AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–653

VETERANS AFFAIRS DATA PRIVACY BREACH: TWENTY-SIX MILLION PEOPLE DESERVE ASSURANCE OF FUTURE SECURITY

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 20, 2006

Printed for the use of the Committee on Veterans' Affairs

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

29-717 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON VETERANS' AFFAIRS

LARRY E. CRAIG, Idaho, *Chairman*

ARLEN SPECTER, Pennsylvania
KAY BAILEY HUTCHISON, Texas
LINDSEY O. GRAHAM, South Carolina
RICHARD BURR, North Carolina
JOHN ENSIGN, Nevada
JOHN THUNE, South Dakota
JOHNNY ISAKSON, Georgia

DANIEL K. AKAKA, Hawaii, *Ranking Member*
JOHN D. ROCKEFELLER IV, West Virginia
JAMES M. JEFFORDS, (I) Vermont
PATTY MURRAY, Washington
BARACK OBAMA, Illinois
KEN SALAZAR, Colorado

LUPE WISSEL, *Majority Staff Director*
BILL BREW, *Minority Staff Director*

C O N T E N T S

JULY 20, 2006

SENATORS

	Page
Craig, Hon. Larry E., Chairman, U.S. Senator from Idaho	1
Letter dated July 18, 2006 from James H. Burrus, Federal Bureau of Investigation, regarding the recovered stolen records	3
Akaka, Hon. Daniel K., Ranking Member, U.S. Senator from Hawaii	4
Murray, Hon. Patty, U.S. Senator from Washington	5
Salazar, Hon. Ken, U.S. Senator from Colorado	6
Burr, Hon. Richard, U.S. Senator from North Carolina	25
Thune, Hon. John, U.S. Senator from South Dakota	28

WITNESSES

Nicholson, Hon. R. James, Secretary, Department of Veterans Affairs; accompanied by Robert Howard, Senior Advisor to the Deputy Secretary; Tim McClain, General Counsel; and Robert Henke, Assistant Secretary for Management, Department of Veterans Affairs	7
Prepared statement	10
Response to written questions submitted by Hon. Daniel K. Akaka	11
Opfer, Hon. George J., Inspector General, Department of Veterans Affairs; accompanied by Jon A. Wooditch, Deputy Inspector General; and Maureen Regan, Counselor to the Inspector General, Department of Veterans Affairs	12
Prepared statement	14
Response to written questions submitted by Hon. Daniel K. Akaka	19

APPENDIX

Newsweek article, "The Best Medical Care in the U.S."	38

VETERANS AFFAIRS DATA PRIVACY BREACH: TWENTY-SIX MILLION PEOPLE DESERVE ASSURANCE OF FUTURE SECURITY

THURSDAY, JULY 20, 2006

U.S. SENATE,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–418, Russell Senate Office Building, Hon. Larry E. Craig, Chairman of the Committee, presiding.

Present: Senators Craig, Burr, Thune, Akaka, Murray, and Salazar.

OPENING STATEMENT OF HON. LARRY E. CRAIG, CHAIRMAN, U.S. SENATOR FROM IDAHO

Chairman CRAIG. Good morning, everyone. The Senate Committee on Veterans' Affairs will come to order. I want to welcome all of you to this very important hearing. Secretary Nicholson, Inspector General Opfer, welcome, and thank you for taking the time to be with us this morning.

On May 3rd, theft of a laptop computer and external hard drive from the home of a VA employee has been reported as an embarrassing and expensive management failure of VA. While that may be true, in the 8 weeks since our joint hearing with the Homeland Security and Governmental Affairs Committee, there has been much news, both good and bad, on the issue.

We have learned that the employee was not authorized to take the data home and did not safeguard the data once he brought it home. We have learned that the appropriate people within VA were not informed of the stolen data in a timely manner. We have learned that VA policies, practices, and procedures are inadequate to safeguard personnel and proprietary information. And we have learned that VA has insufficiently address long-standing OIG-reported information security weaknesses.

