNED	

SECTION - B SUPPLIES OR SERVICES AND PRICES/COSTSB.1 SERVICES

This contract is for the evaluation, selection, acquisition and installation of a Relational Database Management System (RDBMS) to operate on the mainframe computer located at the Executive Office of the President's Data Center. The acquisition of the selected RDBMS will be used to support major EOP budget-related applications and large systems development applications. These systems are more fully described in Section C.1.3.

B.2 TYPE OF CONTRACT

This is a Indefinite Quantity Level of Effort type contract for database management services and support. The Contractor shall provide the necessary personnel to perform the tasks as described in Section C.1.2 on a level of effort basis.

Special Note: There is no guarantee of number of hours of work to be ordered under this contract; however, the government does guarantee, and is obligated to purchase as a minimum, the amount of work as outlined as "Task Number I", which is hereby issued simultaneously with the base contract on a Firm Fixed Price basis in the amount of \$34,470.32.

B.3 PRICING SCHEDULE

The following schedule outlines the labor categories and fully loaded hourly rates of contractor personnel anticipated for performance under the tasks described herein. The hourly rates reflected are not subject to increase during the contract period.

Labor Category

Senior Analyst/Project Manager
Database Analyst
Database Programmer
Acquisition Technician

Hourly Rate

This information is being withheld pursuant to 5 U.S.C. Section 552 (b)(4).

Loaded rates include (b)(4) Overhead, (b)(4) G&A and a (b)(4) Fee. Any equipment/software acquisitions provided shall not exceed a mark up of (b)(4)

SECTION - B SUPPLIES OR SERVICES AND PRICES/COSTS

The Government will issue delivery orders under this Contract as the need for the performance of tasks described in Section C.1.2 arise. The only items open for negotiations are:

- (1) number of hours required to complete task;
- (2) categories of individuals required to complete task and;
- (3) number of individuals in categories.

B.4 TASK CEILING

Each task described herein shall not exceed the ceiling amounts as set forth below without the prior written consent of the Contracting Officer.

Task I Evaluation and Selection

Services: Issued simultaneously with contract award on a Firm Fixed Price basis for the amount of \$34,470.32.

Task II Acquisition/Lease and Installation

Services: \$89,631.40 (acquisition & installation)

Supplies: \$52,500.00 (software lease not to exceed \$7500 per month for the period 03/01/91 - 09/30/91)

Task Ceiling NTE = \$141,871.40

Task #3 Implementation support

Services: \$72,500.00 (on-going support/training)

Task Ceiling NTE = \$72,500.00

B.5 GRAND ESTIMATED TOTAL

The grand estimated total amount of this contract during contract period is \$249,101.72.

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTSB.6 DELIVERY ORDERS

Delivery orders issued for the performance of services as specified herein will contain funding for each individual order. All Delivery orders will be issued by the Office of Administration Procurement Branch and signed by a contracting officer of this office. Delivery Orders placed shall contain the following information:

- Date of order
- Contract number and order number
- Delivery or performance date
- Place of delivery or performance
- Packaging, packing, and shipping instructions, if applicable
- Any other pertinent information

SECTION - C DESCRIPTION/SPECS./STATEMENT OF WORKC.1 BACKGROUND

The EOP Data Center provides computer data processing support to Executive Office agencies, including the White House and the Office of Management and Budget (OMB).

OMB depends on a number of separate application systems for the computer support required in the development and publication of the Budget of the United States. These application systems support both, formal processing and reporting requirements as well as ad hoc and decision support reporting. During recent years interest in the integration of these separate systems using a variety of data storage methods into a system using a single more advanced data storage has been expressed by many groups involved in the budget process.

C.1.1 GENERAL SCOPE

It is the objective of the Government that the Contractor shall provide the following services:

- provide support to the Government in the selection of a RDBMS;
- Perform acquisition and lease arrangement of the selected RDBMS under optional contract provision as described in Contract Section H.10;
- Support Government staff in the initial installation and administration of the RDBMS on the IBM mainframe computers located at the EOP Data Center;
- Provide hands-on training to Government systems programmers, selected application programmers, and database administrators.
- Provide on-going technical support as required.

SECTION - C DESCRIPTION/SPECS./STATEMENT OF WORKC.1.2 TASK AREAS

The Contractor shall perform work in accordance with Contract Section C to accomplish the objectives as outlined in each Task Area below.

Task I - Validation/Evaluation and Selection

The Government would like the contractor to review the requirements in Section C.2, evaluate the leading IBM compatible mainframe RDBMS packages against these requirements, and provide the Government with a recommendation as to the product that best meets the requirements. More specifically:

The Contractor will interview EOP staff to become familiar with the current mode of operation of the systems described in Section C.1.3. The draft list of RDBMS functional and technical requirements will be reviewed and modified to fully reflect any additional requirements.

The Contractor shall survey commercially available, off-the-shelf database software to identify products which provide RDBMS facilities. Candidate products will be identified and selected for evaluation. The selected products shall be evaluated against the requirements specified in Contract Sections C.2.1 and C.2.2, and any other requirements that may be revealed during this phase.

The Contractor shall document the results of its evaluation of RDBMS software and provide a recommendation to the EOP as to selection of an RDBMS.

The Contractor shall provide cost information for the recommended RDBMS which shall consist of lease, purchase, and maintenance costs.

Deliverable: Recommendation of RDBMS package(s) and cost information for lease, purchase and maintenance.

Due Date: January 15, 1991

SECTION C - DESCRIPTION/SPECS./STATEMENT OF WORKTask II - Acquire/Furnish and Install

Once the Government has selected the RDBMS the Contractor shall acquire, furnish for lease and assist with the initial installation of the RDBMS on the EOPDC IBM 3081G computer system operating under IBM MVS/XA. More specifically:

The Contractor shall furnish the selected software and provide a transferable leasing arrangement for the specified software products. Such leasing arrangement shall be mutually agreed to by both contracting parties.

Optional software items, i.e., graphic package, front end query language, shall be included as optional items for lease.

The Contractor shall coordinate installation with EOPDC systems programming staff and RDBMS vendor support personnel to review MVS/XA operating system prerequisites and resolve any incompatibilities in advance of installation.

The Contractor shall assist in tailoring the RDBMS configuration parameters to operate efficiently within the application environments defined herein.

The Contractor will assist EOP software applications and system programming personnel to optimally configure the logical and physical RDBMS software and assist in developing tests to validate RDBMS performance.

Deliverable: Specified RDBMS software and license with transferable leasing arrangement.

Due Date: March 1, 1991

Task III - Implementation Support

The Contractor shall assist in the development of RDBMS application programming and database design standards and techniques. Contractor shall review the existing EOP application development and data administration organizational structure and make recommendations as to its suitability to support operation in an RDBMS environment in which users assume increased responsibility for data access and query.

SECTION C - DESCRIPTION/SPECS./STATEMENT OF WORK

The Contractor will provide technical training support to EOPDC systems programmers and selected applications programmers as may be required.

The Contractor shall provide on-site and on-call support as may be required to assist in problem solving that may occur from RDBMS installation or usage.

Deliverable: To be specified at time of issuance if applicable.

REMAINDER OF PAGE NOT USED

C.1.3 DESCRIPTION OF EXISTING ENVIRONMENT

C.1.3.1 CENTRAL BUDGET MANAGEMENT SYSTEM (CBMS)

Analytical Information System. CBMS provides automated information decision support for OMB policy officials. CBMS is used to analyze and track various budget proposals, to support the preparation of the President's Budget and for ad-hoc analytical exercises. Use of the system is continuous throughout the year but peaks during "budget season" which occurs from October thru January. The primary responsibility for tasks using CBMS resides in the Office of Management and Budget.

Data Repository. CBMS uses Model 204 as a data repository, with access through IFAM COBOL and PL/I programs. Some auxiliary data is stored in VSAM files.

Data structure. CBMS holds hundreds of different versions of the federal budget to allow for analysis and comparison of various proposals. Up to one million budget data records can be stored. The complexity of the federal budget classifications and processes must be reflected in the budget data stored. The data structure allows for user-defined fields and processes. With major system requirement changes from year to year, some changes to CBMS are required, but effort is put into continuing to make the system flexible enough to handle changing requirements with no programming changes. CBMS uses "chunky" data fields, with a fixed record structure defined by source programs. It does not use the Model 204 data dictionary feature.

Non-budget data in CBMS includes thousands of sets of stored instructions which allow users to re-use previously created instructions to perform tasks such as selecting budget data, arranging, aggregating, and sorting budget data.

Application software. CBMS uses COBOL, PL/I, OS JCL, Model 204, ISPF Dialog Manager, TSO CLISTS, VSAM and EasyRetrieve.

CBMS users. The users of CBMS are all located in OMB. They access the mainframe through IBM 3270 terminals or PC's using IBM PC3270 emulation software or IRMA boards. Users also have the ability to connect to the mainframe away from work through 1,200-9,600 baud start/stop or 4,800 bisync dial-up lines using PC's using emulation software.

Outputs. CBMS is used to manipulate data and to produce information through queries and reports for analytical and comparison

reporting, fall scorekeeping, historical tables, GRH processing and analysis, appropriation tracking, comparison of OMB and CBO data, and ad hoc analytical exercises.

SYSTEM CHARACTERISTICS. The CBMS System is a highly complex and sophisticated system comprising over 15 on-line PDS libraries which contain over 1500 members using the following technology:

- Over 100 source programs (COBOL, PL/I)
- Over 100 batch JCL procedures
- Over 200 ISPF panels
- Over 150 ISPF skeletons
- Over 200 TSO CLISTS (command procedures)
- Over 200 production jobs
- Over 300 Model 204 user language programs
- Over 50 documentation files
- Over 50 TSO HELP files
- 2 CICS automatic scheduler modules and help entries

CBMS is both an on-line interactive system and a batch processing system:

On-line interactive mode. At all times except when the system is not down for housekeeping or nightly production, it is available for online updating, the development and running of ad hoc analysis. The ISPF Dialog Manager and file-tailoring capabilities are used to generate user-specified batch report jobs. Reports can be printed immediately or held for on-line viewing, with printing done later at the option of the user.

Batch processing. Reports are run during the day in batch based on the specifications the user gives to the on-line system. During major peak production seasons a nightly processing cycle is run which is comprised of a number of different processes, including report generation similar to that done during the day, and loading of data from external sources. These are time-critical processes.

EXTERNAL DATA LOAD FEATURES. The CBMS database receives data from two major external sources, the Congressional Budget Office and the Budget Preparation System. The external data load process consists of a data translation step and a load step. The data translation is done by a COBOL program that receives specific instructions from a table set up by the expert users of CBMS. They can control, among other things, which data is selected for loading, which CBMS fields will be filled, and how the data will be identified once it is loaded. Once the data is fully prepared, it can be put into the database using either Model 204 FLOD code or a batch IFAM (host language interface) program written in PL/I.

C.1.3.2 BUDGET PREPARATION SYSTEM (BPS) SUMMARY

Financial Information System. BPS is a large, complex budget and financial information system whose function is to support the formulation, analysis, updating and printing of the President's Budget. This is a continuous effort which takes place throughout the year but peaks during "budget season" which occurs during the months from October thru January. The primary responsibility for this process resides in the Office of Management and Budget.

Data Repository. The primary data repository consists of a set of on-line VSAM data files updated during the day via CICS applications software and at night in batch mode.

Data structure. The financial data collected consists of appropriation and receipts planning data for all government agencies. There are about 1,800 appropriation accounts and 800 receipt accounts. At the lowest level between 30,000 and 80,000 records of financial data exist. The entire data base consists of less than 20 million bytes.

While the volume of data contained in BPS is modest, the coding schemes used to identify appropriation and receipts data is quite complex. In addition, classification codes, information recording requirements, and reporting requirements undergo major changes from year to year.

Application software. Written in the language best suited to each particular solution, languages include COBOL, PL/I, ALC, CLISTS, OS/JCL, and ISPF/DMF.

Users. The users of BPS include OMB's Budget Review Division (BRD), Program Divisions, Executive Branch Agencies, and the Congressional Budget Office. Of these users about 300 are in-house OMB users connected to the IBM mainframe systems with coaxial cables, 600 are outside agency users connected to the IBM mainframe systems through 1,200-9,600 baud start/stop or 4,800 bisync dial-up lines. In-house terminal equipment ranges from IBM 3270 terminals to IBM PCs using IBM PC3270 emulation software or IRMA boards. Outside user equipment consists largely of IBM PCs or PC-compatible machines using emulation software (FTTERM, PROCOMM).

Maximum concurrent CICS users: 160.

Outputs. The outputs of BPS provide the basis for most of the financial information shown in the published federal budget document volume containing:

- The Budget of the United States Government,
- The Budget of the United States Government - Appendix, and
- Special Analysis, Budget of the United States.

Machine-readable outputs and computer-generated reports are also used by other Government agencies in the Executive and Legislative Branches.

Interface software currently in production provides the capability to:

- Photocompose the Budget Accounts Listing (BAA), (Federal Programs by Agency and Account), a major table in the Budget of the United States Government.
- Migrate financial data from the BPS data base to the Government Printing Office (GPO) Budget Appendix text data base, thus reducing manual input and proof reading which is required in the photocomposition of the Budget of the United States Government - Appendix.

System Characteristics. Characteristics of the processing system include the following:

- Highly complex and sophisticated software systems comprising over 28 on-line PDS libraries containing over 2,000 objects (members):
 - Over 700 Source Programs (COBOL, ALC, PL/I)
 - Over 400 Batch JCL Procedures
 - Over 300 TSO Command Procedures
 - Over 300 TSO Help Entries
 - Over 500 CICS Help Entries
 - Over 200 Documentation Files
 - Over 200 Separate Production jobs.
 - Over 200 Major Reports.
- Treasury data interface for Prior Year reconciliation.
- Congressional data interface (Budget Authority and Outlays).
- Table-Driven Interpretive Processor:
 - Over 300 complex balancing rules.
 - 10 - 25 % change rate in balancing rules per year.
 - Changes made almost daily during production cycles.
 - Majority of balancing criteria maintained by user.
- Table-Driven field validation edit and error message generation processing. Majority of edit and message criteria maintained by user.

- Interactive and batch master file updates for four major master files.
- Photocomposition interface with GPO for BAA.
- Interface for migration of financial data from BPS to GPO Budget Appendix text photocomposition data base.

C.1.3.3 BUDGET STATUS SYSTEM (BSS) SUMMARY

Financial Information System. Originally designed in the early 70's, this system was to provide a more flexible end user tool for the analysis of budget data. Its use has decreased over the years, and it is expected to be phased out as more modern tools become available.

Data Repository. The primary data repository consists of a set of sequential data files containing data extracted from BPS as well as data entered by users.

Data structure. The financial data contained in BSS parallels appropriation and receipt planning data contained in BPS, but it is organized around OMB divisions; division level data is shared by a number of users.

Application software. Written in PL/I, CLISTS and OS/JCL.

Users. The users of BSS include OMB's program divisions and Executive Branch Agencies.

Outputs. Relatively flexible report formats based on control parameter files result in relatively informal user reports used for analytical purposes.

2. MODEL 204 APPLICATIONS.A. Name List Services (NLS).

Description: Maintain lists of individuals who have had contact with the President or high government officials. Used for providing reports for White House staff, letters, labels, mailgrams, telegrams, etc.

Offices: White House , Office of Records Management and Office of Travel and Telegraph.

Primary Users: Terry Good, Frances Campbell, Billy Dale

Responsible Programmer: David Naegele

Hardware: IBM 3081, XEROX 9700, IBM-PC, VAX PS40

Software: Model 204 User Language

Status: Operational since 1982

Database size: NLS - 80 mbytes
Media - 28 mbytes
TTO - 5 mbytes

Potential Growth in Size: 100% 1st year (NLS only)
10% thereafter

Storage Size of Code: 4.7 mbytes

B. Mail Analysis System.

Description: Used to answer Presidential mail from the general public. Uses precanned replies to respond to this mail based on the topic and disposition (pro or con) on the issue.

Office: White House, Office of Correspondence

Primary User: Maureen Hudson, Lillie Bell

Responsible Programmer: David Naegele

Hardware: IBM 3081, VAX PS40

Software: Cobol, SPF Screens, Model 204 IFAM, Model 204 User Language

Status: Has been operational since 1982

Database Size: 66 mbytes - 3 months on line

Potential Growth in Size: 10% per year

Storage Size of Code: 4.5 mbytes

C. Classification Index System.

Description: Used to maintain and print the White House classification index scheme.

Office: White House, Office of Records Management

Primary User: Terry Good

Responsible Programmer: Vanessa Bennett

Hardware: IBM 3081, XEROX 9700

Software: Model 204 User Language

Status: Operational

Database Size: 9.5 mbytes

Potential Growth in Size: 1% per year

Storage Size of Code: .5 mbytes

D. Christmas Card List

Description: Used to aid in the process of addressing Christmas cards sent by the President each year. The objective is to avoid sending more than one card to the same individual.

Office: White House, Correspondence Office,

Primary User: Charles Horvath

Responsible Programmer: David Naegele, Vanessa Bennett

Hardware: IBM 3081

Software: Cobol, SPF screen, Model 204 IFAM, Model 204 User Language

Status: Operational

Database Size: 33 mbytes

Potential Growth in Size: 10% per year

Storage Size of Code: 2.8 mbytes

E. Mail Tallying System.

Description: Tallies the count of Presidential mail received daily by primary issue and disposition (pro or con).

Office: White House, Office of Correspondence

Primary User: Lillie Bell, Roger Spiegel

Responsible Programmer: Vanessa Bennett

Hardware: IBM 3081

Software: Model 204 User Language

Status: Operational since Fall 1985.

Database Size: 2.0 mbytes

Potential Growth in Size: 5% per year

Storage Size of Code: 1.5 mbytes

Note: The President receives a weekly summary from this system of the mail that has been tallied for the week and since the start of the Bush Administration.

F. US Mail Locator System

Description: Tracks forwarding addresses of departed
EOP staff and Federal Commissions.

Office: White House, Office of Correspondence

Primary User: Tony Mendoza

Responsible Programmer: Vanessa Bennett

Hardware: IBM 3081

Software: Model 204 User Language

Status: Operational since Summer, 1987

Database Size: 5 mbytes

Potential Growth Size: 5 $\frac{1}{2}$ yr until 1989,
200 $\frac{1}{2}$ 1989 (Change in
Administration),
5 $\frac{1}{2}$ 1990 and up

Storage Size of Code: 2 mbytes

G. EOP Locator System.

Description: Keeps track of the current location and phone number of EOP government staff. Used to answer queries concerning employees phone numbers and room location. Also used by mail forwarding system.

Office: Office of Administration, Personnel Division

Primary User: Director of Personnel

Responsible Programmer: Vanessa Bennett

Hardware: 3081

Software: Model 204 User Language

Status: Operational

Database Size: 6.4 mbytes

Potential Growth in Size: None

Storage Size of Code: 2.8 mbytes

Note: This system is regenerated every 2 weeks. On line data shows those employees (paid by Treasury) that were active during the 2 week period the load took place, and 6 months of inactive employees.

H. Parking Permit System.

Description: Produce the monthly parking permits for EOP parking areas.

Office: White House

Primary User: Betty Ubbens

Responsible Programmer: Vanessa Bennett

Hardware: IBM 3081

Software: Model 204 User Language, SPF-DMF, Cobol, Easytrieve

Status: Operational. Production Control oversees the running of monthly parking stickers.

Database Size: 1.3 mbytes

Potential Growth Size: None

Storage Size of Code: 2.1 mbytes

Note: This system does not keep historical information, only active records.

I. Office of National Service System.

Description: Maintain lists of contribution leaders to the Thousands Points of Light Program. Used for sending letters to select groups.

Office: Office of National Service

Primary User: Leah Geraghty

Responsible Programmer: Vanessa Miller

Hardware: IBM 3081, IBM-PC, VAX PS40

Software: Model 204 User Language

Status: Operational

Database Size:

Potential Growth in Size:

Storage Size of Code:

Note: This is a clone of NLS which has been modified to reflect the field names relevant to this program. A STAIRS file is to be generated for retrieval purposes.

J. Presidential Contacts System.

Description: Maintains list of names and addresses of individuals identified as important to the President. The M204 software for updating information is presently a clone of NLS.

Office: White House Office, Correspondence Office

Primary User: Jan Burmeister

Responsible Programmer: David Naegele

Hardware: IBM 3081

Software: Model 204 User language, STAIRS

Status: Operational

Database Size:

Potential Growth Size:

Storage Size of Code:

Note: This sytem has two STAIRS files - one for general WHO users and another more private file for select users.

K. Document Distribution System.

Description: Tracks distribution of EOP publications to public, and other government agencies.

Office: Office of Administration, Library and Information Services Division.

Primary User: Don Watt

Responsible Programmer: Vanessa Bennett

Hardware: IBM 3081

Software: Cobol, SPF screens, Model 204 IFAM, M204 User Language

Status: Operational

Database Size: 7.1 mbytes

Potential Growth in Size: None

Storage Size of Code: 1.7 mbytes

Note: This system does not keep historical records. It is an administrative system used to facilitate the disbursement of printer material, i.e. press releases. Records are deleted after a "pick list" is generated daily.

L. Security Tracking System.

Description: Tracks processing of security access of those individuals working in EOP complex and those individuals considered for Presidential appointment.

Office: White House, Office of the Counsel to the President, Security Office

Primary User: Jane Dannenhauer, Chuck Easley

Responsible Programmer: Vanessa Bennett

Hardware: IBM 3081

Software: Model 204 User Language

Status: Operational mid-July 1988

Database Size: 15.5 Kbytes

Potential Growth in Size: 10%

Storage Size of Code: 900 Kbytes (or.9 mbytes)

M. Electronic Requisition System.

Description: An automated system designed to integrate the process of requesting goods and services with EOP agencies including the completion of Procurement documents and the acceptance of these goods.

Office: Executive Office of the President

Primary User: ERS Working Group

Responsible Programmer:

Hardware: IBM 3081

Software: Model 204 User Language

Status: Office of Administration online since August 1988

Database Size: 15 cylinders

Potential Growth in Size: 30 cylinders.

Storage Size of Code: 5 cylinders

N. EOP Drug Testing

Description: This system is for use by personnel in the Office of Administration, Personnel Division, Information is taken from biweekly tapes provided to OA by the Treasury Department. The system allows the users to update data, generate reports, and download data to PCs for further analysis.