We have also learned that law enforcement officials recovered the stolen data and hard drive. That is a good news indeed. And even better news is that based on computer forensics examinations, both the FBI and the OIG have a high degree of confidence that the data was not accessed or compromised after the burglary, and they foresee no reason for that assessment to change. And that is very good news for America's veterans.

However, the issue is, I believe, far from closed. This incident has had far-reaching implications. America, I believe, is watching

VA and what VA does to learn from and correct its mistakes, because the issue of data security is a problem not only across Government, but within the private sector as well. I think what happened at VA should be an awakening to all of Government. There is not a single American who does not expect and, frankly, does not deserve assurances from their Government, one of the world's largest custodians of sensitive personal information. They deserve a vigilant security program to protect that information.

So we are here today to talk about what needs to be done to improve data security and how VA intends to make that happen. How do we ensure that the policies, practices, and procedures at VA discourage the potential compromise of sensitive data? How do we prevent another wholesale failure to recognize the importance of a potential breach of security? And can VA more accurately assess the extent and scope of an incident in order to report these incidents to VA and Congressional leadership in a timely manner? And, finally, how do we leverage this enormous success that VA has had with electronic medical records to become the gold standard in information and cyber security as well? That ought to be a real and important challenge.

The solution to some of these problems may lie in more strictly enforced policies, increased education about those policies, and increased utilization of data encryption and passwords. Some would argue that the solution lies in increased legislation and appropriations. But at the heart of it all, VA must resolve its repeatedly identified vulnerabilities, establish a clear chain of command, and implement an accountability structure for the security of its information.

VA will testify today that they have an implementation strategy that is the road map to success and that they are on their way. Clearly, that puts their testimony at odds with historic patterns.

I look forward to understanding the mechanics of this road map, so much so, in fact, that I will take this opportunity to post my first question of the hearing. Is this implementation strategy something which every single VA employee understands? Can I have a chat with the systems administrator at the Boise VA about the implementation strategy for securing VA information or perhaps even a claims supervisor at that same facility? Even bigger than the challenge of finding lost data is the challenge of making the security of those in the VA system everyone's top priority.

I hope this hearing, like the one we held 2 months ago, will shed some more light on the situation, provide clarity to some of my concerns and the Committee's concerns—I think we hold this jointly—and, most importantly, provide 26 million veterans with answers they deserve.

Before I turn to the Ranking Member, I would like to bring to the Committee's attention the July 18, 2006, letter from the FBI reiterating its high degree of confidence that the files on the external hard drive where the VA data was stored was not compromised. This letter will be made a part of the hearing record today.

[The letter from James H. Burrus, Jr., Federal Bureau of Investigation (FBI) follows:]

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 18, 2006

Honorable Larry E. Craig
Chairman
Committee on Veterans' Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

By letter dated July 14, 2006, you invited our Director, Robert S. Mueller, to testify at a hearing of the Senate Committee on Veterans' Affairs regarding information security practices at the Department of Veterans Affairs (VA).

Inasmuch as the FBI's investigation is ongoing relative to the theft of VA data, it would be inappropriate for the FBI to provide testimony at this time. However, the FBI is aware of the continued concern related to the possible compromise of VA data. On June 28, 2006, the stolen VA employee laptop computer and external hard drive were recovered intact. Based on all of the facts gathered thus far during the investigation, as well as on the results of separate computer forensics examinations by the FBI and VA, Office of the Inspector General (VA OIG), the FBI and VA OIG are highly confident that the files on the external hard drive, where the VA data was stored, were not compromised.

Based on the above, I hope this letter addresses the committee's concerns and questions. Thank you for your patience as the FBI continues to investigate this important matter in conjunction with local law enforcement, the VA OIG, and the Department of Justice.