Office: Office of Administration, Personnel Division

Primary User: Director of Personnel

Responsible Programmer: Vanessa Bennett

Hardware: IBM 3081

Software: Model 204 User Language, SAS, /FT/TSO

Status: Operational

Database Size: 7 cylinders, 6,251 bytes

Potential Growth in Size: 1 trk a month (max)

Storage Size of Code: 4 cylinders, 3,572K bytes

O. FMD Query System.

Description: This system is for use by personnel in the Office of Administration, Financial Management Division. Information is taken from biweekly tapes provided to OA by the Treasury Department. The purpose of the system is to provide on-line access to the information contained in these tapes so that FMD personnel may query selected data, generate reports and download data to PCs for further analysis.

Office: Office of Administration, Financial Management Division

Primary User: Angela Johnson

Responsible Programmer: Vanessa Bennettt

Hardware: IBM 3081

Software: Model 204 User Language, FT/TSO

Status: Operational

Database Size: 56 cylinders, 49,491 bytes

Potential Growth in Size: 15 trk a month (max)

Storage Size of Code: 30 trks, 14,100K bytes

C.1.3.5 EOP DATA CENTER (EOPDC)

Hardware/Software. The EOPDC operates two loosely coupled IBM 308x mainframes under the OS/MVS XA/JES II operating system and expects eventual migration to ESA. Software includes CICS, TSO, BATCH, ISPF, DMF, ACF2, VTAM, TPX, and M204.

C.2 DEFINITION OF REQUIREMENTS

C.2.1 FUNCTIONAL REQUIREMENTS

One of OMB's major responsibilities is the formulation and tracking of the budget of the United States Government. The three application systems, BPS, CBMS, and BSS described above currently comprise the majority of the data processing systems available to OMB to assist with the performance of these functions.

The following characteristics underlying the process are important in the evaluation of alternative data base solutions:

- Frequent significant changes in the structure and coding of financial data;
- High data complexity (numerous exceptions to general rules);
- Relatively low data volume;
- Cyclic periods of activity with short-lived peaks of activity;
- Need for a large number (200-300) of different standard production reports;
- Need for flexibility in changing structure and presentation of very complex reports;
- Need for flexible ad hoc reporting;
- Need for full-featured, general-purpose query facility;
- Need for user initiated retrieval and analytical reporting;
- Need to quickly respond to high level policy changes affecting information storage and output requirements;
- Need by some users to be able to access and modify the entire data base;
- Need by some users to be able to access and modify only part of the data base.

C.2.2 TECHNICAL REQUIREMENTS

Mandatory RDBMS Requirements

1. The RDBMS must operate on the EOPDC IBM mainframe systems.
2. Access: TSO/CICS. The RDBMS must support concurrent access from TSO, TSO batch, and CICS through a single image of the software.
3. Audit Trail. Sufficient information regarding database access shall be captured to record "who did what/where/when."
4. The audit facility shall be activated at the system level.
5. Directories. The RDBMS must have a directory/catalog system or other descriptor facility as a system database of essential system related objects.
6. The RDBMS must catalog file descriptions, user authorities, indices, subschema, other database objects and characteristics.
7. The RDBMS directory shall be accessible using the standard RDBMS query facilities that will be provided with the RDBMS.
8. The RDBMS must support the use of synonyms for files, fields, and subschema.
9. Data Independence. The DBMS shall provide for altering, adding, or deleting objects in the data base.
10. The RDBMS shall provide for designing/changing and storing alternative subschemas of data stored in a database.
11. The RDBMS shall provide for extending the length of existing data elements, adding or deleting data elements from the existing data base.
12. The RDBMS shall provide the capability to define sub-schemas for the database, and sub-schemas that span multiple files.
13. The RDBMS shall provide documentation of data base records that have been modified and what impacts on the application programs result after a change is made to the data base.
14. Data Integrity. The RDBMS must be able to actively enforce relationships between primary and foreign keys; i.e. the RDBMS must be able to actively enforce referential integrity.

15. The RDBMS shall be able to apply locks to data being concurrently accessed for update in such a manner that data integrity is guaranteed.
16. The RDBMS shall be able to support the access of data from the same record by multiple users in such a manner that data integrity is guaranteed (i.e., data is preserved in uncorrupted form for its intended purpose).
17. Deadlock. The RDBMS shall protect from a deadlock situation and shall detect and resolve any deadlock conditions in a predictable manner.
18. Indexing. The RDBMS shall support indexing on any field or combination of fields.
19. The RDBMS shall support the ability to dynamically add new indices or delete old indices without requiring reloading or reorganizing the data tables to which these indices apply.
20. The RDBMS shall be able to apply read and write locks at the field level, either directly or by means of views, to data being concurrently accessed for update in such a manner that data integrity is guaranteed and concurrent update access to a single record is minimally restricted.
21. Data Manipulation. The commit operator (or "verb") (i.e., make all tentative updates firm) and roll-back (i.e., undo all tentative updates) must be supported by the RDBMS.
22. Database Administration. All RDBMS administration capabilities/utilities shall be available on-line. (Third-party software acceptable for on-line update.)
23. The RDBMS shall include a substantial database administration capability that may be part of the RDBMS, an "add on" utility, or a combination of the two. If an "add-on" utility is proposed, it must be included in the cost proposal.
24. The RDBMS administration capability shall include a configurable resource limiting facility to control the quantity of systems resources consumed by a query and prevent a "run away" query.
25. The RDBMS administration capability shall include a capability to print all or portions of user data and DBMS control information (e.g., pointer, record headers, links) from any page/file.

26. The RDBMS administration capability shall include a capability to activate and deactivate any file/schema in the data base.

Activate: subject to normal access privileges

Deactivate: lock, halt all update activity or halt read and update activity

27. The RDBMS administration capability shall include a facility to set (grant/revoke) privileges for categories or groups of users with a minimum amount of DBA staff effort.
28. The RDBMS administration capability shall include on demand monitoring of RDBMS performance and security control providing statistics on numbers of accesses, updates, contentions, overflows, and attempted violations.
29. The database administration capability shall include a mechanism to determine and alter the size and distribution requirements of physical data storage to permit storage optimization.
30. Logical data security. The RDBMS shall be able to be protected by access control under batch, TSO, and CICS via the services currently provided at the EOPDC by ACP2.
31. The RDBMS shall provide for the provide security of database operations during data entry, update, delete, retrieval, and during the creation of schema indices.
32. The RDBMS shall provide an imbedded security system that limits the access of on-line and batch programs at the levels of schema and record, logging and reporting each attempted violation.
33. Physical Data Integrity. In all RDBMS procedures/activities the integrity of the application data shall be insured.
34. The RDBMS shall provide for dumping/restoring on tape or disk at the user's option.
35. The RDBMS shall provide a dual logging capability for both the active and the archive log.
36. The RDBMS shall provide a system for dumping/restoring a partial database of selected files.
37. The RDBMS shall provide a system for dumping a database for back-up purposes and for restoring from a previously taken back-up dump.

38. The RDBMS shall provide a system to recover from a hardware or software failure.
39. The RDBMS shall provide a system for dumping/restoring an incremental database of system-selected files of data that had been updated since the previous incremental dump.
40. RDBMS: General. The RDBMS shall be capable of exploiting MVS/XA and MVS/ESA, when installed at the EOPDC at a later date.
41. The RDBMS shall provide support for the following (COBOL, PL/I) data types: timestamp, decimal value, full word integer, half word integer, character string, varying length character string, date, time, single-precision floating point, double-precision floating point.
42. The RDBMS shall have a facility for evaluating SQL commands and explaining how a query would be executed in order to optimize the performance of the SQL commands and prevent inappropriate or excessive system resource consumption.
43. The RDBMS shall have an associated "data load" utility capability that can be used to load external data into existing files with options such as append or replace, and can optionally create and load new RDBMS files to specific DASD volumes, including files that span multiple volumes.
44. The RDBMS shall have a multi-thread capability with users sharing common re-entrant executable code concurrently.
45. The RDBMS shall support batch and on-line activities concurrently with multiple retrieves and updates on the same database.
46. Recovery/Restart. The RDBMS recovery/restart procedure shall automatically restore the results of completed transactions on the journal log file (or other systems file) that occurred since the last checkpoint.
47. The RDBMS recovery/restart facility shall support a transaction roll backward capability (i.e., replace the "before image" journal entry for each transaction back to a previously defined checkpoint). This procedure shall be DBA activated.
48. The RDBMS recovery/restart procedure shall have database checkpoints periodically recorded on a journal log indicating data integrity to that point in time (i.e., the journal log and database are synchronized).

49. The RDBMS recovery/restart procedure shall automatically restore subschema and undamaged portions of a database up to the most recent checkpoint after a system failure.
50. The RDBMS recovery/restart procedure shall support definable time periods or numbers of transactions processed between RDBMS checkpoints at the systems or database administration level.
51. The RDBMS shall provide a capability to recover the database activity and/or data after a system failure and provide a restart capability that can be completed in a reasonable period of time.
52. The recovery/restart facility shall support a transaction roll forward capability (i.e., restore a database from a backup copy and bring it forward by applying all changes from the journal log from the time of backup until the time of systems failure).
53. The RDBMS shall provide for the capability to automatically back out inflight transactions after system failures. If it is unable to determine whether the transaction was committed, it must record the event and notify the user.
54. Related software and equipment. The contractor shall identify all items of software and equipment not currently installed at the EOPDC that are required for the use and/or maintenance of all proposed systems software.
55. Structured Query Language (SQL). The RDBMS shall use SQL as the Database Definition Language (DDL).
56. The RDBMS shall use SQL as a basic environment for creating and executing command sets.
57. The RDBMS shall use SQL as the Database Manipulation Language (DML).
58. The SQL shall conform to the specifications and requirements of the most recent edition of FIPS PUB 127 in effect at the time of lease/purchase.
59. SQL/HLI Interfaces. The RDBMS shall support a SQL-to-host language interface (HLI) accessible from FIPS standard PL/I, COBOL, and FORTRAN.
60. SQL: Query, Dynamic. The RDBMS shall support ANSI SQL standard for dynamic queries submitted interactively.

61. SQL: Query, Static. The RDBMS shall meet the ANSI SQL standard for static queries embedded in COBOL, and/or PL/I, and/or FORTRAN.
62. Training. RDBMS product training must be commercially available for systems programmers, database administrators, and for application programmers.

Highly Desirable Features/Ranking Factors

1. Bind. Rebinds of user programs should be allowed to take place automatically, if changes in one or more objects have occurred, triggered by any use of the program.
2. Catalog. The RDBMS catalog should be capable of allowing for "comments" to be added to systems tables to provide additional descriptive information.
3. Third Party Product Support. The availability of a significant number of third party software products that work with the RDBMS in the environment specified for this contract would be beneficial.
4. Limitations. Any logical or physical limitations inherent in the proposed RDBMS that would limit growth in either complexity of design or in data volumes need to be identified and considered in the selection.

SECTION D - PACKAGING & MARKINGD.1 PRESERVATION AND PACKING

Preservation, packing and packaging shall be in accordance with good commercial practices to assure delivery at destination and to prevent deterioration of supplies and damages due to hazards of shipping, handling and storage.

D.2 MARKING OF SHIPMENTS

The Contractor shall mark all shipments under this contract with, as a minimum, the Contract Number. The shipments shall also be marked in accordance with standard practice for commercial packaging.

SECTION E - INSPECTION AND ACCEPTANCE

E.1 This section incorporates the following contract clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

<u>TITLE</u>	<u>FAR CITATION</u>
Inspection of Services - Fixed Price	52.246-04
Inspection of Supplies - Fixed Price	52.246-02
Responsibilities for Supplies	52.246-16
Stop Work Order	52.212-13

FAR Citation references the Federal Acquisition Regulation (48 CFR, Chapter 1)

E.2 ACCEPTANCE

Processing of payment on an invoice does not in itself constitute acceptance. Contract performance, or deliveries under a task, will be deemed accepted by the Government upon specific certification of an invoice to that effect by the COTR.

SECTION F - DELIVERIES OR PERFORMANCEF.1 CONTRACT CLAUSES INCORPORATED BY REFERENCE

This section incorporates the following contract clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

<u>TITLE</u>	<u>FAR CITATION</u>
FOB Destination	52.247-34
Diversion of Shipments Under FOB	52.247-54

F.2 PLACE OF PERFORMANCE

Services obtained under this contract may be performed within the Executive Office of the President, located in the New Executive Office Building at 725 17th Street; N.W.; Washington, D.C.

F.3 DELIVERABLES

Deliverables to be provided under this contract are as specified under each task herein or as may be specified in each delivery order upon issuance.

F.4 MEETINGS

The Contractor shall meet with the COTR as may be required at the COTR's place of business. In addition, the Contractor may be asked from time to time to attend meetings with EOP working groups to present briefings and to respond to questions that may arise from the Contractor's deliverables.

REMAINDER OF PAGE NOT USED

SECTION G - CONTRACT ADMINISTRATION DATAG.1. CONTRACTUAL INFORMATION

Contractual interpretation and assistance may be obtained by contacting:

Executive Office of the President
Office of Administration
Procurement and Contracts
Room 5001, New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

ATTN: Thomas L. Taylor
Phone: 202-395-3570

G.2. CONTRACT MANAGEMENT

Notwithstanding the Contractor's responsibility for total management of work assigned during the performance of this contract, the administration of the contract will require maximum coordination between the Government and the Contractor. The Contracting Officer's Technical Representative (identified in paragraph G.3.) will be the Government point of contact during performance of the contract.

G.3. CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE

- a. The Contracting Officer hereby designates the below named individual as the Contracting Officer's Technical Representative (COTR):

Name: Dennis Keating

Address: Executive Office of the President
Office of Administration
Room 4202, New Executive Office Building
725 17th Street, N.W. Washington, D.C. 20503

Phone: 202-395-7323

- b. The COTR is responsible for administering the performance of work under this contract. In no event, however, will any understanding, agreement, modification, change order, or other matter deviating from the terms of this contract be effective or binding upon the Government unless formalized by proper contractual documents executed by the Contracting Officer prior to completion of the contract.

SECTION G - CONTRACT ADMINISTRATION DATA (Continued)

- c. The COTR is responsible for: (1) monitoring the Contractor's technical progress, including the surveillance and assessment of performance and recommending to the Contracting Officer changes in requirements; (2) interpreting the scope of work; (3) performing technical evaluation as required; (4) performing technical inspections and acceptances required by this contract; and (5) assisting the Contractor in the resolution of technical problems encountered during performance. The Contracting Officer is responsible for directing or negotiating any changes in the terms, conditions, or amounts cited in the contract.
- d. For guidance from the COTR to the Contractor to be valid; it must: (1) be consistent with the description of the work set forth in the contract; (2) not constitute new assignments of work or change to the expressed terms, conditions, or specifications incorporated into this contract; (3) not constitute a basis for an extension to the period of performance or contract delivery schedule; (4) not constitute a basis for any increase in the cost.
- e. On all matters that pertain to the contract terms, the Contractor must communicate with the Contracting Officer. Whenever, in the opinion of the Contractor, the COTR requests effort outside the scope of the contract, the Contractor should so advise the COTR. If the COTR persists and there still exists a disagreement as to the proper contractual coverage, the Contracting Officer should be notified immediately, preferably in writing if time permits. Proceeding with work without proper contractual coverage could result in non-payment or necessitate the submittal of costly claims under the contract.
- f. The COTR may be changed by the Government at any time, without prior notice to the Contractor. Written notice to the Contractor will be given by the Contracting Officer to effect any change in COTR(s).

G.4. TECHNICAL DIRECTION

(a). Technical direction, as used herein, will be the overseeing of the Contractor and its staff to insure compliance with all of the items in the contract. It will include elaboration of the Specifications (Section C) by filling in details or otherwise completing the general description of the work set forth by the contract schedule.

SECTION G - CONTRACT ADMINISTRATION DATA (Continued)

(b). No new work assignments, which would require the employment of additional personnel, or which would increase or decrease the estimated costs or period of performance, or affect any provision of this contract, may be made without approval of the Contracting Officer. Program and work modifications will, however, be expected as essential to the conduct of an effective information management program, responsible to changing the needs of management and staff in a dynamic work environment. Such modifications will be accommodated by adjustments in existing programs, mutually agreed upon by the Contracting Officer's Technical Representative (COTR) and the Contractor. Work to be performed under this contract shall be subject to the technical direction of the COTR.

(c). If in the opinion of the Contractor, any instruction or direction issued by the COTR is not provided for in any of the clauses of the contract, the Contractor shall not proceed, but shall notify the Contracting Officer in writing within five (5) days after receipt of any such instruction or direction and shall request the Contracting Officer to modify the contract, accordingly. Upon receiving such notification from the Contractor, the Contracting Officer shall issue an appropriate contract modification or advise the Contractor in writing that, in his/her opinion, the technical direction is within the scope of this clause and does not constitute a change under the Changes Clause of the contract. The Contractor shall thereupon proceed immediately with the direction given.

(d). A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect thereto shall be subject to the provisions of the contract clause entitled "Disputes."

G.5. SUBMISSION OF INVOICES

All invoices shall be submitted to the following address:

Executive Office of the President
Office of Administration
Information Resource Management Division
725 17th Street, N.W.; Washington, DC 20503
Attn: Stacia Cropper, Room 4202 NEOB

SECTION G - CONTRACT ADMINISTRATION DATA (Continued)G.6. INVOICES

(a) An invoice is a written request for payment under the contract for supplies delivered or for services rendered. In order to be proper, an invoice must include as applicable the following:

- (i) invoice date;
- (ii) name of contractor;
- (iii) contract number (including order number, if any) contract line item number, contract description of supplies or services, quantity, contract unit of measure and unit price, and extended total;
- (iv) shipment number and date of shipment (bill of lading number and weight of shipment will be shown for shipments on Government bills of lading);
- (v) name and address to which payment is to be sent (which must be the same as that in the contract or on a proper notice of assignment);
- (vi) name (where practicable), title, phone number and mailing address of person to be notified in event of a defective invoice; and
- (vii) any other information or documentation required by other provisions of the contract (such as evidence of shipment).

Invoices shall be prepared and submitted in quadruplicate (one copy shall be marked "original" unless otherwise specified).

(b) For purposes of determining if interest begins to accrue under the Prompt Payment Act (Public Law 97-177):

- (i) a proper invoice will be deemed to have been received when it is received by the office designated in the contract for receipt of invoices and acceptance of the supplies delivered or services rendered has occurred;
- (ii) payment shall be considered made on the date on which a check for such payment is dated;
- (iii) payment terms (e.g., "net 20") offered by the Contractor will not be deemed a "required payment date;" and
- (iv) the following periods of time will not be included:

SECTION G - CONTRACT ADMINISTRATION DATA (Continued)

(A) after receipt of an improper invoice and prior to notice of any defect or impropriety, but not to exceed 15 days (or any lesser period established by this contract); and

(B) between the date of a notice of any defect or impropriety and the date a proper invoice is received.

(Note: When the notice is in writing, it shall be considered made on the date shown on the notice.)

(REMAINDER OF PAGE NOT USED.)

SECTION H - SPECIAL CONTRACT REQUIREMENTSH.1 TERM OF CONTRACT

The period of performance under this contract is for one (1) year from contract award date.

H.2 ORDER OF PRECEDENCE

In the event of an inconsistency between the provisions of this contract, the inconsistency shall be resolved by giving precedence in the following order: (a) the Schedule (excluding the Specification); (b) Terms and Conditions of the Solicitation, if any; (c) General Provisions; (d) other provisions of the contract, when attached or incorporated by reference; (e) the Specifications; and (f) such portions of the Contractor's Technical Proposal as may be incorporated into the contract.

H.3 ADVERTISING OF AWARD

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the Contractor is endorsed or preferred by the Federal Government, or is considered by the Government to be superior to other firms.

H.4 ON-SITE CONTRACTOR PERFORMANCE

During all operations on Government premises the Contractor shall comply with the rules, regulations and procedures governing the conduct of personnel as expressed by the Executive Office of the President, Office of Administration's written or oral procedures. Within three (3) days after contract award, the Contractor shall submit the names, dates of birth, and social security numbers of all employees who may need access to the EOP complex.

H.5 SECURITY CLEARANCES

It shall be incumbent on the Contractor to provide personnel for work under this contract whose security clearance is not denied. The Contractor shall cooperate with appropriate EOP officials to obtain security passes for all personnel assigned to the EOP facilities. The Government will render every possible assistance to the Contractor in complying with security requirements. (NOTE: This clearance can not be obtained in advance of contract award.)

SECTION H - SPECIAL CONTRACT REQUIREMENTS (Continued)H.6 CONTRACTOR'S LIABILITY FOR INJURY AND/OR DAMAGE

The Contractor shall be liable for damages arising out of injury to employees of the Government (or any other person(s) designated by the Government for any purpose, other than agents or employees of the Contractor), and/or damages to the property of the Government, provided that the injury or damage was caused by the fault or negligence of the Contractor.

H.7 POTENTIAL CONFLICTS OF INTEREST

The Contractor's employees assigned to work on this contract have an affirmative obligation to disclose to the Contracting Officer any personal or business relationship with Government personnel, or financial interests, which could present the appearance of an existing or potential conflict of interest. Failure to do so, if such becomes known by other means could result in a determination of non-responsibility prior to award, or termination of contract after award.

H.8 INSURANCE

In accordance with the clause "Insurance - Work on a Government Installation (Apr 1984)(FAR 52.228-5)" and this schedule, the Contractor shall acquire and maintain during the entire performance period of this contract insurance of at least the following kinds and minimum amounts set forth below:

a. Workman's Compensation and Employers' Liability Insurance in accordance with the amounts specified by the laws of the states in which the work is to be performed under this contract. In the absence of such state laws, an amount of \$100,000 shall be required and maintained.

b. General Liability Insurance: Bodily injury liability in the minimum amount of \$300,000 per occurrence.

c. Automobile Liability Insurance in the amount of; \$100,000 per person and \$300,000 per occurrence for bodily injury and \$10,000 per occurrence for property damage.

H.9 PRIVACY ACT SAFEGUARDS

Details of the safeguards which the contractor may design or develop under this contract shall become the property of the Government and are not to be published or disclosed in any manner without the written consent of the Government. Also, the details of the safeguards which may be revealed to the contractor by the Government in the course of performing under this contract are not to be published or disclosed without the express written consent of the Government.

SECTION H - SPECIAL CONTRACT REQUIREMENTS (Continued)H.10 LEASE

This contract provision provides for the Government to lease from the contractor the selected Relational Data Base Management System (RDBMS) software products.

The Contractor shall furnish and the Government will lease under Task II a transferable lease arrangement for the selected software products for the period March 1, 1991 through September 30, 1991. Prices to the Government shall be as low or lower than those charged the Contractor's most favored customer for comparable quantities under similar terms and conditions. In any event, lease costs to the Government shall not exceed the ceiling amount set forth in Contract Section B.4 (Task II - Supplies) without written consent of the Contracting Officer.

H.11 SPECIAL 8(a) CONTRACT CONDITIONS

The Small Business Administration (SBA) agrees to the following:

(a) To furnish the supplies or services set forth in this contract according to the specifications and the terms and conditions hereof by subcontracting with an eligible concern pursuant to the provisions of section 8(a) of the Small Business Act, as amended (15 U.S.C. 637(a)).

(b) That in the event SBA does not award a subcontract for all or a part of the work hereunder, this contract may be terminated either in whole or in part without cost to either party.

(c) Delegates to the Executive Office of the President (EOP) the responsibility for administering the subcontract to be awarded hereunder with complete authority to take any action on behalf of the Government under the terms and conditions of the subcontract; provided, however, that the EOP shall give advance notice to the SBA before it issues a final notice terminating the right of a subcontractor to proceed with further performance, either in whole or in part, under the subcontract for default or for the convenience of the Government.

(d) That payments to be made under any subcontract awarded under this contract will be made directly to the subcontractor by the Executive Office of the President (EOP).

(e) That the subcontractor awarded a subcontract hereunder shall have the right of appeal from decisions of the Contracting Officer cognizable under the "Disputes" clause of said subcontract.

SECTION H - SPECIAL CONTRACT REQUIREMENTS (Continued)H.12 SPECIAL 8(a) SUBCONTRACT CONDITIONS

(a) The Small Business Administration (SBA) has entered into Contract No. OA1C03 with the Executive Office of the President (EOP) to furnish the supplies or services as described therein. A copy of the contract is attached hereto and made a part hereof.

(b) The Information Management Consultants (IMC), hereafter referred to as the subcontractor, agrees and acknowledges as follows:

(1) That it will, for and on behalf of the SBA, fulfill an perform all of the requirements of Contract No. OA1C03 for the consideration stated therein and that it has read and is familiar with each and every part of the contract.

(2) That the SBA has delegated responsibility for the administration of this subcontract to the Executive Office of the President (EOP) with the complete authority to take any action on behalf of the Government under the terms and conditions of this subcontract.

(3) That it will not subcontract the performance of any of the requirements of this subcontract to any lower tier subcontractor without the prior written approval of the SBA and the designated Contracting Officer of the EOP.

(c) Payments, including any progress payments under this subcontract, will be made directly to the subcontractor by the Executive Office of the President (EOP).

H.13 SECTION 8(a) AWARD

(a) By execution of a contract, the Small Business Administration (SBA) agrees to the following:

(1) To furnish the supplies or services set forth in the contract according to the specifications and the terms and conditions by subcontracting with the Offeror who has been determined an eligible concern pursuant to the provisions of section 8(a) of the Small Business Act, as amended (15 U.S.C. 637(a)).

(2) Except for novation agreements and advance payments, delegates to the Executive Office of the President (EOP) the responsibility for administering the contract with complete authorith to take any action

SECTION H - SPECIAL CONTRACT REQUIREMENTS (Continued)

on behalf of the Government under the terms and conditions of the contract; provided, however that the contracting agency shall give advance notice to the SBA before it issues a final notice terminating the right of the subcontractor to proceed with further performance, either in whole or in part, under the contract.

(3) That payments to be made under the contract will be made directly to the subcontractor by the contracting activity.

(4) To notify the Executive Office of the President Contracting Officer immediately upon notification by the subcontractor that the owner or owners upon whom 8(a) eligibility was based plan to relinquish ownership or control of the concern.

(b) The offeror/subcontractor agrees and acknowledges that it will, for and on behalf of the SBA, fulfill and perform all of the requirements of the contract

H.14

PRE-CONTRACT COST AUTHORIZATION

This contract provision authorizes the Contractor to incur costs in the amount not to exceed \$30,000 under the performance of "Task Number I". This authorization is effective November 15, 1990 and is issued pending SBA approval of the final contract documents.

H.15

TRAVEL

The Contractor may bill the EOP for actual cost incurred for local travel only when occurrence is in the performance of the contract. The Contractor shall submit to the COTR documentation to support all local travel expenses incurred up to the not-to-exceed amount of \$500.00 as set forth in the contract. The Contractor shall not be reimbursed for its hourly wage or mileage/parking when travel is from home to the Executive Offices of the President. Any travel other than local travel must have prior approval of the COTR.

Local travel is defined as travel within a 50 mile radius of the Washington D.C. metropolitan area. Local travel incurred shall be invoiced separately.

SECTION - H SPECIAL CONTRACT REQUIREMENTS (Continued)H.16 PRIVACY ACT NOTIFICATION

The Contractor may be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

H.17 PRIVACY ACT

(a) The Contractor agrees to--

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies--

- (i) The systems of records; and
- (ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

SECTION H - SPECIAL CONTRACT REQUIREMENTS (Continued)

(c)(1) "Operation of a system records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(d) Inclusion of this clause in any contract will not cause records belonging to a component within the Executive Office of the President to become subject to the Privacy Act if they would not otherwise be subject to the Privacy Act.

(REMAINDER OF PAGE NOT USED)

SECTION I - CONTRACT CLAUSES

I.1. The following clauses are hereby incorporated by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

("FAR Citation" in the following list refers to the Federal Acquisition Regulation (48 CFR Chapter 1)).

<u>TITLE</u>	<u>FAR CITATION</u>
Definitions	52.202-01
Covenant Against Contingent Fees	52.203-05
Officials Not to Benefit	52.203-01
Gratuities	52.203-03
Examination of Records by Comptroller General	52.215-01
Audit-Negotiation	52.215-02
Price Reduction for Defective Cost or Pricing Data	52.215-22
Price Reduction for Defective Cost or Pricing Data-Modifications	52.215-23
Subcontractor Cost or Pricing Data	52.215-24
Subcontractor Cost or Pricing Data Modifications	52.215-25
Indefinite Quantity	52.216-22
Utilization of Small Business Concerns and Small Disadvantaged Business Concerns	52.219-08
Special 8(a) Contracts Conditions	52.219-11
Special 8(a) Subcontracts Conditions	52.219-12
Utilization of Women-Owned Small Businesses	52.219-13
Limitations on Subcontracting	52.219-14
Preference for Labor Surplus Area Concerns	52.220-01
Utilization of Labor Surplus Area Concerns	52.220-03
Labor Surplus Area Subcontracting Program	52.220-04
Notice to the Government of Labor Disputes	52.222-01
Convict Labor	52.222-03
Contract Work Hours and Safety Standards	52.222-04
Overtime Compensation--General Walsh-Healey Public Contracts Act	52.222-20
Equal Opportunity	52.222-26
Affirmative Action for Special Disabled Vietnam Era Veterans	52.222-35
Affirmative Action for Handicapped Workers	52.222-36

SECTION I - CONTRACT CLAUSES (Continued)

Service Contract Act of 1965	52.222-41
Clean Air and Water	52.223-02
Certification Regarding a Drug Free Workplace	52.223-05
Drug Free-Workplace	52.223-06
Buy American Act-Supplies	52.225-03
Buy American Act-Trade Agreements	52.225-09
Act-Balance of Payments Program	
Certain Communist Areas	52.225-11
Patent Indemnity	52.227-03
Insurance-Work on a Government Installation	52.228-05
Federal, State and Local Taxes	52.229-03
Cost Accounting Standards	52.230-03
Administration Cost Accounting Standards	52.230-04
Disclosure and Consistency of Cost Accounting Standards	52.230-05
Payments	52.232-01
Discounts for Prompt Payment	52.232-08
Limitation on Withholding of Payments	52.232-09
Extras	52.232-11
Progress Payments	52.232-16
Interest	52.232-17
Assignment of Claims	52.232-23
Disputes-Alternate I	52.233-01
Protection of Government Buildings, Equipment, and Vegetation	52.237-02
Changes--Fixed-Price	52.243-01
Subcontracts Under Fixed-Price	52.244-01
Contracts Alternate I	
Competition in Subcontracting	52.244-05
Property Records	52.245-01
Government Property (Fixed-Price Contracts)	52.245-02
Termination for Convenience of the Government (Fixed-Price)	52.249-08
Default (Fixed-Price Supply and Service	52.249-08
Remedies for Illegal or Improper Activity	52.302-10

SECTION K - CERTIFICATIONS AND REPRESENTATIONSK.1. CERTIFICATE OF INDEPENDENT PRICE DETERMINATION (APR 1984)

(a) The offeror certifies that --

(1) The prices in this offer have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror or competitor relating to (i) those prices, (ii) the intention to submit an offer, or (iii) the methods or factors used to calculate the prices offered;

(2) The prices in this offer have not been and will not be knowingly disclosed by the offeror, directly or indirectly, to any other offeror or competitor before bid opening (in the case of a formally advertised solicitation) or contract award (in the case of a negotiated solicitation) unless otherwise required by law; and

(3) No attempt has been made or will be made by the offeror to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.

(b) Each signature on the offer is considered to be a certification by the signatory that the signatory --

(1) Is the person in the offeror's organization responsible for determining the prices being offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contrary to subparagraphs (a)(1) through (a)(3) above; or

(2) (i) Has been authorized, in writing, to act as agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to subparagraphs (a)(1) through (a)(3) above: [Insert full name of person(s) in the offeror's organization responsible for determining the prices offered in this bid or proposal, and the title of his or her position in the offeror's organization.]

Douglas K. Stevens, Jr., Senior Vice President

Donald C. Reynolds, Vice President

John Locke, Vice President

(ii) As an authorized agent, does certify that the principals named in subdivision (b)(2)(i) above have not participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) above; and

(iii) As an agent, has not personally participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) above.

SECTION K - CERTIFICATIONS AND REPRESENTATIONS (Continued)

(c) If the offeror deletes or modifies subparagraph (a)(2) above, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the disclosure.

K.2. CONTINGENT FEE REPRESENTATION AND AGREEMENT (APR 1984)

(a) Representation. The offeror represents that, except for full-time bona-fide employees working solely for the offeror, the offeror --

[Note: The offeror must check the appropriate boxes. For interpretation of the representation, including the term "bona-fide" employee," see Sub-part 3.4 of the Federal Acquisition Regulation.]

(1) has, has not employed or retained any person or company to solicit or obtain this contract; and

(2) has, has not paid or agreed to pay to any person or company employed or retained to solicit or obtain this contract any commission, percentage, brokerage, or other fee contingent upon or resulting from the award of this contract.

(b) Agreement. The offeror agrees to provide information relating to the above Representation as requested by the Contracting Officer and, when subparagraph (a)(1) or (a)(2) is answered affirmatively, to promptly submit to the Contracting Officer --

(1) A completed Standard Form 119, Statement of Contingent or Other Fees, (SF 119); or

(2) A signed statement indicating that the SF 119 was previously submitted to the same contracting office, including the date and applicable solicitation or contract number, and representing that the prior SF 119 applies to this offer or quotation.

K.3. TYPE OF BUSINESS ORGANIZATION

The offeror, by checking the applicable box, represents that it operates as a corporation incorporated under the laws of the State of Virginia, an individual, a partnership, a nonprofit organization, or a joint venture.

K.4. AUTHORIZED NEGOTIATORS

The offeror represents that the following persons are authorized to negotiate on its behalf with the Government in connection with this request for proposals or quotations; [list names, titles, and telephone numbers of the authorized negotiators].

Douglas K. Stevens, Jr., Senior Vice President	703/893-3100
Donald C. Reynolds, Vice President	703/893-3100
John L. Locke, Vice President	703/893-3100

SECTION K - CERTIFICATIONS AND REPRESENTATIONS (Continued)**K.5. CORPORATE CERTIFICATION**

The following certification is to be executed, corporate seal affixed, and returned with any proposal submitted:

CERTIFICATE

I, William D. Kee, certify that I am the Secretary of the corporation named as Offeror herein; that Donald C. Reynolds, who signed this offer on behalf of the Contractor, was then the Vice President of said Corporation; that said offer was duly signed for and in behalf of said Corporation by authority of its governing body and that the signing of the offer by Donald C. Reynolds was within the scope of his Corporate power.

William D. Kee

(SIGNATURE)

CORPORATE SEAL

K.6. SMALL BUSINESS CONCERN REPRESENTATION

The offeror represents and certifies as part of its offer that it (x) is, () is not a small business concern and that (x) all, () not all supplies to be furnished will be manufactured or produced by a small business concern in the United States, its possessions, or Puerto Rico. "Small business concern," as used in this provision, means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation.

K.7. SMALL DISADVANTAGED BUSINESS CONCERN REPRESENTATION

(a) Representation. The offeror represents that it (x) is, () is not a small disadvantaged business concern.

(b) Definitions.

"Asian-Indian American," as used in this provision, means a United States citizen whose origins are in India, Pakistan, or Bangladesh.

"Asian-Pacific American" as used in this provision, means a United States citizen whose origins are in Japan, China, the Philippines, Vietnam, Korea, Samoa, Guam, the U.S. Trust Territory of the Pacific Islands, the Northern Mariana Islands, Laos, Cambodia, or Taiwan.

"Native Americans," as used in this provision, means American Indians, Eskimos, Aleuts, and native Hawaiians.

SECTION K - CERTIFICATIONS AND REPRESENTATIONS (Continued)

"Small business concern," as used in this provision, means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria and size standards in 13 CFR 121.

"Small disadvantaged business concern," as used in this provision, means a small business concern that (1) is at least 51 percent owned by one or more individuals who are both socially and economically disadvantaged, or a publicly owned business having at least 51 percent of its stock owned by one or more socially and economically disadvantaged individuals and (2) has its management and daily business controlled by one or more such individuals.

(c) Qualified groups. The offeror shall presume that socially and economically disadvantaged individuals include Black Americans, Hispanic Americans, Native Americans, Asian-Pacific Americans, Asian-Indian Americans, and other individuals found to be qualified by the SBA under 13 CFR 124.1.

K.8. WOMEN-OWNED SMALL BUSINESS REPRESENTATION

(a) Representation. The offeror represents that it () is, (x) is not a women-owned small business concern.

(b) Definitions.

"Small business concern," as used in this provision, means a concern, including its affiliates, that is independently owned and operated, not dominate in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria and size standards in 13 CFR 121.

"Women-owned," as used in this provision, means a small business that is at least 51 percent owned by a woman or women who are in U.S. citizens and who also control and operate the business.

K.9. WALSH-HEALEY PUBLIC CONTRACTS ACT REPRESENTATION

The offeror represents as a part of this offer that the offeror is (x) or is not () a regular dealer in, or is (x) or is not () a manufacturer of, the supplies offered.

K.10. PREVIOUS CONTRACTS AND COMPLIANCE REPORTS

The offeror represents that --

(a) It (x) has, () has not participated in a previous contract or subcontract subject either to the Equal Opportunity clause of this solicitation, the clause originally contained in Section 310 of

SECTION K - CERTIFICATIONS AND REPRESENTATIONS (Continued)

Executive Order No. 18925, or the clause contained in Section 201 of Executive Order No. 11114;

(b) It (x) has, () has not, filed all required compliance reports; and

(c) Representations indicating submission of required compliance reports, signed by proposed subcontractors, will be obtained before subcontract awards.

K.11. AFFIRMATIVE ACTION COMPLIANCE

The offeror represents that (a) it (x) has developed and has on file, () has not developed and does not have on file, at each establishment, affirmative action programs required by the rules and regulations of the Secretary of Labor (41 CFR 60-1 and 60-2), or (b) it () has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

K.12. CLEAN AIR AND WATER CERTIFICATION

The Offeror certifies that --

(a) Any facility to be used in the performance of this proposed contract is (), is not (x) listed on the Environmental Protection Agency List of Violating Facilities;

(b) The Offeror will immediately notify the Contracting Officer, before award, of the receipt of any communication from the Administrator, or a designee, of the Environmental Protection Agency, indicating that any facility that the Offeror proposes to use for the performance of the contract is under consideration to be listed on the Environmental Protection Agency List of Violating Facilities; and

(c) The Offeror will include a certification substantially the same as this certification, including this paragraph (c), in every nonexempt subcontract.

SECTION K - CERTIFICATIONS AND REPRESENTATIONS (Continued)**K.13. BUY AMERICAN CERTIFICATE**

The offeror certifies that each end product, except those listed below, is a domestic end product (as defined in the clause entitled "Buy American Act—Supplies"), and that components of unknown origin are considered to have been mined, produced, or manufactured outside the United States.

Excluded End Products

Country of Origin

(List as necessary)

Offerors may obtain from the contracting officer lists of articles, materials, and supplies excepted from the Buy American Act (listed at 25.108 of the Federal Acquisition Regulation).

K.14. GSA ADP SCHEDULE CONTRACT INFORMATION

a. Offeror shall state whether or not he has a current GSA ADP Schedule contract for services/equipment identified in this solicitation.

_____ Yes

 x No

b. If the answer to a, above, is "Yes" cite the applicable contract number and expiration date below.

c. Notwithstanding your response to subparagraphs a and b above, when an ordering agency finds that an identical product (make and model number) or service is available from another source at a delivered price lower than the GSA contract price, such agency is free to purchase items at the lower price without violating the GSA requirements.

K.15. CONTRACTOR REPRESENTATION

Unless the Contractor expressly states otherwise in his proposal, where functional requirements are expressly stated as part of the requirements of this solicitation, the Contractor, by responding, represents that in its opinion the systems/items proposed are capable of meeting those requirements. However, once the systems/items are accepted by the Government, contractor responsibility under this clause ceases. In the event of any inconsistency between the detailed specification and the functional specification contained in the solicitation, the former will control.

52.219-11 SPECIAL 8(a) CONTRACT CONDITIONS
(FEB 1990)

The Small Business Administration (SBA) agrees to the following:

(a) To furnish the supplies or services set forth in this contract according to the specifications and the terms and conditions hereof by subcontracting with an eligible concern pursuant to the provisions of section 8(a) of the Small Business Act, as amended (15 U.S.C. 637(a)).

(b) That in the event SBA does not award a subcontract for all or a part of the work hereunder, this contract may be terminated either in whole or in part without cost to either party.

(c) Except for novation agreements and advance payments, delegates to the *Exec. Office of the President* the responsibility for administering the subcontract to be awarded hereunder with complete authority to take any action on behalf of the Government under the terms and conditions of the subcontract; provided, however, that the *Exec. Office of the Pres.* shall give advance notice to the SBA before it issues a final notice terminating the right of a subcontractor to proceed with further performance, either in whole or in part, under the subcontract for default or for the convenience of the Government.

~~(d) That payments to be made under any subcontract awarded under this contract will be made directly to the subcontractor by the *Executive Office of the President*.....~~

(e) That the subcontractor awarded a subcontract hereunder shall have the right of appeal from decisions of the Contracting Officer cognizable under the "Disputes" clause of said subcontract.

(f) To notify the *Exec. Office of Pres.* Contracting Officer immediately upon notification by the subcontract that the owner or owners upon whom 8(a) eligibility was based plan to relinquish ownership or control of the concern.

(End of clause)

Mr. PETERSON. Mr. Chairman, you will see in there that the Bush administration was attempting to establish the same kind of Data Base as we are examining here today. And I really think that some of your comments here are a little misleading in terms of what actually is in the Data Base. I think that there is some question about the amount of money that was spent. Someone who has been involved in this business and has been involved in this somewhat in the private sector, I think that the amount of money that they spent was probably a little excessive, although the contract with the Bush administration, I think, probably could be criticized similarly.

You know, your characterization that somehow or another this contains all kinds of information about contributors, there's 200,000 people in this Data Base, and there's only 774 that have any kind of mention of the word "contributor" in their records. From what I know, there is no information about contributions in these records. There's information about a relationship to the First Family and issues and party affiliation.

But I would like to call your attention to the document that I gave you. Under the system that the Bush administration ordered, one of the things on page 25 of 59, they want to maintain a list of names and addresses of individuals identified as important to the President, which is similar to, I think, what you are complaining about with this Data Base. They also wanted to maintain a list of contribution leaders to the Thousand Points of Light Program used for sending letters to select groups, which is, I think, exactly what you are complaining about.

The point is that I think that every administration probably had something similar to this. You know, back in the old days they had it on a Rolodex or some kind of a not automated system probably. So at least at this point, I haven't really seen any kind of sinister use of this system.

From my point of view, they might be criticized for their lack of using the system because, basically, it has a lot more capability than what they are actually using it for. They haven't developed a good system to get the information in, and most of the information, as near as I can tell, that got into the system came through the social office, where they were figuring out who to invite to parties and who was at these parties. And then that information got transferred over to the Data Base, and they initially had this idea that they were going to have people around the White House put information into the system, but like happens with a lot of these systems, that never really got established, and that information never really got organized in any kind of consistent manner.

So I am not saying that there may not be something in here that I would have some problems with, but I haven't been able to find it at this point, and I am unaware that the GAO has been able to find anything of any major importance at this point, either.

And, you know, we will just have to see whatever else we dig up. So I think that, you know, your characterization, I think, is a little bit overblown as to what may or may not be in this system, and, you know, that's—I would just like to put that into the record as kind of a counterpoint.

And I am, again, concerned that the White House isn't here today. I don't know if you are going to have them back at some later date to talk about this situation, but it seems to me that they should have been here to tell their side of the story.

Mr. MCINTOSH. If you think it is appropriate for us to issue that invitation, I will gladly work with you to try and work that out.

Mr. PETERSON. I am not sure we need to have another hearing, but, I mean, I think it would have been better, maybe, if they would have been here.

You know, the other thing that happened during this whole process is these letters that went back and forth, I think could have been solved had you and your staff gone down to the White House earlier, like I did, rather than send letters back and forth. But I guess that is water over the dam at this point.

So I guess we just move—I would hope that we would move ahead at this point and try to look at the facts of what is in the system, you know. And if we are going to continue along this line and continue to investigate, you know, I am not so sure we shouldn't go back and try to reconstruct what happened in the Bush administration, whether they kept this same kind of information. As I understand it, they erased all of this at the time that the Clinton administration came in. So is that appropriate? You know, should that information be available so we can tell what happened back during the Bush administration? Did they keep this same kind of information? Were they tracking contributors? I don't think we are going to know because they, as I understand, erased all of this, and it was eliminated when the Clinton administration came in. So I think that is a question.

And, you know, in your comments about this kind of information being illegal if it was Members' of Congress computer, maybe we ought to investigate some of the leaders of the Congress in both parties to see whether or not they have this kind of information in their Data Bases, because I will bet you we will find some Members of Congress who have similar kinds of information in their official Data Base, in terms of people that they interact with and information about those people, and, you know, maybe this committee ought to expand and not just look at the White House. Maybe we ought to look at some of the leaders of the Congress and see if, in fact, they are following the letter of the law.

Mr. MCINTOSH. Let me mention to you, I have talked to Bill Thomas about this, and if we have any indication of that, I am sure he would conduct a very thorough investigation because he feels very strongly about this and has worked to create rules to prohibit exactly this type of activity.

Mr. PETERSON. Well, my point is that some of what you are complaining about is just—I mean, you can look at this two different ways, but, I mean, we can take—as I understand it, we can take political information from our campaigns and put it into our official Data Bases and use it then in our official capacities. You cannot take—once the information is in the system, you cannot take it back out of the system, back into your political campaign.

So some of what you are complaining about here is information that the White House took from their lists, you know, the Vice President's list, the President's list, that they had prior to becom-

ing elected and used that as a basis to start their Data Base. Well, I think probably most Members of Congress do the same kind of thing when they are elected.

Mr. MCINTOSH. Let me clarify that, because there is a very important difference. You can't take information from your campaigns. You can take the official voters lists, but they have a screening mechanism that even there they take out any party affiliation. So you are not allowed as a Member of Congress to designate people as Democrats or Republicans.

Mr. PETERSON. Maybe we ought to change the law and say that the White House can't keep that information as well. But out of 200,000 people that are on the system, there is only 7,252 that have party affiliation. So it doesn't look like there was any big, huge, massive effort to determine what every Member—every person that is on this list, what their political party affiliation is. You know, so that is a very small percentage of the whole Data Base. And maybe we ought to look at some of those issues.

Mr. MCINTOSH. Actually, apparently the White House has provided you with some information about the Data Base that they have not given to the subcommittee. Would you be willing to submit that for the record?

Mr. PETERSON. Absolutely.

Mr. MCINTOSH. Thank you.

Mr. PETERSON. This is information that I asked—when I went down there in early—late July or early August and went through the Data Base, I asked for them to run these different fields to find out how many people have information in some of these different fields. So, as I say, they have—774 out of 200,000 have contributions; 7,000 have ethnicity, field filled in. You know, as I say, there doesn't appear to be any kind of a big push to get all of that information in. I mean, I looked at my own record. I have the party affiliation of myself in there. That would make sense.

So I think a lot of those are probably Members of Congress, other kinds of political people, that get in there because we are political.

So, you know, I just think that the rhetoric around this is a little overblown at this point for what we know, and I just hope that we would focus in on what the actual facts are and not blow this way out of proportion until we know.

Mr. MCINTOSH. Let me just state for the record that the President's spokesman indicated that somewhat less than half are contributors, and some of the people like Arthur Coia, they don't have anything down for political affiliation, but then in the source section, they clearly indicate that he is there because he is a top 20 supporter of President Clinton's.

Mr. PETERSON. But that could have come out of a list, you know, when they first came here, and he had some kind of a Data Base that he kept and moved that—the only way they could get information into the system was to move it in from those areas, you know. So, I mean, I'm not sure there is anything sinister about that.

Mr. MCINTOSH. That is what we want to find out.

Mr. PETERSON. That could be how you put information together.

Mr. MCINTOSH. Let's begin with this first panel of witnesses. Let me call forward the panel from the General Accounting Office, Mr.

Jack Brock, Mr. Keith Rhodes and John Hess. If I could ask each of you to raise your right hand and repeat after me.

[Witnesses sworn.]

Mr. MCINTOSH. Thank you. Let the record show that each of the witnesses answered in the affirmative.

By the way, for a point of clarification, Chairman Clinger has asked that we ask all witnesses to be sworn so we are not selecting out any individual witness.

STATEMENTS OF JACK BROCK, DIRECTOR, INFORMATION MANAGEMENT ISSUES, GENERAL ACCOUNTING OFFICE; KEITH RHODES, TECHNICAL ASSISTANT DIRECTOR, OFFICE OF THE CHIEF SCIENTIST, GENERAL ACCOUNTING OFFICE; AND RON HESS, GENERAL ACCOUNTING OFFICE

Mr. MCINTOSH. Mr. Brock, you have a prepared statement for us today.

Mr. BROCK. Yes, Mr. Chairman, I do.

If I could just briefly summarize the statement and ask that you submit it into the record.

Mr. MCINTOSH. Seeing no objection, we will submit the entire statement for the record.

Mr. BROCK. You have already introduced Keith Rhodes on my right and Ron Hess on my left, but I would like to acknowledge their leadership and direction during the course of the audit. Keith is an Assistant Technical Director in our Office of Chief Scientist, and Ron is a senior information systems analyst within my group.

You asked us early on, I want to stress this, to do a technical review of the White House Data Base. You wanted us to determine who uses it, the source of information populating the Data Base, and to evaluate the performance and operational characteristics of the Data Base. And I want to stress that the review that we did of the White House Data Base was very similar to reviews that we might do of Data Bases in other government organizations.

The Data Base was developed, began to be developed, in 1994, and it was designed primarily to facilitate contacts that the White House had with individuals outside the White House, individuals that were important to the Presidency.

Among other things, the Data Base, as I indicate in my statement, was used for developing invitation lists for White House events; for providing information to individuals; to prepare thank you notes, holiday cards and other correspondence; and the Data Base contains a wide range of information going from names, addresses, phone numbers, Social Security numbers, contributor information, dates of birth, and then ranging to individual relationships with the First Family, as well as political affiliations. There are about 200,000 entries in the Data Base. We are not sure how many of those are individuals and how many might be duplicate accounts.

In commenting on the three elements of our review, I just want to eliminate one right now and stress that this is an interim review. We have not yet completed our audit. We don't have yet enough information on the source of information to be able to comment on that today. So we are going to reserve that for our final report.

In terms of users of the Data Base, we interviewed the principal users of the Data Base, and I think for the most part they were pleased with the system. They were generally satisfied. For those that had had experience with the legacy systems that had been in use at the White House before the White House Data Base was in place, they found it easier to use, they found it more responsive, and it generally reflected their needs. And I think in part this is because the developers went through a very elaborate process of ascertaining user needs and developing and designing the Data Base. One of the flaws in the process they used, however, was they built a very elaborate system that reflected everybody's wants, I think, instead of actually reflecting the requirements of the system, and we will get into that in a little bit.

But we interviewed—as you indicated, I think, there is about 150 people, somewhere in that neighborhood, had accounts. About 100 people, again, in that neighborhood, have actually used the system, and when you break that down even further, we reviewed the—examined the user accounts, things like that, we identified about 25 users and identified the top 10 users and interviewed all of them.

Our concern, when we did the technical review, dealt primarily in two areas: One, in how the system actually operates and performs. The system is supposed to be a relational Data Base. The way it has been designed, however, it's more of a sequential index and doesn't really perform as a Data Base. As a result, it's fairly slow. It has 125 individual tables in the Data Base, and when you try to access it or do any sort of search, its performance is hampered by having to go across a very wide range of tables.

A critical aspect in this, that even though users themselves may not see any sort of effect right now, is that the White House has had to turn off two key aspects of the system in order not to take performance hits. One, and we are going to discuss this in a little bit more detail later on, is that they were not able to turn on the audit trail. That is not on. They have indicated to us that they did not turn that on because it would unnecessarily—or not unnecessarily, but would severely limit the performance of the system.

Second, they did not turn on the capability of doing the referential integrity checks. Very simply, these are the things that you do, the edit checks and things, as you are entering information or getting information on, it checks, does this make sense? And it's based on preestablished rules that are common in most Data Bases. This was not turned on also because of system administrators' concerns that it would affect drastically the performance of the White House Data Base.

So we believe that as a result of the structure of the Data Base, the way it was put together, the vast number of tables, and the fact that they didn't take advantage of the relational capabilities of the Data Base, is that they have had to make some compromises in areas which affect their internal controls. And that's our second area that I would like to briefly discuss.

I would like to refer to Circular A-130, which is put out by the Office of Management and Budget and effectively lays out the needs for policy, rules and behaviors governing system use, training and the need to incorporate good controls. I would like to make one quote directly from A-130: "It has long been recognized that

the greatest harm has come from authorized individuals engaged in improper activities, whether these are intentional or accidental." And a concern that we have with the White House office Data Base is that the internal controls are not fully implemented.

I think everyone would stipulate that the White House Data Base has important, sensitive information and, further, that this information is used by a number of offices in the White House to perform critical mission needs. And the White House has taken, we believe, several very positive steps to create a system of internal controls. For example, they have a very good system of individualized, personalized training. Most users are trained on a one-on-one basis, which can last anywhere from an hour to several days, depending upon the application. Users are required to sign a document stating they will take measures to protect information, including establishing and protecting passwords, logging out when leaving their computers and reporting unauthorized access to the system. We reviewed their files, and, in fact, these documents are in place.

Password access is required to enter the system, and a warning screen appears, as I am sure you observed, to inform the user that information within the Data Base is for official use only. The Data Base has a very effective defense against outside intruders or hackers that might try to break into the system.

And last, as noted in the letters back to you, they have established controls to limit access to certain portions of the Data Base to authorized users, and, further, they stated that only a limited number of users have authority to print reports.

Even with these processes in place, though, we found that a lot more needs to be done. For example, you don't create a Data Base unless you intend to use it to a reasonable effective extent. There are no user manuals that are widely distributed. Only one user of all those we interviewed had a user manual. We believe that this limits the effectiveness of people knowing when to input information, what to look for, what sort of controls should be in place, and will ultimately limit the effectiveness of the Data Base. In other words, if you have gone to the expense of establishing a Data Base, you want to make sure that it reflects accurate information, that it's completed and that everyone within your office is following generally the same processes and procedures.

We found that in some instances, the processes weren't followed from office to office. While some offices clearly had some good internal processes to that office, others were much more informal about the use.

We found that even though most users could effectively navigate the system, that in some cases we found that duplicate information was continuing to be used and entered, and at some times information was entered into the wrong field; further, that even though the White House has established security policies regarding passwords, et cetera, the system does not require frequent changes in passwords, and only one of the application users that we interviewed had, in fact, changed their password since they had been on the system. I think typically in most business applications, this goes from anywhere from 1 to 3 months. In GAO, for example, we are forced to change our password every 3 months.

And even though the controls are present that would limit the printing of reports, in fact, anyone can do a screen print if they desire, if they have Netware printing; and anyone can use a clipboard feature, which is present on Windows, which they use to effectively capture the information on the screen, download it to a clipboard, and then download that to a WordPerfect file and then e-mail it. The White House does have, though, in fact, one control which they do a sample of outgoing e-mail, and this is, in fact, one measure or one control that should be in place. I am not sure that it's enough, however.

And most importantly, and this is an area that we are in complete agreement with the White House, is there is no audit trail. And I want to go back to my comments on A-130, which states that accountability is normally established by identifying and authenticating users and subsequently tracing actions on the system to the user that initiated them.

The White House, I think, can effectively determine who last changed information on a particular node, but it cannot do the tracing. If they had the audit capability that's present in Sybase, they could monitor and react to attempts to log on and log off the system. They could look at the execution of update and delete and insert operations that might take place. They could look at restarts of the system and a number of things that they are presently not able to do.

So to sum up this, we believe that while the White House has taken some steps that are good to initiate controls, that they do not yet have a proper and complete control environment.

That concludes my summary, Mr. Chairman. We would be happy to respond to questions that you or the other Members might have.

[The prepared statement of Mr. Brock follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Economic Growth,
Natural Resources, and Regulatory Affairs
Committee on Government Reform and Oversight
House of Representatives

For Release
on Delivery
Expected at
10 a.m.
Tuesday
September 10, 1996

**INFORMATION
MANAGEMENT**

**Technical Review of the White
House Data Base**

Statement of Jack L. Brock, Jr.
Director, Information Resources Management/General
Government Issues
Accounting and Information Management Division



Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in the Subcommittee's hearings on the White House Data Base. You requested that we do a technical review of the data base to determine who uses it, to determine the source of information populating the data base, and to evaluate the performance and operational components of the data base. Today I will provide an interim update on data base users and operational components of the data base. Additionally, I will briefly describe how the data base is configured and how it works. We do not yet have enough information to provide meaningful comments on data source and will provide that information at a later date.

In performing our review, we reviewed technical manuals and other documentation for the products supporting the data base. We reviewed documentation showing how users are assigned access rights to data base data. Further, we reviewed the data base's process models, computer programs, and directory structures;¹ toured the computer center where the main data base computer is located; and ran a small number of data base queries to initially sample the data base population. We also conducted interviews with the most active data base users as well as with the data administrator and the primary data base administrator.

WHITE HOUSE DATA BASE CONFIGURATION

The White House Data Base was developed in 1994 to facilitate contacts with individuals and organizations who are important to the Presidency. It replaced a number of existing data bases with a single system which was intended to be easy to use and provide a greater level of service to a variety of users. The system has been operational since August 1995.

Among other things, the data base is used for developing invitation lists for White House events and for providing information to help prepare thank you notes, holiday cards, and other correspondence. As such, the information contained on the data base ranges from names, addresses, phone numbers, social security numbers, contributor information, and dates of birth to individual relationships to the First Family and political affiliations. According to the White House, the data base contains personal information on about 200,000 individuals.

In developing the data base, the White House used a widely accepted approach--Joint Application Development. Under this approach, users meet with programmers in a more intensive design session than usual--with the goals of eliminating rewrites of user interfaces and paving the way for faster application development. Development of the data base began with a series of technical interviews with potential users to determine, among other things, the

¹A table of identifiers and references to the corresponding data items.

sources of the data for the data base and the extent to which the data would be shared with nonfederal entities or individuals.

Once these interviews were concluded, design and development elements were pursued on several fronts. First, potential users were asked to review functional aspects of the system and provide feedback. Second, the system architecture² was developed and implemented based on detailed requirements and joint design elements provided by the customers and others.

The data base operates on and is accessible through the White House's local area network, or LAN.³ While more than 1,600 users are authorized to access the LAN, less than 150 users have been given access to the data base and even fewer actually use the data base. The products supporting the White House LAN, operating system, and data base system are widely used in the government and commercial sectors. The LAN uses version 3.12 of Novell's network operating system. The data base runs on Microsoft's Windows NT operating system using Sybase's System 10 data base management system.

Sybase's System 10 is a relational data base management system, which is a system that allows both end-users and application programmers to store data in, and retrieve data from, data bases that are perceived as a collection of relations or tables. The data base is comprised of 125 tables. Data is input to and retrieved from these tables using simple screens and drop-down menus.

Sybase's System 10 is built with published and readily available interface specifications. It is open to the extent that anyone can write a program that will connect to the server.⁴ This is unlike traditional proprietary data base management systems, which could be accessed only with vendor-supplied tools or programs written with vendor-specific languages and compilers.

²A system architecture is the logical and physical layout of a system that includes hardware, software, communications, data management, and security.

³A local area network is a group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables the computers to interact with each other.

⁴A stand-alone computer in a local area network that holds and manages the data base.

GAO OBSERVATIONS ON USERS, DATA SOURCE, AND OPERATING PROCESSES AND PERFORMANCE

In developing the data base, the White House acquired well-established, commercially available products and created a system that users we interviewed were generally satisfied with. However, as I will discuss in more detail, the design of the data base limits system performance. Further, the system--while having in place some internal controls--needs additional controls to assure the integrity and accuracy of data.

Data Base Use and User Satisfaction

As noted earlier, data base users primarily use the data base as a tool for maintaining contact with individuals and organizations important to the Presidency. Users told us that they were generally satisfied with the system.

Less than 100 White House staff actually use the system, and only about 25 make moderate to heavy use (relative to other users) of the system--with the heaviest users representing the White House Social Office, Personal Correspondence Office, and Outreach Office, as well as system administrators. We examined user accounts and interviewed those staff making heavy use of the system in terms of amount of data both input to and read from the system. These included two staff in the Social Office, one in the Outreach Office, two on the Personal Correspondence staff, the data base data administrator, and a Sybase system administrator. We also interviewed four other business users and a system administrator who represent less heavy users of the system.

Social Office personnel use the system to assist in developing invitation lists and planning state dinners and other events. Personal Correspondence personnel use the data base to help compose letters for the President. In doing so, they retrieve information from the data base on addresses, names of family members, White House events attended, and how the correspondent knows the President. The Outreach user we interviewed entered data into the data base for use in generating lists of holiday card recipients. Many users supplement the data base with information from manually accessed address lists. All those users we interviewed who had used the prior systems believed that the new system was better, and--for some users--the system is critical to their ability to complete their tasks.

System administrators--who account for about 10 percent of all people who have accessed the data base--manage the system and maintain data base information. For example, they perform system backups, troubleshoot, and perform routine maintenance in the normal course of managing the system.

Operating Characteristics

The individual components supporting the data base--the network, server, and data base engine--are individually well-regarded and could be considered to be leading edge components for business applications similar to those run by the White House. However, the strength of the individual system components has been diminished by the design of the data base itself. Specifically, in developing the system, the White House attempted to meet all user requirements for a large array of potential information needs. Rather than take advantage of the relational data base capabilities of Sybase, the designers established a one-to-one relationship between the logical and physical attributes of the data base resulting in 125 tables. The data base operates more as an index sequential data base where relationships between and among data elements have to be established across many tables. This contributes to increased system overhead (requires the system to process additional steps) and thus taxes the performance capabilities of the system.

Because the data base has relatively few users and is an improvement over what users had been using, individual users have probably not been affected by the data base design. However, if demand increased, system performance could unnecessarily degrade.

In order to minimize performance impact, system administrators have made compromises which affect the data base's internal controls. First, system administrators told us that turning on the internal audit trail, which I will discuss later, would seriously slow down system performance; and that to turn on the audit trail would take several staff weeks of programming effort to minimize the impact on overall system performance. Second, system administrators have chosen not to use the referential integrity capability⁵ that Sybase offers because of performance issues. Referential integrity is critical to any data base to assure that necessary checks are in place to limit inappropriate data input and assure that output is accurate. For the White House Data Base, referential integrity is implemented through the application itself. Because of the complexity of the application structure, it is difficult to assure that all edit checks are in place and work properly across the application. We found that some checks are not operational which in turn leads to a higher probability of inaccurate information being input or retrieved from the system.

Operating Processes and Procedures

Good business systems operate in a controlled environment to ensure that data within these systems is accurate, that data output is reliable, and that data integrity is assured so that only authorized users have access to the data and that such access is appropriate to their needs. To provide such assurance, an organization needs well-articulated policies and procedures, good training, and an ability to ensure compliance with established processes and procedures.

⁵Referential integrity is the constraint or rule that must remain true for a data base to preserve integrity. For example, that at most only two biological parents can exist for a child.

For the government, these concepts are embodied in the Office of Management and Budget's Circular A-130 which lays out the need for policies, rules of behavior governing system use, training, and the need to incorporate good controls. Circular A-130 states that accountability is normally accomplished by identifying and authenticating users and subsequently tracing actions on the system to the user who initiated them. As a system containing sensitive information on up to 200,000 individuals, and, as a system that is important to meet the work needs of several White House offices, data base users and managers need to apply the principles of A-130 to system operations.

We found that the White House has taken several positive steps to create a controlled environment. For example:

- Personalized training is available to all users.
- Users are required to sign a document stating that they will take measures to protect information including establishing and protecting passwords, logging out when leaving their computers, and reporting unauthorized access to the system.
- Password access is required to enter the system and a warning screen appears to inform the user that information within the data base is for official use only.
- The data base has an effective defense against outside intruders or "hackers" breaking into the system.
- Controls have been established within the system to limit access to certain portions of the data base to only those with a need to know. Additionally, only a limited number of users have authority to print reports.

Even with these processes in place, we found that the data base requires additional measures before data integrity and operational effectiveness can be assured. For example:

- Users do not have well-documented processes and procedures for how and when to use the data base. Written documentation, reinforced with training and operational processes, would provide a better basis for assuring system managers that the data base was being used effectively and that all users were appropriately keeping the data base current. While users were trained individually by system administrators or other users, only one user out of the nine business users that we interviewed reported having a users manual. None of these users reported having training concerning the security of the system. Such guidance can help ensure that users are familiar with the system and are entering information correctly. In talking with users we found that most everyone could navigate the system adequately; however, we also found that some duplicate information on individuals was being entered into the system and that some information was being entered into the wrong field. This causes

some data base tables to contain more information than necessary and slows down the processing of information.

- Although the data base has established security policies, procedures necessary to make them effective have not been well-documented. For example, the system does not require frequent changes in passwords. Only one of the applications users we interviewed has changed their password since the system was initiated.
- Although controls exist to limit printing of reports, any user having general network printing⁶ capability can print the screen contents. Additionally, all users have the ability to download screen content onto an electronic notebook⁷ which could then be mailed electronically to a third party. None of the users we interviewed stated that they were aware of this capability. Additionally, White House officials told us that every month they review a sample of outgoing e-mail traffic to identify inappropriate use of the electronic mail system and to comply with records management requirements.
- Most importantly, there is no audit trail. Although Sybase 10 has this capability, we were told it has not been turned on because it would inhibit system performance. The Sybase audit capability would allow system administrators to monitor and react to attempts to log on and log off the system; execution of update, delete, and insert operations; restarts of the system; execution of system administration commands; and changes to system tables. Without this feature, data base administrators are limited in their ability to ensure that users are properly accessing and using the system.

-- -- -- -- --

Mr. Chairman and Members of the Subcommittee this completes my testimony. I will be happy to answer any questions you may have.

(511098)

⁶Having the capability or authority to output data over the network to a printer.

⁷A simple word processing program that allows users to copy information from one program onto the notebook.

Mr. MCINTOSH. Thank you very much, Mr. Brock.

Thank you, and Mr. Hess and Mr. Rhodes, for your diligent work in finding out about this Data Base.

Let me first ask you a question to clarify the scope of your review. And I wanted to ask you, has GAO undertaken any analysis or effort to determine whether any laws were broken by the White House creating or maintaining this White House Data Base?

Mr. BROCK. Well, the—as we indicated, the limit and the scope of our review was technical. So, for example, if we had been reviewing the procurement or something like that, we might have been able to observe whether the procurement was done in a legal manner or not. We did not look at the data. I do not know if the data falls into some sort of a legal categorization or not. So we didn't find any examples in the way they built and constructed and maintained the Data Base that anything was illegal. But as I indicated in my statement, we think that a lot of the things that they did could have been done better, to assure the right kind of control environment.

Mr. MCINTOSH. OK. So you did not perform a legal audit on the uses of the Data Base?

Mr. BROCK. No, sir, we did not.

Mr. MCINTOSH. OK.

Let's turn to this audit trail issue. You state at the end of your written statement that there is no audit trail, and that this is the most important problem that you have identified. Can you give the subcommittee a brief, 30-second explanation of what an audit trail would do and why it's so important to ensure accountability and integrity of a government computer system?

Mr. BROCK. If I could do that in sort of two parts, give a very, very brief overview and ask Mr. Rhodes to provide a more technical overview.

In general, if you don't have an audit trail, you can't tell what's going on in the course of business. You have to completely rely on users. And while everyone likes to trust users that use the system, in effect this is not a proper control. And without controls, you can't provide certainty that the information is used in a reasonable and responsible manner, and this is true for all systems that contain sensitive information.

And Keith, I think, can describe in a little more detail, if you would like, about what some of that might involve.

Mr. MCINTOSH. That would be great.

Mr. RHODES. The things that you can cover in an audit trail would be, for example, log-in, when somebody logged into the Data Base, when somebody logged out. It would give you a specific time. You can configure it down to the field level, where the columns and rows and the tables actually intersect and say when was the last time that that particular bit of data was changed.

You can audit remote procedure calls, that is, calls that were made from one system to another system or from one part of an application to another part of an application, if you want.

You can audit the time that a stored procedure is executed, when some part of the Data Base application is actually executed. You can get a time when it was started, a time when it was ended and

who actually executed it. That's what you are building. It's following the user's actions through the Data Base.

Mr. MCINTOSH. So in the normal routine Data Base, if you wanted to ensure that someone wasn't misusing sensitive information, you would engage an audit trail to periodically check and see that only people who are authorized to have access to certain information looked at it or used it or changed it in some way?

Mr. RHODES. Yes. If you turn it on, it constantly works. It's not turning it on, and then it's only on for a little bit, and then it's off for a little bit. If it's on, it's on.

Mr. MCINTOSH. Certainly in the context after the June 27th public revelation of this where we were concerned people might go in and change or erase data, you would want to have the audit trail there to ensure that none of that activity could possibly have occurred?

Mr. RHODES. That would be one of the controls that you would have to make certain that data had not been changed.

Mr. MCINTOSH. When you first asked the White House if they kept an audit trail for the White House Data Base, what was the answer? What were you told by the White House staff?

Mr. BROCK. At the time we had that interview, we asked if there was an audit trail, and they said that the audit trail had not been turned on.

Mr. MCINTOSH. And I will reference my first letter to Mr. Quinn on, I think, it's August 12, that indicates we passed that on to him and said we were very disturbed by that.

Now, at the same time, as you were being told this, Mr. Quinn wrote back to me that it was never installed. Is this statement accurate?

Mr. BROCK. The—an audit capability is installed when you install Sybase. At a subsequent interview that we had with the White House technical staff, I believe on Friday, we were told, again, that it had not been turned on. Then in a meeting we had with them yesterday, they said that two key components of the audit capability had not been installed.

Is that correct?

Mr. RHODES. Yes.

Mr. MCINTOSH. Only yesterday that information came to you from the technical people?

Mr. BROCK. Yes.

Mr. MCINTOSH. Have you had access to the actual Data Base to confirm that?

Mr. BROCK. We have not yet had an opportunity to examine that.

Mr. MCINTOSH. It strikes me as odd that just moments before the hearing, that that would become true.

If there were some key components not installed, how much time would it take to install those, and would it be necessary to turn the rest of the audit function on?

Mr. BROCK. I am going to let, again, Mr. Rhodes answer that. It's clear that turning on a full, complete audit of the system would take a fair amount of time, because of the vast number of tables. We don't think doing a more limited review or a limited audit of key components would be that time consuming. But I think Keith can give you a more precise answer.

Mr. RHODES. Based on the conversations that we had yesterday, the White House technical staff said it would take approximately 4 to 6 hours to install the additional files that were necessary.

Again, as Mr. Brock explained, if I want to do an entire audit of everything that is occurring on the Data Base, because of the structure of the Data Base and because they are trying to navigate all the linkages in the Data Base, that would be time-consuming. If they wanted to turn on, for example, audit log-in and just monitor the log-ins to the system, or just to monitor when a stored procedure were executed or something like that, that would be smaller.

One of the time constraints that they had in the discussion yesterday was figuring out exactly what they did want to audit.

Mr. MCINTOSH. So let me ask you this: Is it accurate to say that given sensitive personal and political data on that Data Base, is it impossible for the Data Base to function with the audit function installed because the system would be too slow?

Mr. RHODES. The White House has never stated that it would be impossible. They have stated how much time it would take to turn it on. Part of that has been to figure out what would need to be audited and what performance tuning to the system would be necessary in order to keep the system running.

They have said if we—the statement has been if we turned everything on, it would just crash, but it's not that it couldn't be turned on and that it couldn't be configured to run.

Mr. MCINTOSH. So this isn't an unacceptable tradeoff in the performance of this system? It's a concern of installing it and bringing it up to operation after it's installed?

Mr. RHODES. Right, with finding out what they actually do want to audit and not having too severe a degradation.

Mr. MCINTOSH. The answer seems to vary widely from 6 hours to 3 to 5 weeks in the letter.

My time has expired. I will come back with some few additional questions.

Mr. Peterson.

Mr. PETERSON. Thank you.

As I understand it, the problem is I have been told that if they turned on the complete audit function on the whole system, it would degrade the performance by a factor of four. In other words, it would be four times as slow as it is now.

Mr. RHODES. We weren't given an exact degradation of performance. We were told that it would crash.

Mr. PETERSON. That's what I was told, and people are already complaining that it's too slow. And I think you are right, that they overbuilt the system, which they usually do with these kind of things, especially when you give them this much money to spend programming.

So, Mr. Chairman, I think part of the problem is that—why this wasn't turned on, is that to turn it on for the entire system, first of all, probably is not necessary, and it would degrade it more than would be acceptable.

So then what you have to do, the reason you are getting these wide disparities in times, is you have to go in and figure out what part of it you want to actually have an audit trail, as they were

saying, whether it's going to be the log-ons, whatever. That takes time to figure—first of all, figure out what you are going to audit. Then you have to write special programming to make sure that this works properly or it will crash. If you try to turn this, and you don't have this thing configured right, your program probably will crash. So there's more to it than just turning on a switch if you are going to try to limit this, and I think that's part of the problem the White House has been struggling with.

I guess my question, do Members of Congress have an audit trail in their Data Base systems? I don't think they do. Did the Bush administration have this audit trail turned on in their system? I'm not sure if they did, and we don't know, I guess.

And in my looking at the system, I mean, part of the way that they were controlling this was they have very limited access in terms of who can get into what parts of the system. And the areas that you are focusing on that are sensitive, there is very limited access to those parts of the system. As I understood it, there were only four or five people that could get that far into the system.

So I think rather than control it after the fact, there was a decision made to control it at the front end by who could get in using passwords and so forth. That was a decision that was made, I think, in the White House. And I, frankly, probably would make the same decision.

Now, you know, I mean, if we are going to require that everybody in government have an audit trail that we can figure out who logs in and out of all of their computers, I think we are going to bring the whole government to a standstill. And I don't know why we ought to require the White House to do something that nobody else is doing. So, you know, I think we need to keep this—again, keep this whole thing in perspective.

And I have a question, you know. Do you know, is the Clinton administration doing anything different than the Bush administration did in terms of the way this Data Base is established?

Mr. BROCK. We don't really know. We are aware of some of the legacy Data Base that were present that were abandoned, but we didn't look at the structure of the Data Bases or the administration of the Data Bases. I don't believe there were people around, I am not sure, within the range of people that we interviewed that would have any knowledge of that.

Mr. PETERSON. There were two people we talked to with 20 some years experience through all of these situations. And I have a question of whether there is any difference here, and I guess I was wondering would the chairman join me in requesting that the Bush archives, if we can get access to copies of their Data Base to see if there is—so we can have some kind of meaningful comparison if what is it going on here is any different than under Bush.

Mr. MCINTOSH. I will certainly take that into consideration and work with you on that.

Mr. PETERSON. I think this whole—I don't know if you have got this information on this audit trail, Mr. Chairman, but I have got some information on how long it would take to put in the various components and so forth, and frankly, if I were making this decision, I don't think I would decide to do this because I think it would degrade the system to the point where you are going to have

more trouble with users than you want to have, because they designed the system wrong in the first place. They put all of this stuff on it, then they are not using it, right?

Mr. BROCK. Yes, sir.

Mr. PETERSON. As I said in my opening statement, I think the biggest criticism I would have of this is they built this big overblown system, and they are basically using it as a Rolodex, right?

Mr. BROCK. Yes.

Mr. PETERSON. Even though there is information in these fields, I am not sure they are set up in any kind of way they could really use them because they haven't really got relational capabilities programmed. It wasn't put in that way, it looks like to me, but—

Mr. BROCK. They have a difficulty running relational searches. It takes a long time.

Mr. PETERSON. Right. From what I could tell, I don't know they are doing that. That information may be in there, but it didn't sound like that was one of the uses they were making of the system, from what I could tell when I asked them questions.

It has been a couple of months, but did you find out how many searches they made, or did you look into that kind of information?

Mr. BROCK. We started doing inquiries yesterday, and we did run some relational searches, and they can be done. They are slower than the other searches, and I think some of them would appear relevant to the normal course of business, things you want to do. Certainly the Data Base was originally intended to run that way.

Mr. PETERSON. Can you tell whether they did searches or not? Is there any kind of record of that?

Mr. BROCK. The only thing we can tell is based on anecdotal information. Because of a lack of an audit trail, we have difficulty going in telling what has been done or not done.

Mr. PETERSON. No kind of handwritten record of information they pulled out? If they ran some kind of a search, it would seem to me they were trying to come up with a list maybe to send an invitation to some kind of event or something.

Mr. BROCK. We talked to users about the outputs of some of their searches such as when they are building an event or sending out cards or things like that, but we actually haven't seen any logs or details of what they were checking for when they were putting together the searches.

Mr. PETERSON. Well, my time has gone now, Mr. Chairman, so—

Mr. MCINTOSH. Thank you, Mr. Peterson.

Let me say certainly since June 27, I would have thought the White House would have wanted an audit trail to demonstrate to everybody they weren't going in and changing the Data Base regardless of merits prior to that, which seem to me to be pretty clear as well.

Let me now turn to Mr. Ehrlich, who has joined us as vice chairman of the subcommittee.

Mr. EHRLICH. Thank, Mr. Chairman.

I am a little confused, and our friend here has a good question. Let me get something straight in my own mind.

Mr. Rhodes, you just told us relational searches were performed yesterday. You have anecdotal evidence concerning the use of the

system. You have no particular details, yet in answer to a question concerning an analogy to a Rolodex, you said yes, it was used as a Rolodex. Isn't it true you really don't know at this point—you don't have the information to know exactly what it was used for?

Mr. BROCK. During the course of interviews with the users, we asked each of the users what they did it for. In fact, several of them brought up the word "Rolodex" themselves. They use it to either supplement a Rolodex, if they already had employees, for names and addresses, or in some cases they used a Rolodex to supplement it, and they gave us a fairly detailed description of how they used it in terms of putting together the events lists. Did we see any of those lists? Yes, we have seen samples of what they do with the output.

Mr. EHRLICH. Are you satisfied that your search is complete?

Mr. BROCK. We are not satisfied that the search is complete. But we are satisfied, in that we did review the content structure and code that made up each of the 125 tables, so I think we have a very good understanding of the structure and what you can and cannot do with the Data Base.

Mr. EHRLICH. So the potential use you certainly have an idea?

Mr. BROCK. Yes.

Mr. EHRLICH. But the actual use you still need to fill in information?

Mr. BROCK. That is correct.

Mr. EHRLICH. Thank you, sir.

It is the joke in my office I want to get into the 1890's, not the 1990's, in the computer, so please I apologize for my rather elementary education here when it comes to computers.

Aren't audit trails usually designed for systems such as this?

Mr. BROCK. Yes. Sybase has an audit trail that is built into it, and whether they use that audit trail or some other audit trail, when you are putting together a system that is protecting sensitive information, the trade offs you look at when you are establishing the system design is your audit capability. I think the problem the White House has now is when you try to put in an audit capability after the fact, it proves to be very difficult with the compromises that have already been made in the system design.

Mr. EHRLICH. Let me stop you there. In answer to a question the chairman asked you, I believe you related to us the White House told you yesterday that two key functions had not been installed. Is that related to your last answer, that we are trying to reinvent the wheel here, at least the White House is? First of all, is this new information the fact those new functions had not been installed?

Mr. BROCK. Yes.

Mr. EHRLICH. How does that dovetail into the previous answer?

Mr. BROCK. I think the White House, since the audit came and the letters that originally came over from the subcommittee, is now examining can we install the audit trail; what would it take to do; and how would it affect performance?

Mr. EHRLICH. OK. Obviously we have a bunch of information here, and I have been given information. The White House said it hired five outside contractors and paid \$545,000 to develop the White House Data Base. Did the taxpayers get their bang for the buck?

Mr. BROCK. I am going to put a caveat on my answer. We have not examined the cost of the Data Base. I don't know if it cost \$540,000 or not. If, in fact, they spent \$540,000 on the development and implementation of the Data Base, I don't think the bang for the buck is there.

Mr. EHRLICH. Would it be fair to say the element of accountability is an important factor in sensitive systems, such as a White House Data Base?

Mr. BROCK. I think it is critical. I don't know if you were present when I was reading a quote from A-130, OMB Circular A-130, which stresses that is a critical element of any sort of information system.

Mr. EHRLICH. Thanks a lot. I appreciate it.

Mr. MCINTOSH. Thank you, Mr. Ehrlich.

Mr. Hastert has joined us.

If you do not have any questions at this time, we will return to you in the next round.

Let me continue, Mr. Brock, with some questions I have. Perhaps one of the most important questions that is coming up and which we have sought to get an answer is, where did the information come from? There is a category in the Data Base marked "sources" that contained some of the most politically relevant terms, 1992 supporters, top 20 DNC lists, and so forth, along with some other surprising ones when we asked them to flip through it for us, such as the ACLU and other references to organizations like that.

We understand that some of the data has been manually entered, and some of it has been electronically uploaded. Your statement indicates you don't have enough information to answer this question effectively yet for the subcommittee. Has the White House responded to your questions about the sources of the data in a timely manner?

Mr. BROCK. We are, I think, in the process of trying to work with the White House to determine how to get to the source of the information. This has been very tricky. Just for a very brief background, information that is currently being entered is being done for the most part manually. However, the original population of Data Base came from a variety of sources, and apparently—I am going to ask Ron to describe the different kinds of sources and how it gets in, but we have just, I think, begun discussing with the White House yesterday about how we might get a response to that question.

Mr. HESS. We had asked specifically what is the source field used for? What is source? And the answer that we received yesterday is that source could reflect a number of things. Source relates to the information that is present on the basic information screen that I'm sure you have seen when you all had your demo, which includes the person's name, their telephone number and other basic descriptive information. Source reflects where that information came from, and that could be from a list that the White House received from some other organization. It could be—the source could be the person that typed the information into the system. The source could be the legacy Data Base that the information was uploaded from. Source could be the office in the White House that the person who entered the information works in, or source could be a telephone

contact that they had with an individual to get information on them.

So that is really the extent of what we know source is at this time. We have requested—

Mr. MCINTOSH. So the entry "1992 Early Supporter," "Top 20," which one of those categories would that fit into?

Mr. HESS. I cannot answer that at this time. We have requested from the White House a list of all of dropdown items that you could pick from as you are entering information and a definition of those items.

Mr. MCINTOSH. They provided you with that list?

Mr. HESS. They have not provided that at this time. We are supposed to receive that at the end of the week.

Mr. MCINTOSH. Let me ask this, because it is an important time question. Mr. Brock, we met in July. I asked how long you thought such an audit would take. You said, a week, maybe two, if we get full and complete access. It is now 6 weeks later. Have you all not been asking the questions, or have they not been providing the answers?

Mr. BROCK. We have been asking questions, and they have been providing answers, but there is frequently a delay between when we ask questions and when they get answered.

Mr. MCINTOSH. You stand by your original estimate?

Mr. BROCK. No, it has been over 2 weeks. I think if we had complete access to the technical staff at the White House, who, I want to add, have been very cooperative with us when we met with them, we could have completed the audit in a very short period of time.

Mr. MCINTOSH. Since it has taken a lot longer, am I correct to infer you have not had complete access in order to get your questions answered?

Mr. BROCK. I think eventually we get access, but typically we go through a multistep process where first we meet with a representative from the Counsel's Office, then a discussion with the counsel present and technical staff to discuss the parameters of the question. Then we meet with the technical staff; sometimes with a representative of counsel's present, sometimes not. And there is typically a delay between these—each of those steps, so some of the information we have requested August 2—

Mr. HESS. August 6.

Mr. BROCK.—August 6—we are just now getting and hope to get the rest of the information by the end of the week.

Mr. MCINTOSH. How often do they make you go through those different hoops? How often do they let you actually meet with the technical staff?

Mr. BROCK. We have had several meetings with the technical staff. In fact, when we first started the audit, after some initial delay of getting in, we had a series of meetings with the technical staff where we very quickly were able to develop an overview of the system. When we started getting into more detailed information about the queries and some of the structure, then those meetings were delayed. Sometimes we were provided with a reason, they were doing—fulfilling some other requests they had, and sometimes we just didn't get a response to our telephone calls.

Mr. MCINTOSH. Frankly, this is unbelievable to me and a classic stonewall technique. You said you asked for, but have not received, a printout of the sources and a description of what those different items mean. How about on the political participation menu? Have you asked for a list there?

Mr. BROCK. Mr. Hess is looking it up.

Mr. HESS. Yes, just 1 second.

We have asked for a list of all the dropdown menu items that are available on the search screen that you would have seen in your demo here. There are 25 dropdown items you can pick from as you are filling those fields. We have asked for a list of those as well as all of their definitions.

Mr. MCINTOSH. When did you ask for that?

Mr. HESS. I believe we asked for that August 6, and on August—we met with the White House on August 20, and they asked us if there were certain ones we were interested in, and we said that there were. We requested descriptions of those items for the following fields: source, political participation and family relationship. The White House agreed to expedite those items, which they did not, and we are expecting to receive them by the end of this week.

Mr. MCINTOSH. Are these particularly difficult lists to produce?

Mr. HESS. I do not believe they would be difficult, but, of course, I am not a systems administrator over there, so there may be some particular exigency that I am not aware of.

Mr. BROCK. I don't think it would be difficult, but because of the vast number of tables, it certainly could be time-consuming. I think we were originally promised the list by the end of the month?

Mr. MCINTOSH. Wait a second, Jack. When I was down there at White House, they scrolled through that on the screen for me. How difficult would it be to print out a list of somewhere between 20 and 100 items?

Mr. BROCK. For that one screen you are on, it probably wouldn't be difficult. When you go through it all, it would probably be cumulative.

Mr. MCINTOSH. Each would have a different job dropdown list?

Mr. RHODES. No. There is a distinction here I think you are trying to make. To get the dropdown menu, that source code exists. They should be able to print that source code out and give it to us.

I think the thing that would take time is getting the definition of those individual items, trying to have a definition of each one of those items, because as Mr. Hess pointed out, some of those are ad hoc inputs from users themselves. Therefore, that would require the time for the definition. But the source code and the actual dump of what a pick list, of what a dropdown menu—

Mr. MCINTOSH. What is that referring to? OK, I understand. When it says "AFL-CIO," you would understand what that meant?

Mr. RHODES. Exactly. That is the key.

Mr. MCINTOSH. But printing the list would be easy?

Mr. PETERSON. Mr. Chairman, if I could.

Part of the problem is they have got to take the system down to do this. They can't do it during the day. Part of the trouble with this is they have to do this in the evening.

Mr. MCINTOSH. Let me reclaim my time quickly. Printing a list of a couple hundred items can't take that long overnight; am I wrong there?

Mr. RHODES. If they are taking it directly out of Omnis and if they are printing it directly out of Omnis, if they are taking the source code, they can print out the source code. If they are trying to print out from Omnis the actual dropdown menu directly from the Data Base, then that could be time-consuming.

Mr. MCINTOSH. Approximately how long?

Mr. RHODES. I have no idea because we haven't done any performance measures on the system.

Mr. MCINTOSH. If you were down there and could use the computer personally, how long would it take you to print it out?

Mr. RHODES. I would click on and do a screen print.

Mr. MCINTOSH. A few minutes?

Mr. RHODES. They say it takes 30 minutes to print a screen, so it would be 30 minutes per pick list.

Mr. MCINTOSH. I am coming back with some additional questions. With unanimous consent let me turn back now to Representative Hastert.

Mr. HASTERT. I thank the chairman.

Let me ask, in going over the briefings and some of the paperwork we had today, and I am sorry I wasn't here right when you started, given the fact that the White House Data Base system is so poorly designed that it would require some modification—except for an audit trail—do you believe the American taxpayers really got what they paid for? The White House admits they hired five outside contractors to the tune of almost 5 and a half—or \$550,000 to develop the White House Data Base. Is this the type of system that you would expect to get for this amount of money?

Mr. BROCK. No. I would expect any system—and these are criteria we would apply to any system we are looking at when we look at systems across the government—that any systems that are designed to have appropriate security and internal controls built into it from the start. If, in fact, these systems and controls—or controls were not built into the system, we would find consistently that the system is inadequate. So in this case the system is inadequate, and as a result I would give it a grade of "I," incomplete. They still have more work to do to make it an acceptable system.

Mr. HASTERT. But the money has been paid, right?

Mr. BROCK. We haven't gone into all the moneys I am not sure all of the money has been paid or not.

Mr. HASTERT. It has been paid, I understand. We paid the money and haven't gotten the results yet. That is one of the problems that we see here in Washington from time to time.

In your testimony, you outline several steps the White House has taken to begin to protect the integrity of the Data Base and the White House system. Now, I would like to run through the items in your list. No. 1, you state that the personalizing—personalized training is available to all users. First, does it actually prevent users from misusing the data?

Mr. BROCK. No, but I think the training has gone well, and I think many of the users have complimented the people on training. It can be an effective mechanism for at least providing some level

of instructions about how to use it and when to use it and whether it is appropriate, because the training is not really documented in terms of the training manuals and things like that. We really can't be certain as to the content of the training.

Mr. HASTERT. So you say it doesn't prevent the users from misusing the data?

Mr. BROCK. No. I think the best you can hope for for training is to use the system properly and alert you to the misuse of data. That is when the audit trail comes in. You have some sort of mechanism that can verify or check to see if users are misusing data.

Mr. HASTERT. We will get to audit trails in just a second. At best then, even if the user were trained, there is no preventive key or trigger to stop them from misusing the data.

Then let's go to the next question. Has every user received personalized training?

Mr. BROCK. I believe that in the users we interviewed, they all received personalized training. We interviewed the top users.

Mr. HASTERT. There are other users?

Mr. BROCK. Well, there are around 150 people authorized to use. One hundred have used it. Twenty-five big users—we didn't interview all the users, but the large-scale users do have training.

Mr. HASTERT. Can you say unequivocally that every one of those people, 150 users, have personalized training?

Mr. BROCK. No, I can't say that.

Mr. HASTERT. So we don't know?

Mr. BROCK. That is correct.

Mr. HASTERT. You state that the users might sign a document before they can use the system as sort of a statement of personal responsibility to kind of—this audit trail thing that we are talking about. Let me ask you if you know if all users of the system, and there are 150 users of the system, have they signed this statement?

Mr. BROCK. We did not do a one-to-one verification for each of the 150 users. We did go rifle through their file drawer. We saw large stacks of signed documents. We pulled out some for the users that we interviewed.

Mr. HASTERT. So what is the answer?

Mr. BROCK. I think that except in one case.

Mr. HESS. Of the users that we interviewed and we saw their documentation, one of the users had not signed their form, and there was another one that was questionable that their form wasn't in their folder, and they were looking for it some other place.

Mr. HASTERT. You have only interviewed one-sixth of the users, the top 25; right?

Mr. HESS. We interviewed the top five business users plus some system administrators that also account for heavy use. So I would say we interviewed a good tenth of the users. But they do—

Mr. HASTERT. A tenth of the users?

Mr. HESS. But they do represent the most heavy users of the system.

Mr. HASTERT. But even those people that use it don't sign?

Mr. HESS. Not everyone one had signed.

Mr. HASTERT. So we don't have an audit trail.

One of the issues the statement addresses is that people need to log out when they leave their computers. Do users always do this as the statements require?

Mr. BROCK. For the most part, when we interviewed the users, most did not log out, or many did not log out. I don't want to say most. There did not seem to be screen savers in place that would automatically blink the screen after a designated period of time.

Mr. HASTERT. I have barely used that system—not that system, but any system—but I understand when you get your password, a password is pretty sacred. Also, users were instructed they had to protect their password, otherwise you could hand it off to somebody else without logging on or off. I would assume part of this would include regularly changing the password; is that right?

Mr. BROCK. That is correct. That is an established procedure for password protection is regularly changing the password.

Mr. HASTERT. Do all the users regularly change their passwords?

Mr. BROCK. Of the users we interviewed, only one had changed their password since being on the system.

Mr. HASTERT. I see my time has expired. Thank you very much.

Mr. MCINTOSH. Mr. Peterson.

Mr. PETERSON. Mr. Chairman, just kind of in followup on Mr. Hastert's question, I think it needs to be pointed out, and I am pretty sure I am right on this, that there is no audit trail on any of our Data Base systems, and there is no guarantee that Members of Congress and their staffs are not using their system inappropriately either.

One of the things I am going to do is I am going to send a letter to GAO asking them to make a similar kind of investigation into the Bush administration Data Base, and including how much money they spent on it, No. 1.

No. 2, I think we ought to investigate Members' of Congress use of their Data Bases to see if we are using audit trails, to see if the same kind of controls are being used so we can make sure that Members of Congress are not inappropriately using their Data Bases, because I don't think anybody has really taken a hard look at that.

Mr. HASTERT. Would the gentlemen yield on a point of agreement?

Mr. PETERSON. Sure.

Mr. HASTERT. What you are saying is no user in a governmental sense—I use a Data Base to keep records in the same Data Base if somebody is giving contributions or doesn't give contributions. That would clearly in our ethics system in Congress would be wrong. We are not supposed to do it now. Now, the check you want to do is see if it's being done or not.

Mr. PETERSON. Right. My point is I don't think there is any audit trail turned on in anybody's Data Base systems. To make this criticism of the White House, we have to look at our own situation.

Mr. HASTERT. But if, in fact, it is being done in the White House, it is not right.

Mr. PETERSON. Well, no, I didn't say that it is right.

Mr. HASTERT. Thank you. I will yield back.

Mr. PETERSON. No. 2, if you look at the breakdown of how this—a good part of the cost of this is licensing for the software and for

the run time so that can you go in and do the programming. I don't know if you have got this breakdown, but there is \$120,000 for a six-gigabyte Data Base, \$75,000 license for server, then there is \$75 for a license so you get a free run time module so you can program it. Then the rest of the cost is these two programmers. The Bush administration's Data Base, they spent \$249,000. I am not sure what they got out of that. Similar kinds of—

Mr. MCINTOSH. Could we have that cost information for the record? And let me ask a point of clarification. Were both of these documents provided from the White House? Do you know?

Mr. PETERSON. This was information my staff has pulled together at my request stemming back from the time that I was originally down there, questions that I asked.

Mr. MCINTOSH. I appreciate the information. I just wanted to make sure we knew where it comes from.

Mr. PETERSON. I didn't make it up.

Mr. MCINTOSH. I understand, but it presumably came from the White House Data Base.

Mr. PETERSON. Right. They are the only ones that know what is going on, I think. They put it together.

Also I wanted to know when this issue of the source list, when did you actually ask for the—you said yesterday you were down there. When did you actually ask for a list of the source?

Mr. HESS. We asked for a printout of the table that contains the source information. We asked for that on August 6.

Mr. PETERSON. And what was the response?

Mr. HESS. The response on August 6 was we would meet again and discuss the difficulty of all the items that we requested, and at some later point, and I honestly don't remember when, it was sometime around the middle of August, he said they would make that available to us at the end of the month.

Mr. PETERSON. Mr. Chairman, when I was down there, I had a similar kind of discussion with them, and their concern was they were being deluged with requests for all of this information. You couldn't go in, and you basically can't go in when the system is up and get that kind of information. You have to take the system down, which means they are using it from 8 a.m. until 6 or 7 p.m. Sometimes they were using it longer than that. Basically what you were having to do is shut the system down early, bring them in, pay them overtime, run all of these lists. It is not as easy as you think.

I got the same kind of answer: We are happy to give you this stuff, but we can't—we have got to continue to run the White House. We can't—this system is something we are relying on now.

So I don't know that I would agree with your characterization there was a stonewalling going on here. I think there is more to this than meets the eye. Maybe they could have provided it faster, but frankly, Mr. Chairman, during all of this—when was the first inquiry, like in July?

Mr. MCINTOSH. June 27.

Mr. PETERSON. I don't think you went down to the White House to look at that yourself until last week.

Mr. MCINTOSH. Even then we were totally unsatisfied with the lack of response on the technical information.

Mr. PETERSON. With all due respect, I think had you and your staff gotten down there earlier, maybe many of these problems wouldn't have happened as well. I don't know if you can blame the White House for all of this. I don't know who's right and who's wrong, but I got this information after I had been down there and asked the questions.

Mr. MCINTOSH. If the gentleman would yield for a second, this is just another indication—and I appreciate your making these possible and part of the record. My staff tells me we have not received this information from them even yet, and I am glad you are able to get that.

Mr. PETERSON. Did you ask for it?

Mr. MCINTOSH. Oh, yes, we have very thorough details. I am curious, was it provided to the GAO folks, the cost breakdowns and the different numbers?

Mr. BROCK. No, but we have a whole series of audit steps we are following, and we have not gotten to that part yet.

Mr. PETERSON. You hadn't asked for it, right?

Mr. BROCK. No.

Mr. PETERSON. I am not sure if anybody asked for it until I did.

Mr. BROCK. I am quite sure we have because it was in our request repeatedly.

Mr. PETERSON. I just think if we are going to subject one White House to all of this, I think we ought to be fair and make sure everybody is being treated alike, so I am going to send some further inquires.

Mr. MCINTOSH. Let me share with you, I do remember serving in the Reagan White House when they were able to use the National Security System's computer Data Base at the same time they did the investigation of all the e-mails Ollie North sent back and forth. So I do think it is possible to function in the White House and to come forward to the American people and tell the truth.

Mr. PETERSON. Well, Mr. Chairman, I think that stuff is on the mainframe, which is a whole different environment than what—this is on a PC-based system, and it is a different situation.

Mr. MCINTOSH. Let me turn now to Mr. Ehrlich.

Mr. EHRLICH. I have two very brief questions, then a quick statement. One, with respect to the interns, can you give me the names; could you supply us with the names of all the interns that had access to the White House Data Base?

Mr. BROCK. Not at this point.

Mr. EHRLICH. Is that because that information is not available?

Mr. BROCK. We never asked for the names of intern accounts. Do we have that on the user list? I believe on the user list they are identified as intern A, B.

Mr. HESS. They are not referred to as "intern," but there are several accounts on the system that are not attributable to a specific name. If I had an account, it would be Hess, R. But there are accounts that are set up for an office in the White House; for example, WHO, SOC, S-O-C is for the Social Office.

Mr. EHRLICH. Anybody from the Social Office could—

Mr. HESS. If he were given access and a password to that account.

Mr. EHRLICH. Great.

Second, this executive White House management information system. I just have a question, and I will read the first sentence concerning the executive summary: "The President and the First Lady requested from Marsha Scott that a resource Data Base containing relevant information concerning all White House events and contacts be designed and implemented."

To your knowledge is that a correct statement?

Mr. BROCK. That is a virtual quote of the documentation we have when we went back to look for the original requirements for the system.

Mr. EHRLICH. I just have a statement, Mr. Chairman. I think Mr. Peterson's request is absolutely relevant and fair. I am very interested, and I think we all are, in seeing what past administrations have done with respect to this entire issue. I want to know what the Bush administration did, and the Reagan administration did, and this administration did. I think as part of our oversight function it is a very legitimate inquiry, and I am interested in seeing if the law needs to be changed.

Obviously, as has been stated here, if we, as Members of Congress, had contribution information on our Data Bases, we would be violating our code of ethics and probably Federal laws. I see a very legitimate function for the White House Social Office to have some information concerning folks they want to have to the White House. I see clear cases where that is appropriate and clear cases where it would be inappropriate with respect to some information, purely political information, that is compiled with the Democratic National Committee and the Republican National Committee and should not be paid for by the taxpayers; what information is relevant and what information is not relevant, what information should be paid for by the taxpayers and what should not be paid for by the taxpayers.

I compliment you, Mr. Chairman, for having this hearing. I want to know and I need to know in order to formulate my own mind and opinion concerning if the law needs to be changed. Thank you.

Mr. MCINTOSH. Thank you, Mr. Ehrlich.

Let me add we will get to the panel of legal experts to see whether the law permits it currently or not.

Mr. Hastert.

Mr. HASTERT. Thank you, Mr. Chairman. I guess I can go on my second round here.

If somebody didn't log out and just left their computer open—now, I have to say I am not the best guy in computer literacy around here, but I watch my staff, and I make sure that they follow a pretty strong set of user requirements. If they don't log out, that means that anybody can sit down at their computer and hack away; is that not correct?

Mr. BROCK. That is correct.

Mr. HASTERT. If there is a habit here of White House staff that have access to this, some 150 people, the 25 users you talk about here, that anybody, if these things are open, can come along—that if anybody had access to the White House Office can go in there and hack away; right? For instance, if I was invited for a state dinner, which I have been a couple of times, I would assume then that there would probably be information under my name and whether

I gave to political donations or didn't give political donations or not; is that correct?

Mr. BROCK. I am not sure. Under your name there would certainly be your name, address, phone number, and Social Security number, and could be other biographical data as well.

Mr. HASTERT. It is really an open book if somebody chose to pursue this; is that right?

Mr. BROCK. That is right.

Mr. HASTERT. Let's say a guy like Craig Livingstone, who isn't one of the users and probably not on the system to use it, I don't know, but he was in charge of security in the White House, and he could get around it, and if one of these things weren't logged out, he would have access to anybody who was on this list, thousands of people; is that correct?

Mr. BROCK. If you do not log out and leave your work station, there is an opportunity for misuse, that is for sure.

Mr. HASTERT. You said this practice is quite prevalent of people not logging out?

Mr. BROCK. Of the people that we interviewed, and I want to state we did not interview everyone, just the heaviest users. That was the prevalent practice.

Mr. HASTERT. That is just of the heaviest users?

Mr. BROCK. Yes.

Mr. HASTERT. Thank you.

Let me ask you something else. You also state that a warning screen pops out when a user enters the system to warn them that the system is for official use only, and official use, I would assume, is not being able to use this for political purposes; is that correct?

Mr. BROCK. I don't really know the answer to that.

Mr. HASTERT. I think they are probably, in most people's minds, a fine line, if there is a line between governmental use and political use.

Mr. BROCK. I am not sure if I were in the position of running correspondence that I would be able to answer that question, I am sorry.

Mr. HASTERT. That is a fair response. Most of us have a fairly good idea of what is on each side of that line.

This is a warning. Does it actually prevent users from misusing the data in the White House Data Base?

Mr. BROCK. No, it wouldn't prevent it, but it is an important first step in a good control program.

Mr. HASTERT. It says, I am warning you this is not good to do; however, if you leave this thing without logging out, somebody else could go along and collect this stuff at their leisure?

Mr. BROCK. That is true.

Mr. HASTERT. Finally, you state there are access restrictions with regard to which users can use certain data and print certain reports. Do you know if these features have always been in place in the White House Data Base system?

Mr. RHODES. We have been—it has been presented as a standard part of the design, so we can only assume it has been there the entire time.

Mr. HASTERT. Do you think that is a fair assumption, or don't you know?

Mr. RHODES. We really don't know if it's a fair assumption or not, because we haven't gone back to early source code and verify.

Mr. HASTERT. Would it surprise you to learn that contractor documents indicate that these features apparently weren't installed until spring of this year?

Mr. RHODES. Yes.

Mr. HASTERT. It would surprise you?

Mr. RHODES. Yes, it would surprise me.

Mr. HASTERT. It appears on the bottom line that the controls put in place at White House really don't go far enough to effectively prevent the misuse of personal and political data, and the White House must install an audit trail to ensure that this data is not being misused. That is the bottom line. We have to know, and there has to be the correct procedures put in place that we know that there is an audit trail and we can find out what is being abused, whose information is being abused and whose information is not being abused.

I agree with my good colleague and friend Mr. Peterson that if this is wrong, it shouldn't be done. It shouldn't be done in the White House or in Congress or anywhere else where people have the right to collect and analyze people's personal data. I think that those audit trails should be in place. I would hope that you would continue to pursue this because I think we will probably be asking more questions.

I thank you for your answers and your candid testimony here, and I will yield back my time.

Thank you, Mr. Chairman.

Mr. MCINTOSH. Thank you Mr. Hastert.

We will go for one final round of questioning. Mr. Peterson.

Mr. PETERSON. Mr. Chairman, first of all, at this point I don't think there has been any proof that there has been any abuse of anything. So let's just—there are still some questions, but I really have a problem of saying that we have discovered there is any kind of abuse.

The information that is in this system has been provided by the individuals. They sign off. There is a form that they sign saying, we know that this is going to go into the system and so forth. So let's be clear about what is in the system. The information that is in here that some people are complaining about, political party affiliation, ethnicity, these kinds of things, were also asked for—if you look at the contract that the Bush administration put out, they are also in there. So this isn't anything different in that regard.

I think the one question that I have, and I think I know the answer to this, but we maybe need to investigate it further, is how—there are 774 documents where the word "contributor" appears, and I guess I have a question as to where—where they came from and how they got into the system. They probably came from some electronic source someplace. I am not sure there is anything sinister there, but that is one thing I would like you to investigate is where they came from and why it says "contributor."

Mr. BROCK. Yes, sir, we will.

Mr. PETERSON. There is no contribution information, but apparently the word appears, or they are in some block or something. Frankly, at this point what is in this Data Base I don't think is

probably very different than what has been in other Data Bases in the White House, and I don't think we have proved at this point that anybody has abused anything, and maybe there will be something that will come out, but frankly, I haven't found it at this point in my looking at this. So I just want to make the record clear on that, and we will continue to hear from other people, I guess.

Mr. MCINTOSH. Thank you, Mr. Peterson.

Mr. Ehrlich, do you have anything?

Let me just do one quick followup on a question Mr. Hastert asked, and I appreciate, Mr. Brock, that you haven't looked at the data or the uses of the data, and therefore it wouldn't be within the purview of your audit to determine whether they were used for political or official purposes. But in a technical sense is it possible from what you know of the Data Base to make queries about individuals on the system and look them up by the entry under the source and relate that to information under the issues category or under political affiliation category? Is the Data Base constructed in such a way you can make those relational comparisons?

Mr. BROCK. The way the Data Base is constructed, that would be a difficult query, but you could write a query that could instruct the Data Base to search for those variables and come up with a list.

Mr. MCINTOSH. If you were pulling up individuals on the screen, is it possible to identify individuals, say, a group of 20, by one of the source categories and then check which issues they might have been interested in?

Mr. BROCK. Yes, you could do that.

Mr. MCINTOSH. So at least in theory it is possible that you could use some of the information that appears to be political in nature in keeping track of government functions or what issues they are concerned on that are being acted on by the White House. I agree with Mr. Peterson, we have to be careful in saying what evidence we have of that use.

One of the problems we have got is there isn't an audit function that's been installed or turned on in determining that, but we in the subcommittee are committed to getting to the bottom of that, and each one of these references that we have had today about possible uses of the system is a subject of a question that we have addressed to the White House, and we haven't received adequate answers yet, and the committee will remain committed to it, and I commend you in your efforts and urge you to complete your report. As you mentioned earlier, it is just an interim report.

One of the things I will note, just for the record, in the subcommission of Mr. Peterson's from the Bush administration, on page 32, one of the requirements they have is you have an audit trail with sufficient information regarding whether Data Base access shall be captured to record who did what, when and where. At least they were mindful in the previous administration of the need to provide that security measure.

I have no further questions of the panel, and thank you very much for your participation today and your hard work, and I urge you to continue diligently in working on that. Hopefully we will get close to the 2-week estimate in the next couple of weeks.

I understand, Mr. Hastert, you have a final question for the panel?

If there are no further questions for this panel, thank you very much. We will move on to the next panel.

Let me now call forward our panel of legal experts, Professor Lillian BeVier and Professor John Harrison, both from the University of Virginia Law School. If I could ask both of you to come forward and also remain standing. As I mentioned, Mr. Clinger asked we administer the oath to all witnesses before the subcommittee.

[Witnesses sworn.]

Mr. MCINTOSH. Thank you.

Let the record show both witnesses answered in the affirmative.

Let me turn now to Professor BeVier. Thank you for coming today. I am familiar with many of your writings, and you have great expertise not only in constitutional law, but in questions of what is the appropriate use for taxpayer funds by various administration officials.

Do you have a prepared statement to share with us today?

Ms. BEVIER. I do, Congressman.

Mr. MCINTOSH. If I could ask you to submit the full statement for the record, and if you could summarize the important points today for the committee.

STATEMENTS OF LILLIAN R. BEVIER, DOHERTY PROFESSOR OF LAW AND ELIZABETH D. & RICHARD A. MERRILL RESEARCH PROFESSOR OF LAW, UNIVERSITY OF VIRGINIA SCHOOL OF LAW; AND JOHN HARRISON, PROFESSOR OF LAW, UNIVERSITY OF VIRGINIA SCHOOL OF LAW

Ms. BEVIER. Yes, I certainly will do that.

I have been invited here as a scholar who has done some writing and thinking about the subject of legal and institutional mechanisms for protecting privacy of information about individuals that is in the hands of government. I have been asked to offer a few thoughts in general terms and in principle that may be relevant to the White House Data Base and its implications for individual privacy.

I want to concentrate my own remarks on what ought to be the standards for the handling of personal information by the government and to suggest to you some reasons why in principle you and your constituents might be concerned about certain aspects of the White House Data Base. Others, in particular my colleague Professor Harrison, will address questions about whether the Data Base represents a proper expenditure of taxpayer funds, and I will confine my remarks to the privacy issues.

I first draw your attention to the Code of Fair Information Practices that was founded in 1973 by what was then the Department of Health, Education and Welfare is now HHS. The code incorporated the following precepts: First of all, there must be no personal data recordkeeping systems whose very existence is secret. Second, there must be a way for an individual to find out what information about him or herself is in a record, and how it is used. Third, there must be a way for an individual to prevent information about him or her obtained for one purpose or from being used or made available for other purposes without consent. Fourth,

there must be a way for an individual to correct or amend a record of identifiable information about him or her. And fifth, any organization creating, maintaining, using or disseminating records of identifiable personal data must assure their reliability for their intended use and must take reasonable precautions to prevent misuse of the data.

Now, I have never seen, nor have I read, nor have I heard, a dissent to the values that these principles represent, nor have I ever heard it suggested by anyone that the implementation of these principles by the government should be limited to situations in which they are required to be observed by law.

Instead, these principles represent universally applicable aspirations concerning how the government should treat information about individuals that comes into its hands.

So whether or not the Privacy Act itself mandates that the White House Data Base comply with its technical requirements, it seems reasonable to hope and to expect that the executive branch would not need to be prodded to embrace the spirit of this Code of Fair Information Practices.

It's important to acknowledge, I think, that it's not, per se, illegitimate for the White House to attempt to establish and maintain an efficient information management system that would include relevant information about individuals with whom the administration has been, for one reason or another, in contact. Some kinds of personal recordkeeping do just seem to be variations on the "Rolodex" theme.

And it's also important to acknowledge that computer technology enhances everyone's, including the administration's, ability to gather and store and analyze and process information of all sorts, not excluding information about individuals. And few would argue that it's per se illegitimate for the administration to exploit this new technology.

At the same time, it's important, I think, to acknowledge that there are a number of contexts in which the collection or storage or processing of information about individuals by those with governmental power would be universally condemned.

For example, condemnation would rightly ensue were officials in the executive branch to use power of the government, in combination with personal information about individuals that they acquired in their capacity as government officials, to intimidate or punish their political enemies or to bestow unwarranted or illegitimate favors on their political friends.

Such uses of information about individuals by governmental officials would clearly breach the public trust. They would not only threaten the exercise of constitutionally guaranteed first amendment rights but they could serve no identifiable public purpose.

This is why the Privacy Act, for example, not only limits the use of disclosure of personally identifiable information by government agencies but also, with minor exceptions not relevant here, forbids the maintenance of records that describe how individuals exercise the political freedoms guaranteed to them by the first amendment.

Also, just as computer technology can add significantly to the value of information in the government's hands by enhancing its efficient processing and storage and recombination, so does that very

same technology multiply the opportunities for the misuse and abuse of information by unauthorized persons for unauthorized purposes or even by authorized persons for unauthorized purposes.

This is a particular problem with respect to information about individuals whose privacy and political freedom is thereby put at risk, and this is why, for example, the Privacy Act requires agencies to maintain something that is quite analogous to, although not explicitly the same as, what you might call an audit trail, that permits monitoring to ensure that only authorized users have access to particular kinds of information and to make certain that information about individuals is, in fact, put to the particular public purposes for which it was gathered.

The privacy problem with which this subcommittee is ultimately concerned seems to me to be fundamental and pervasive and endemic to an activist government. The challenge you face is a triple one: How to guarantee, first, that the government makes only legitimate use of personal information that it collects from individuals; second, how to make credible the promise that the government vigilantly protects the privacy of its citizens; and, third, how to provide individuals with reliable access to their own personal records so that they themselves can monitor the government's use of information about them.

In meeting this triple challenge, I believe that we as citizens are, to a very real extent, at the mercy of the good faith and personal integrity of governmental officials. We are forced, in fact, to offer governmental officials our trust, whether they prove worthy of it or not.

The challenge of ensuring access to, privacy of, and proper use of personal information by government can probably not be met by trying to hold government officials legally accountable to more Draconian laws. The challenge can only be met by electing trustworthy persons and then by holding those whom we do elect strictly accountable, politically and personally, for the use or the abuse of the trust we place in them.

I think the word that I would emphasize—and I will probably repeat it in the context of the questioning that will follow—is “accountability.”

Thank you.

Mr. MCINTOSH. Thank you very much, Professor BeVier.

[The prepared statement of Ms. BeVier follows:]

**Summary of
Testimony of Professor Lillian R. BeVier
Doherty Charitable Foundation Professor of Law
University of Virginia Law School**

**Before the House of Representatives
Committee on Government Reform and Oversight
Subcommittee on National Economic Growth, Natural Resources and
Regulatory Affairs**

September 10, 1996

As a scholar who has studied and written on the subject of legal and institutional mechanisms for protecting the privacy of information about individuals in the hands of government, I am present today at the invitation of the Subcommittee. I have been asked to offer some thoughts regarding the White House Data Base (WhoDB) and its implications for individual privacy. It is a privilege to be of possible assistance to the Subcommittee.

I want to concentrate my remarks on what ought to be the standards for the handling of personal information by the government, and to suggest some reasons in principle why you and your constituents might be concerned about certain aspects of the WhoDB. Since others will address questions about whether the WhoDB represents a proper expenditure of taxpayer funds, I will confine my remarks to the privacy issues that the data base might be thought to raise.

I first draw your attention to the Code of Fair Information Practices that was propounded as long ago as 1973 by what was then the Department of Health, Education and Welfare. The Code incorporated the following precepts:

- 1) There must be no personal-data record-keeping systems whose very existence is secret.
- 2) There must be a way for an individual to find out what information

about him is in a record, and how it is used.

- 3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- 4) There must be a way for an individual to correct or amend a record of identifiable information about him.
- 5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability for their intended use and must take reasonable precautions to prevent misuse of the data.

I have never seen nor read nor heard a dissent to the values that these principles represent, nor have I ever heard it suggested by any one that the implementation of these principles by the government should be limited to situations in which they are required by law (such as the Privacy Act, which embodies them) to be observed. Instead, these principles represent pervasive aspirations concerning how the government should treat information about individuals that comes into its hands. Thus, whether or not the Privacy Act mandates that the WhoDB comply with its technical requirements, it seems reasonable to hope and expect that the Executive Branch would not need to be prodded to embrace the spirit of the Code of Fair Information Practices that the Act embraces.

It is important to acknowledge that it is not per se illegitimate for the White House to attempt to establish and maintain an efficient information management system that would include relevant information about individuals with whom the Administration has been for one reason or another in contact. It is also important to acknowledge both that computer technology enhances the Administration's ability to gather, store, analyze, and process information of all sorts, including information about individuals, and that it is not per se illegitimate for the Administration to exploit this technology.

At the same time, however, it is important to acknowledge that there are a number of contexts in which the collection, storage, and processing of information about individuals by those with governmental power would be universally condemned. For example, condemnation would rightly ensue were officials in the Executive Branch to use their governmental power, in

combination with legitimately acquired personal information about individuals, to intimidate or punish their political enemies or to bestow unwarranted favors on their political friends. Such a use of legitimately acquired personal information by a governmental official would clearly entail a breach of the public trust. It would not only threaten the exercise of constitutionally guaranteed First Amendment rights, but it could serve no identifiable public purpose. This is why the Privacy Act not only limits the use and disclosure of personally identifiable information by government agencies but also (with minor exceptions not relevant here) forbids the maintenance of records that describe how individuals exercise rights guaranteed by the First Amendment.

In addition, it is important to acknowledge that, just as computer technology can add significantly to the value of information in the government's hands by enhancing its efficient processing, storage, and recombination, so does the very same technology multiply the opportunities for the misuse and abuse of information, in particular information about individuals. This is why, for example, the Privacy Act requires agencies to maintain "audit trails" that permit monitoring to insure that only authorized users have access to particular kinds of information, and to make certain that information about individuals is in fact put to legitimate public use.

The problem with which this Subcommittee is ultimately concerned is fundamental, pervasive, and endemic to an activist government. The challenge is a triple one: how to guarantee, first, that the government makes only *legitimate* use of personal information that it collects from individuals; second, how to make credible the promise that the government vigilantly protects the privacy of its citizens; and third, how to provide individuals with reliable access to their own records so that they themselves can monitor the government's use of information about them. In meeting this triple challenge, I believe that we as citizens are to a very real extent at the mercy of the good faith and personal integrity of government officials: we are forced, in fact, to offer government officials our trust, whether they prove worthy of it or not. The challenge of insuring access to, privacy of, and proper use of personal information by government can be met only by trying to elect trustworthy persons and then holding those whom we do elect strictly accountable for the use---or the abuse---of the trust we place in them.

Mr. MCINTOSH. Let's hear from both witnesses. So, Professor Harrison, if you could share your proposed testimony, and then we will have questions for both of you.

Mr. HARRISON. Thank you, Mr. Chairman. I do have a prepared statement. I would like to enter that into the record, and I will just say a few things.

Testifying before any body of the House of Representatives on appropriations questions, of course, is like being asked to brief the Pope about doctrine. But I will try to outline some of the fundamental principles that I know are quite familiar to the subcommittee.

The basic idea of Federal appropriations law, of course, is the straightforward one that appropriations are available for their objects, for the purposes for which they are appropriated, and not for other purposes. That means they are available for public purposes and not for other purposes.

In a context like this, there is a more pointed and also well-known corollary: that although there may be inevitable political uses of public funds by certain high officers, such as the President of the United States and elected Members of the House of Representatives and the Senate, public appropriations are not supposed to be available for campaign activities. Political Campaign activities are not supposed to be funded with public money. They are supposed to be funded from other sources, except in the case of public funding for Presidential campaigns, where the accounting rules are supposed to be quite strict to keep everything straight and on the up and up.

So the question one wants to ask in looking at some of this information, in particular the information maintained apparently under the heading "political participations," is: how does having that information that's available to the President's personal staff, his eyes and ears, the people who work with him personally—how does having that information available to the President through his personal staff further the President's public functions as opposed to furthering campaign functions?

Everybody expects the President to be involved in political campaigns. Modern Presidents are political figures. That's not news. Naturally, the President is involved in the campaign activities of his national party. Naturally, a President who is running for reelection has his own principal campaign committee. Of course he does, and of course he is going to be involved in raising funds for those efforts.

The point, of course, that's well-known is that the President is not supposed to be using public funds in his fund-raising activities, or any of his political campaign activities.

And so, again, to apply the appropriations law principles, the question that one needs to ask is, how does this information, this particular information being maintained in a publicly funded Data Base, further the President's public and perhaps his political activities as opposed to his political campaign activities?

At this point, we can just try to infer what the reasoning of the White House must have been. As far as I know—I mean, we don't know what the line of reasoning was; I don't know what kind of advice of counsel they received. So we have to try to come up with,

any plausible story that we can and try to evaluate it, as to what the public use of information like this would be.

And that's the problem. That's what's troublesome here. It's very hard to come up with an explanation like that, whereas it's very easy to come up with an explanation connected to campaign activities—in particular, campaign fund-raising.

Naturally, campaign organizations, as part of their fund-raising activities, are going to have lists of how people participated with them. Of course they do that. But why does the government need such a list? Does it need such a list in order to know what somebody's ideological attachments are, what his political associations are?

The trouble with such a story is, first, that there are much more direct ways to know somebody's political affiliations. And do I infer correctly that, in fact, political affiliation is a separate subject that can be searched in this Data Base other than political participations?

Mr. MCINTOSH. Based on the Arthur Coia example, yes, there's a "political affiliation" category as well as a category called "sources" that has political information in it.

Mr. HARRISON. The logical thing to do, if the President needs to know whether somebody is a political friend or a political opponent, is to have information about somebody's political attachments, where he or she stands on the ideological spectrum.

I suppose there is another less appetizing possible use for information like this. If you take it that American political practice has established that it's a permissible use of public office to reward those who help to raise you to office, perhaps you would want to have information as to who those people were so that you could allow it to influence policy. That's obviously very troubling in all sorts of ways.

So both of those possible explanations have serious difficulties associated with them. The first is not terribly plausible; the second is kind of unappetizing. Whereas the explanation for having this information that seems most natural to me is that it's associated with political fund-raising. That's a perfectly fine explanation as long as it's done by a political campaign organization.

So one is left to wonder, what is the purpose of having information like this available for the President in his public, taxpayer funded functions? That's the hard question, and that's the mystery here at this stage.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Harrison follows:]

Statement of
John C. Harrison
Associate Professor of Law
University of Virginia

Thank you Mr. Chairman. The Subcommittee has requested that I testify on the appropriations law aspects of the White House's decision to maintain political contributor information in a database used to support the President's official activities.

At the outset, I should emphasize that my comments will reflect the fact that, like the rest of the public, I have incomplete knowledge of the facts. What we do know, once again, is that appropriated funds were used to collect and maintain information about individuals' political activities and in particular their financial contributions to various campaign organizations. I assume, for purposes of this analysis, that the funds at issue were from an appropriation for the purpose of providing assistance to the President.

We also do not know the reasoning on which White House decision makers based their conclusion that this is a permissible use of appropriated funds. I am thus unable to comment on their rationale. Instead, I will discuss possible arguments.

Three possible reasons for keeping this information for the President's use have occurred to me. The first involves what might be characterized as a public purpose but is not very plausible. The second also involves what might be a public purpose, but it is troublesome in various ways and in certain circumstances raise independent legal problems. The third is very plausible and as far as I can tell otherwise lawful, but it does not involve a public purpose and hence would not represent a permissible use of appropriated funds. This third, quite plausible possibility is that the purpose of maintaining these data was to assist the President in political campaign fund-raising.

The fundamental principle of federal appropriations law is almost tautological: appropriated funds may be applied only to their statutory objects. One standard corollary of this is that appropriated funds may be applied only to governmental purposes, not private purposes.

Such generalities often do not decide concrete cases. With respect to the White House and funds appropriated to the President, however, they imply a more specific principle that is of

central importance here: appropriated funds may not be used for political campaigns. The President's job is to preserve, protect, and defend the Constitution, and to take care that the laws are faithfully executed. It is not to run for President, or to help other people run for office.

To put the same point slightly differently, the President is President of the entire country, but he is a leader and the candidate only of his political party. Everyone's tax dollars go to pay his official expenses, but for his campaign expenses he must turn to other sources.

Just as it is a commonplace that appropriated funds may not be spent for campaign purposes, it is well known that the modern presidency is not the office envisioned by the Federal Convention and occupied by George Washington. Modern Presidents are political figures in ways that President Washington was not; in particular, they are associated with political parties. There is a vital difference, however, between political activities and political campaign activities. That difference sometimes will involve difficult questions of line-drawing. But sometimes those questions will not be so difficult.

In a similar fashion, difficult problems can arise when an expenditure unavoidably supports both public and campaign functions at once. The job of the Secret Service is to be with the President whatever he is doing, whether he is appointing to an office, jogging, or addressing a campaign rally. Once again, however, the fact that there are hard questions does not mean that there are no easy ones.

The question we need to ask is thus this one: What governmental purpose is served by letting the President know what political contributions people have made? What is his need to know, as chief executive of the federal government, about such payments? What would he want that information for?

One possibility is that, because the presidency is political and politics is partisan, the President needs to know who his political friends are. He needs to know whether and how strongly people support him and his policies.

This rationale might support keeping official records of Americans' positions on policy questions, and perhaps of their political affiliation. When the President goes into a meeting, his aides might brief him on the policy stances and political attachments of the various participants. When he works a cocktail party, he might need the same information to further his policies among those present.

As for contributor information, the story thus would go something like this: An individual's financial support of various political campaigns is a good indicator of his or her political views. Money talks, people put their money where their heart is, or whatever you like.

Of course, if the President's staff were trying to use political contributions as a proxy for political views they would need to combine these data with other information. Politics being what they are, lots of people contribute to political campaigns and organizations that are opposed to one another. Indeed, it is common, apparently, for PACs associated with economic interests to contribute to both candidates in one election, and to contribute to both political parties. Hence information about political contributions, standing alone, could be very misleading: the President might think that someone was favorably disposed to him politically, only to learn that the individual in question was hedging political bets.

So if this information were being maintained as an indicator of people's policy commitments, we would expect the White House to have sought, for example, information about contributions to the Republican National Committee and its campaign organizations, and to the Bush campaign in 1992. As far as I know the database does not include this information.

My observation about covering political bets, of course, brings out another purpose of political contributions: to obtain influence or, as it is said, access. One contributes to both candidates so that, whoever is elected, one will have access and influence.

A cynical but insightful definition of an honest politician is one who stays bought. In order to be honest, by this definition, a politician who has achieved office needs to know who his contributors were. That, as I just noted, is different from knowing who one's supporters are on substantive issues.

This theory assumes, of course, that dispensing official favors to repay one's political debts is a legitimate use of public office and therefore a legitimate use of public funds appropriated to support the activities of that office. Whether that is true is the subject of debate. Of course, it should be borne in mind that certain quid-pro-quo transactions concerning campaign contributions in exchange for public benefits are federal crimes. See, e.g., 18 U.S.C. 600.

Neither of the stories I have suggested so far is very wholesome: one involves researching people's political contributions in order to get at their policy views, while the other involves the use of office to repay campaign contributions. Both, however, tell a story about government purposes, at least on one rather cynical view of government.

There is, of course, a much less troublesome reason for knowing about someone's political contributions: so that you can know where to turn next time you need a political contribution, so that you can encourage people to continue their support. If you are running the Virginia Republican Committee, or the Maryland Democratic Committee, or the Democratic National Committee, it is part of your job to know who gave money and how much. There's nothing unwholesome about it, any more than there is anything unwholesome about officials of any non-profit organization knowing the names of their contributors and the amounts they have given. That information makes possible the kind of recognition and continuing relationships on which non-profits thrive. Indeed, with the contributors' consent non-profit organizations routinely make public people's contributions, in order to recognize their commitment and to encourage other supporters of the non-profit organization to emulate their generosity. As a believer in private charitable activity (and private political activity) I find these efforts laudable. I hope that all the non-profits I support about have the best available software for fund-raising.

This reason for maintaining computerized contributor information is fine and admirable. The story it suggests is an eminently believable one. It is, though, the reason of the relevant non-profit organization, be it the Nature Conservancy or the Republican National Committee. If the President's reason for knowing about political contributions is so that he can help encourage people to make further political contributions, then he is acting in his capacity as candidate or party leader. Public funds, of course, may not lawfully be expended in support of such activities. Taxes are not campaign contributions, and they are not supposed to be used to encourage other campaign contributions.

(This testimony is provided to the Subcommittee as a public service. It is not presented on behalf of any client or the university where I teach.)

Mr. MCINTOSH. Thank you, Professor Harrison.

Let me start out with a series of questions designed to make sure that I follow the legal strictures here that both of you have talked about.

Professor BeVier, on the Privacy Act, am I correct in summarizing your description of the principles involved there, that government agencies aren't allowed to keep lists that reflect people's first amendment—exercise of their first amendment rights, unless they have a legitimate governmental purpose?

Ms. BEVIER. Yes.

Mr. MCINTOSH. And so that even the creation of such a list, without a legitimate governmental purpose, would be a violation of the Privacy Act?

Ms. BEVIER. Yes. I think—the only qualification I would have there is that I have to enter a caveat here with respect to the question of whether the Privacy Act itself applies. Part of my analysis—in fact, the burden of my analysis—is to suggest that I am talking about principles of governmental behavior rather than actual legal strictures. But if we assume that the Privacy Act applies, the answer would be, yes.

Mr. MCINTOSH. And I understand that that's a technical question based on certain offices encompassing the Presidency. Let us, for purposes of this question, assume that the Privacy Act does apply, and we will try to seek information on whether that's the case.

Ms. BEVIER. All right.

Mr. MCINTOSH. If it does apply, is that legitimate purpose a one-time purpose or—and after that, is it required of the agency to get rid of or eliminate or destroy or no longer use the list? Or can it be an ongoing purpose, legitimate government purpose?

Ms. BEVIER. Well, the Privacy Act requires that the Government agency keep records of personally identifiable information up-to-date and accurate and that they not keep information in the record that is not relevant to the particular purpose or for which it was gathered. OK? In other words, the information is required by the act to be timely and relevant.

Mr. MCINTOSH. Relevant.

So, for example, would somebody's party affiliation or title of an office within a political party—is that a first amendment right that they would—by choosing to be denominated a Democrat or a Republican, are you exercising a first amendment right?

Ms. BEVIER. I believe so.

Mr. MCINTOSH. OK. So there would have to be a legitimate purpose that was ongoing, and they would have to limit its use for that.

Obviously if people take a position on an issue, that would be an exercise of a first amendment right. Would there be a problem under the principles of the Privacy Act if the White House maintained a list of people who disagreed with them on issues? Nixon got into trouble with an enemies list.

Ms. BEVIER. Yes. In fact, I think that's one of the difficulties here. First of all, yes, it would be. And I think that particular aspect of the Privacy Act was incorporated precisely because of the concern of using personally identifiable information for—to punish political enemies. And the notion that if citizens believe that their

government can, in fact, collect that information—in particular, collect it in secret—and then use it to punish them for their political beliefs, they will be less inclined to exercise their first amendment rights.

So you have sort of two different faces of this coin. One is collecting information about your enemies, which makes it a violation of the Privacy Act in terms of punishing the exercise of first amendment rights. The other is collecting information about your political friends, which makes it, in some sense, an illegitimate use of taxpayer funds.

Mr. MCINTOSH. Turning to you, Professor Harrison, you have mentioned three possible theories about why the President may want to maintain this type of Data Base. The first is, that he wanted to know his supporters on particular issues; the second is, that he might want to reward supporters for their support; and the third is, that he might want to use it to facilitate campaign financing, seeking contributions.

Let me make sure I understand clearly. What was your view on the legality of using taxpayer funds to accomplish each of those three purposes?

Mr. HARRISON. From the standpoint of appropriations law, as opposed to any other Federal law—for example, the Privacy Act—the first is—seems fairly clearly—and, again, all of this is sort of—this is how business is done in government in the 20th century; it's not the way things were a long time ago. The President engages in political activities. He engages in political advocacy; he is a political figure; and, hence, there is some reason for the President to know where other people stand politically. There are obvious problems with that associated—that the Privacy Act is designed to address. But that, I think, is not terribly troublesome.

The second possibility, that the purpose of knowing who your financial supporters in the campaign are is to be able to reward them, is more troublesome both as a matter of general ethics and, of course, as a matter of the Federal statutes. At some point, quid pro quo transactions of contributions in exchange for political favors are a Federal crime. In any event, even vaguer transactions along those lines are very bothersome.

I hope the theory that the White House is relying on is not, we need to know who the President's political friends were so that we can do them favors in any way that's not actually a felony.

And finally, of course, there is a problem with what I think to be the most likely, the most plausible, explanation for keeping this information is to facilitate political fund-raising, sort of a fundamental principle of, here are the appropriations law, the idea that this is for public and not for political campaign purposes, that that's not permissible; that's something that public funds can't be used for.

As I say, sometimes there are difficult line drawing problems. But the straightforward use of public funds to support political fund-raising, political campaign activities, goes beyond the appropriation. I think everybody agrees with that.

Mr. MCINTOSH. Would that be a criminal violation if that was done?

Mr. HARRISON. It could be. It depends on further information about the circumstances. There is a criminal provision that enforces certain aspects of the appropriations law. That, though, is a harder question and one that depends a lot on the facts of the situation. So that's something we need to know more about to address with any real confidence.

Mr. MCINTOSH. OK. My time has expired. I would be interested in knowing what facts are relevant and which way they cut on that statute.

Mr. Peterson.

Mr. PETERSON. Thank you, Mr. Chairman.

It's curious to me why we are sitting here speculating about why the White House may have done this or that. It would seem to me it would have been a lot more relevant to have them here so they could answer rather than to have speculation about why they might have done this or that. I again want to point out that the former administration asked for similar information.

I think because—and it would be nice to have them on the record, and maybe we ought to just send them a letter and ask them—that the President is in a different situation than anybody else in the country in that he is in the White House and anybody that gets in there has to be cleared.

As Members of Congress, we can keep a separate Data Base of our political contributors. We can go down to the Hyatt Regency and have a fund-raiser and invite people over, and you don't have to go through the whole White House operation. The President can't do that.

So I think you have got a different situation, and I think that's part of why they are asking for this information—I am not sure—and part of why previous administrations also kept that kind of information.

You know, and as I understand it, and correct me if I'm wrong, but in 1982 the Reagan administration, there was a counsel—a White House counsel directive or proclamation that they were exempt from the Privacy Act. Is that—am I right about that?

Ms. BEVIER. I don't know. I think that various White House offices have asserted that they were exempt. I do—and there have been some legal—some cases that have said for a particular provision—for a particular administrative office—with respect to particular issues, the White House is exempt.

But I do think that that is an issue, with respect to this Data Base, that would very much depend on the particular facts and who was using it within the White House and so forth.

Moreover, I guess I would make a different point. I mean, I am not sort of claiming to be asserting that the White House should be held or is held to the provisions of the Privacy Act. I think what I am making is a more broad claim, in principle, with respect to the White House's willingness to be accountable for the way it treats information about individuals that comes within its ken.

Mr. PETERSON. Do you have any indication that they are not accountable? From what I have seen and what this administration has done in maintaining this Data Base is that every bit of this information is voluntarily given, and these people sign a release before the information goes in.

So, I mean, where are you making this allegation that there's not accountability and that they are, somehow or another, violating people's privacy? Do you have information that I don't have?

Ms. BEVIER. I didn't know that the individuals—the 200,000 people on this Data Base—that each one of them has signed a release saying—

Mr. PETERSON. There is information—as I understand it, if there's information of the kind that you are talking about, there's a release form that's signed where they voluntarily have given this information, Social Security numbers, private phone numbers, political affiliation, and all that sort of thing, and they sign off.

Ms. BEVIER. Do they sign off on them—

Mr. MCINTOSH. Mr. Peterson, let me interject and say that that contradicts what the White House has told us. They told us nobody has signed a release.

Mr. PETERSON. No; I mean, they—

Ms. BEVIER. What I would be interested in, Congressman, is not only whether people signed off, and I am not sure—I mean, if the facts support that assertion, then perhaps that's correct.

But what I would be interested in is what they then said about the possible future use of that information. One of the things that the Privacy Act and the principles that underlie the Privacy Act are concerned about, and that the use of computers has exacerbated as a problem, is the potential for reuse of information in ways that are unexpected by the person who might give the information voluntarily in order, for example, to get access to go to a White House dinner, for example, but then have it be used for purposes that are different, unexpected, and perhaps might have changed the individual's willingness to have the information be given in the first place.

So if you want to talk about the release, I would like to see what it says and how it is considered.

Mr. PETERSON. Well, I guess I—

Ms. BEVIER. And the second aspect of the question you are asking me about accountability is that we have talked this morning about the absence of an audit trail and how the very fact that the White House is not willing to or hasn't yet provided or turned on the function about what happens to the information when they get it, that's a lot of what accountability is about.

Mr. PETERSON. Well, Members of Congress, I don't think, have an audit trail either. Are you saying that we are up to something, too, and abusing the information we—

Ms. BEVIER. Well, you might be. You might be. But I would think that the power of the executive branch is rather different from the power of individual Members of Congress, which does not excuse either one from unwillingness to be accountable for how they are handling personal information.

Mr. PETERSON. Well, I don't think other Presidents have handled it any differently either, from what we know, and, as I understand it, the Reagan administration sought and obtained from the Office of Legal Counsel a formal ruling that White House records maintained on Office of Administration computers were exempt. That was in April 1982. And as I—the Reagan White House, the Bush

White House, and now the Clinton White House, as I understand it, are all operating under this same ruling.

Ms. BEVIER. As I suggested, Congressman, in my view, the issue is not an issue that is one that turns simply on the legalities and whether the Privacy Act covers it.

Mr. PETERSON. Yes. I think that's what we are trying to get at here. But at this point I don't think that anybody has—there has been a lot of allegations thrown around, but nobody has proven anything.

Ms. BEVIER. That's because we don't have the records of what's happened to the information. We don't have the audit trail. It's very hard to—

Mr. PETERSON. I don't think that's true. I don't think you can make that statement that we don't have the records. If people can't figure out how to analyze a Data Base, it doesn't mean that somehow or another whoever put the Data Base up is hiding something. It could be the ignorance of the people that are trying to look at this, and to some extent that's what it is. And there's a—you know, an awful deficit of people that have been looking at these systems in terms of their understanding of how all this works. I mean, that's become apparent to me.

So I just wish that we could have had the White House here so that they could have responded to some of these questions. I think we could have cleared up some of the speculation that's gone on.

Mr. MCINTOSH. Thank you, Mr. Peterson.

Let me return now to Professor Harrison.

Oh, I am sorry, Denny. I thought you had left. We have another round of questioning.

Mr. HASTERT. I think I do have time here.

Mr. MCINTOSH. Yes.

Mr. HASTERT. I would like to agree with my friend from Minnesota, Mr. Peterson; we don't know. But I think one of the reasons we don't know is that we don't have the audit trail. And also, when we have procedures in place that people don't log out and these things are left open, we don't know who is hacking in here and digging up what information and how it's being used. I mean, that's the question.

I go back. You know, I don't know how Members of Congress use their information systems and their computers, but I know how they are supposed to use them, and we have pretty strict rules around this place. As a matter of fact, I just worked the fair in my district all weekend, and there was a political booth, and down the way a little ways we had a governmental booth. And when I went to the political booth, I, you know, accumulate the stickers and all this kind of stuff and made very sure when I went down to the governmental booth, that we sponsored, that those stickers were off and we didn't mix politics with government and, you know, that the issues there were governmental issues, that that's what we had to talk about.

So I know that most of us—I am including my friend from Minnesota—probably go through excruciating pains to make sure that we don't mix political base—political information with governmental information. And I think it's pretty plain that if we do, any

Member of Congress that does that is somewhat remiss and could go before an ethics committee.

So one of the things that I am concerned about, and I go back, Professor, that you have testified that it would violate the Code of Fair Information Practices for information obtained for one purpose, that information was used for one purpose—obtained for one purpose and was used for another purpose without the individual's consent.

Sure, I might have a constituent that gets invited to the White House for one reason or another, even myself, and we give that Social Security number. That number, and any other information that may come up, can be accumulated, and we don't know what that information is being used for. We assume it's going to be used just for the gateway into the White House for some event. But what we are starting to find out, it can be used for a lot of things and could be used for even more things, even political things.

And so, really, we come down to the question, if somebody provided the White House with their name, Social Security number, and date of birth to visit the White House on a particular date, do you think that that's proper to store that information permanently on the White House Data Base and use it alone or in combination with other information for other purposes in the future?

Ms. BEVIER. No. I think that's at least questionable and certainly does violate the Code of Fair Information Practices. The storage alone violates it, not to mention the notion of collecting it just for letting you get in the gate and then keeping it permanently in a Data Base that, as you suggest, can be used for any number of things.

Some of those possible uses you might not object to, but some of them you might well object to. And part of the difficulty here is that what is being broadly asserted is the right just to enter them in the Data Base and trust us. We will use them appropriately.

Mr. HASTERT. And the follow-up to that then is that if you don't know, if the audit trails aren't in place, if the procedures aren't in place, if some people are trained how to use it and some people aren't trained how to use it, and, beyond training, what's right to do and what's right not to do, and if the protections aren't there, even if it said this is classified information but you leave your computer on without logging out and anybody that happens along can use it, then that's not the purpose; is that correct?

Ms. BEVIER. That would seem to me to be a troublesome thing.

Mr. HASTERT. And even beyond that, the problem is, people could misuse that information. That is the whole issue here.

Ms. BEVIER. Yes, that's right. And that feeds into my notion about accountability: that an ability to find out what has been done with the information, where it's being kept, who is using it, who has access to it, for what purpose, is a way to make the people who have the information—

Mr. HASTERT. And I assume that you sat here and listened to the testimony by the previous panel.

Ms. BEVIER. I did.

Mr. HASTERT. Basically what they said is, there isn't any accountability. I mean, the audit trails aren't in place. People don't

log out. The principal users even don't log out, aren't following this procedure. So it's a very, very dangerous situation.

Professor Harrison, let me ask you, following on your other testimony, you said the system is designed to include information on issues and positions held. Would it be disturbing to you to know that these issue fields are not used extensively but the source and political participation fields are?

As a matter of fact, I understand the political participation basically is another word for contributions, which really doesn't ask for contributions in the computer itself.

Mr. HARRISON. That, again, leads one to wonder what use the appropriation is being put to. The frequency with which different functions of the Data Base are used is an indication of what its actual purpose is, of what it's really being used for. And to the extent that it's really being used for the acquisition of information, that's sort of—you know, I think to any reasonable person, sets off these alarm bells, leads one to wonder, what other than political fundraising activities do you want that information for?

Yes, it's quite disturbing.

Mr. HASTERT. One last question. In your testimony, you testified that certain quid pro quo arrangements regarding political contributions would be Federal crimes, both for the Congress as well as for the Executive Office. You cite Section 600 of the U.S. Criminal Code which provides that it is a Federal crime to directly or indirectly promise any employment, position, compensation, contract, appointment, or other benefit or any other special consideration in obtaining any such benefit, favor, or reward for any political activity or for the support or any opposition to any candidate or political party. That's out of the text of the statute.

So let me ask, an arrangement where the President or the White House staff offers special consideration or other benefits in exchange for political or campaign support would violate the Criminal Code, in your opinion?

Mr. HARRISON. Easily could. Again, you don't want to accuse even a hypothetical person of violating a Federal criminal statute without knowing all the facts.

Mr. HASTERT. No, we are not accusing anybody. But with that apparatus in place—

Mr. HARRISON. Section 600 is—

Mr. HASTERT. For people not even responsible for other people—not responsible, to be able to come in and hack out information, that's a dangerous situation.

Mr. HARRISON. It certainly looks that way.

Mr. HASTERT. Thank you, Mr. Chairman. I thank the people who testified today.

Mr. MCINTOSH. Thank you, Mr. Hastert.

Let me now pursue with Professor Harrison the line of questioning we began in my earlier questions.

We were talking about your third theory, which you indicated you thought was perhaps the most likely theory. Is it the Anti-deficiency Act that forbids the use of appropriated funds for nongovernmental purposes, specifically, political activities?

Mr. HARRISON. It forbids the use of appropriated funds for anything but the objects for which they are appropriated, which in this

case means nongovernmental activities, meaning especially political campaign activities.

Mr. MCINTOSH. And that is a criminal statute?

Mr. HARRISON. There is a criminal enforcement provision for the Anti-deficiency Act.

Mr. MCINTOSH. Would it be lawful for the White House to collect and maintain, at taxpayer expense, contributor information or information about potential contributors? We often refer to them as "prospects," in campaign parlance. And then would it be lawful for them to maintain that for their own use?

Mr. HARRISON. Again, that sounds very much like the use of appropriated funds for a purpose other than what they are appropriated for. The purpose of identifying a prospect is in order to encourage the prospect to make a political contribution. And that's campaign fund-raising. That's what the appropriated funds aren't for.

Mr. MCINTOSH. If that information was passed on to the DNC or the Presidential Reelection Campaign, would that be a lawful use of taxpayer funds?

Mr. HARRISON. I can't see how. I mean, again, it's the DNC, the reelection campaign, that's supposed to have the information in the first place, keep it and use it, rather than the White House as such.

Mr. Peterson is absolutely right, there's going to be a certain amount of rubbing around, especially with the President of the United States, who necessarily has a large entourage around him. Some incidental transmission of information like that, jotting it down somewhere, yes, something like that can happen.

Systematically keeping the information on a public Data Base rather than systematically keeping it by the DNC or the RNC seems to me to be another phenomenon.

Mr. MCINTOSH. And apparently some of it may depend on who was staffing the President and in what capacity. You have got people in the Social Office inviting people to White House functions. You have got people in the Political Affairs Office maintaining contacts and liaison with the political parties. But then you have also got people in the Office of Management and Budget working on budget; the Office of Administration performing the function of administering the White House government agencies; the National Security Agency.

From your experience at OLC, can you imagine any circumstances in which offices such as the Office of Administration or the Office of Management and Budget would have a need for political information about whether somebody contributed or supported the President?

Mr. HARRISON. That is very difficult to see. And the question you asked makes an important point, which is that it is important to know not only the purpose for which the money is being expended, and hence the function with which it is associated—is that a legitimate public function—but which appropriation the money is coming out of, because the incidental assistance to the President that Mr. Peterson, I think, was talking about, and, as I say, as unquestionably happens in every administration, there's a particular appropriation that's supposed to come out of.

It is not, for example, supposed to be provided by the Department of the Interior. Those funds are not at all to help the President. Some of this assistance comes from the Secret Service appropriation. I mean, there are a few of them.

But there are a lot of appropriations even that can't come out of. That's sort of necessary, incidental rubbing together of the President's official and political capacities.

Mr. MCINTOSH. And within the White House appropriation, which I think is part of the Treasury-Postal bill, there are segregations even there among functions and offices. The Office of Management and Budget is separate from the President's personal staff?

Mr. HARRISON. Right. There's one for the White House Office. There's one for the Office of Administration. I believe the NSC has its own. I don't remember every line, but yes. The Executive Office of the President has a bunch of subappropriations under it.

Mr. MCINTOSH. And let me ask a general question of either witness, or perhaps both of you could share your thoughts. Can you think of any legitimate governmental purpose or reason for keeping information on who received DNC or Clinton/Gore Re-elect communication in this White House Data Base?

Mr. HARRISON. As opposed to the White House Christmas card and so forth, you mean the one that came from the campaign organization?

Mr. MCINTOSH. That's correct.

Mr. HARRISON. It's very hard to imagine what that has to do with the President's official functions, even his political functions as opposed to his campaign operations.

Mr. MCINTOSH. Professor BeVier, did you have anything you wanted to add on this matter?

Ms. BEVIER. No. It's really not my area of expertise. But one of the things you sort of consider is, well, what happens if it is decided that this Data Base, in fact, is going to survive from one administration to the next, so that what is a friends—political friends list in one administration becomes potentially a political enemies list in another.

Now, that is a real—a real privacy concern, because then you have flipped from, again, the possibility of misusing Government funds to collect and store the information to the possibility that—a very different possibility of using it to generate, willy nilly, a political enemies list.

So that's not quite your question, but it's sort of a scary possibility.

Mr. MCINTOSH. Let me zero in on that possibility in just one context. We have the Presidential Records Act which requires that Presidential records be taken out of the White House and delivered to the Presidential libraries. But there seems to have been an effort in this White House to recreate at least the White House personnel lists from the previous administration. And this isn't quite on point for this hearing, but the full committee has been looking into this. Would there be a Privacy Act concern about recreating that list of people who had worked in a previous administration and then obtaining their FBI background files?

Ms. BEVIER. That's a hypothetical question, I assume, and I—

Mr. MCINTOSH. It's very fact based.

Ms. BEVIER. Well, it certainly does raise some concerns, yes. I mean, I don't like to give a sort of straight up answer, but that seems to me to be the precise kind of thing that the Privacy Act is designed to at least permit individuals to monitor, so that at least, at the very least, you would say that the individuals whose names were in those files were told, before they were put in them, that that's what was happening and then had a chance to correct them and also had a chance to follow the trail that they took and to see how they were used, because that's an important aspect of the Privacy Act, this kind of enforcement by individuals of the use of information about themselves that the government makes.

Mr. MCINTOSH. Thank you. My time has expired.

Mr. Peterson.

Mr. PETERSON. Well, Mr. Chairman, thank you.

Just, you know, to—to summarize all of this, I think we need to step back and, you know, the information that's in this system is voluntarily given. You know, some of what you said, you were getting mixed up with the pass system that you have to use to get into the White House, which is a totally different situation. And part of the reason they need the information, people that aren't on the E-pass system or are not in the permanent system to get into the White House, you have to have a Social Security number, you have to have this other information to make sure that that person can get cleared on a temporary basis into the White House.

So I think I need just to point out that there's 200,000 records on this system. We don't know exactly how many people. I am not aware of anybody that has complained about misuse by the White House of information that's in this system. I don't know of one single person who has come forward and complained.

To say that somehow or another they are that keeping contribution information, there's only 774 entries out of 200,000. That doesn't seem like any kind of concerted effort to keep contribution information. We don't know where that came from. But my guess is, it's some electronic information that was transferred when these lists were brought in in the first place.

In terms of the political information, as I understand the system, people at OMB, people in the Office of Administration, do not have access to that part of the system. The people that have access to the political affiliation are the people that are in the Political Affairs Office that need that information so that the President can invite, you know, Democratic Members of the Congress to a meeting or Republican Members of Congress to a meeting or Republican State chairmen to a meeting, or whatever it would happen to be.

I think there is a legitimate reason to have political party affiliation, you know, for the Political Affairs Office, and there's really no other way to do that.

So, you know, until I know of somebody that's come forward and says that somehow or another something has happened here that they think has violated their privacy, I think we are doing a lot of speculation. I think it would be better to bring the White House in and have them explain to us why this information is there rather than to just sit around and speculate about what could be the situation.

Do you want to respond?

Ms. BEVIER. Well, I just would make one comment, and that is that it may very well be that no one has a legitimate complaint, and it may very well be, it's possible, I think—I certainly don't know from this hearing today, how the information is used.

But one of the things about having the Government keep information about you and use it for purposes other than the purposes for which you voluntarily gave it to them is that you often do not know what use is being made of it. And it's very hard to keep track of why sort of certain things are happening to you, why you are getting certain pieces of mail, why certain consequences are seeming to flow.

So the fact that nobody has complained may suggest, as you infer, that it is not being misused and that everyone is very—everyone's privacy is, in fact, being respected and it is being appropriately used by the people who have access to it. It may have a—it may not indicate that, and all I am suggesting is, I don't think you can infer a whole lot from the absence of complaints.

Mr. PETERSON. Well, no. But, again, my point that, you know, if you go in and actually examine the Data Base and who has passwords—you know, they have a security system where you can only get in certain levels of the system if you are at some level; it is very limited, the people that can get to that information, audit trail or no audit trail. That's part of how the system was designed. And anybody that would go down to the White House and start asking questions, you will find that out. There's a very limited amount of people. They did not use those codes, that I can see, on any kind of consistent basis.

So I mean, it's just the—my point is that a lot of this is speculation. You know, I mean, I can wonder why I was audited the day after I got the Democratic nomination to run for Congress when we had a Republican administration, and, you know—you know, it's—

Mr. MCINTOSH. We go after them, too.

Mr. PETERSON. So I mean, I think Members of Congress, you know—I mean, I have had constituents who think that because they opposed a Member of Congress that they were audited by the IRS. It may be coincidence; it may not. So, who knows? I think we just have to keep this all in perspective.

I think there are questions about this that need to be answered, but let's not get too carried away with all the speculation. That's my bottom line point.

Mr. MCINTOSH. Thank you, Mr. Peterson.

Let me just clarify one point. It's very clear that the Anti-deficiency Act and the appropriations laws apply to the White House and all of the constituent offices within the White House. Is that correct, Professor Harrison?

Mr. HARRISON. Yes.

Mr. MCINTOSH. Less clear—and this came out in talking with Professor BeVier on the Privacy Act—but my understanding, and I want to make sure for the record this is correct, that all agencies are covered by the Privacy Act. And the question comes up whether the constituent parts of the White House are an agency.

Ms. BEVIER. Right.

Mr. McINTOSH. We know from settled opinion that certain parts of the White House are considered agencies for the purpose of that act—the Office of Administration, the OMB, the National Security Agency. For other parts of the White House, it depends on their activities and functions, whether they were behaving as an agency would behave.

And so part of the question we will have to address, concerning the Privacy Act, is how this White House Data Base was used by those components that are not automatically covered by the Privacy Act.

Let me address one comment that Collin has made, because I think it is important to indicate in closing where we are headed with this investigation. This hearing today was for the purpose of laying the background. Of what is this Data Base? We saw in press reports that it was called a “big brother.” It was a huge Data Base used by the White House, had very sensitive information, including ethnic background and political affiliation. So we have asked the GAO to tell us how it was created, how it’s used, how it functions. We received an interim report from them today.

We also received a briefing on the legal questions that come to play on whether this is a legal activity for the White House and have found that there are at least two statutes, criminal statutes, that come to bear: the Anti-deficiency Act and the Privacy Act. And part of the question of whether this was legal or illegal behavior depends on the facts surrounding the use of this Data Base.

What we do not know is how the Data Base was actually used and the record of its contents, and that has been the subject of repeated requests to the White House from this subcommittee, including a letter signed by all of the majority members to the President on August 15.

Our next step will be to continue to pursue the procedures outlined in that letter to ensure that we have used every legal means to obtain that information, since it is critical to determine whether or not this activity was legal and appropriate.

After we have obtained the documents from the White House, I agree we should bring the White House officials here and let them explain what was happening in this Data Base. But in order to do that, and in order for the committee to perform its functions effectively, we must have compliance with our document requests from the White House. So it’s going to be my recommendation to Chairman Clinger that we continue to pursue every avenue possible to ensure that that happens expeditiously.

With that, I have no further questions for this panel. This subcommittee is in adjournment.

[Whereupon, at 12:40 p.m., the subcommittee was adjourned.]