Sincerely,

James H. Burrus, Jr.
Acting Assistant Director
Criminal Investigative Division

Chairman CRAIG. Also, before I turn to our Ranking Member and other Members for their comments, I want to recognize Tim McClain, our VA General Counsel who is with us today. Tim is leaving us September 1 to join the private sector. He has been an integral part of VA's senior leadership team as the chief legal counsel since 2001. He was in the Navy's Judge Advocate General Corps and retired from active duty in 1990. He has been the point person to handle crises such as Hurricanes Katrina and Rita. His tireless leadership in support of the Secretary and the VA in addressing the data issues has been key.

Tim, on behalf of the Committee, I want to thank you for your service to VA, to America's veterans, and thank you for your service to the country.

Mr. MCCLAIN. Thank you, Mr. Chairman.

Chairman CRAIG. Thank you very much.

[Applause.]

Chairman CRAIG. Now let me turn to the Ranking Member of the Committee, Senator Danny Akaka.

Danny.

STATEMENT OF HON. DANIEL K. AKAKA, RANKING MEMBER, U.S. SENATOR FROM HAWAII

Senator AKAKA. Thank you. Thank you very much, Mr. Chairman. And I want to take this opportunity to wish my brother well. Chairman Craig, happy birthday.

Chairman CRAIG. Thank you.

[Laughter.]

Chairman CRAIG. Well, it will depend on how the hearing goes today how my birthday is, Mr. Secretary.

[Laughter.]

Chairman CRAIG. Please proceed, Danny.

Senator AKAKA. Mr. Chairman, thank you very much for calling this hearing. It is important. I am with you and with the Committee in trying to assure that we can improve data security for the Veterans' Administration.

I want to welcome Secretary Nicholson and Mr. Opfer in joining us today, and I look forward to their testimony.

I know there was a collective sigh of relief when the computer equipment containing the stolen data was recovered. It was great news to learn that the FBI reached the conclusion that it is highly unlikely that the data was compromised. Mr. Opfer, I thank you and your office for aggressively pursuing this investigation and the timeliness with which you completed it. Your hard work has provided the Secretary and us with recommendations that should go a long way toward fixing VA's information security problems.

I note that the President's budget for the coming fiscal year calls for a serious cut of funding and staff for your office. Yet your office's response to this incident shows that VA needs more oversight of its internal workings and not less.

It should not have taken the loss of personal information affecting 26.5 million veterans, guardsmen, reservists, and active-duty servicemembers, nor the expenditure of millions of dollars for me to realize that VA needs to take drastic steps to improve its cyber and information security.

For the past 6 years, VA's IG has reported that information technology security is a major management challenge. VA has also received failing grades from its Federal Information Security Management Act audits. It should not have taken almost 2 weeks for the Secretary to learn of a problem of this magnitude. The slow reaction which characterized the Department's response to the theft is unacceptable. I am very concerned about the state of VA's internal organization and how the Department functions.

As VA recovers from this incident, it must have information of security policies, procedures, and practices that are standardized for all of its employees. I remain distressed that the removal of data was not a violation of any law or regulation.

As I noted at our Committee's hearing on the data loss, the incident that brings us here today could have easily involved other Government departments and agencies. VA must establish safeguards to prevent any loss of data in the future. Secretary Nicholson, I hope you will be proactive in your efforts to remedy these problems. Veterans have entrusted the Department with their personal information and deserve nothing less, and I know you will certainly be working on it, and this Committee will be interested in how we do that.

Mr. Chairman, I will continue to work with you to ensure that we provide effective oversight of VA's remediation plan. I look forward to hearing from our witnesses and hearing their testimony this morning.

Thank you very much, Mr. Chairman.

Chairman CRAIG. Senator Akaka, thank you very much.

Now let us turn to Senator Patty Murray.

Patty.

STATEMENT OF HON. PATTY MURRAY, U.S. SENATOR FROM WASHINGTON

Senator MURRAY. Well, thank you very much, Mr. Chairman, and happy birthday. I hope it is a good one as well.

Chairman CRAIG. Thank you.

Senator MURRAY. Thank you, Senator Akaka, especially, too, for holding this hearing, and welcome to Secretary Nicholson and the Inspector General.

I know that Chairman Craig and Senator Akaka share my concerns about the recent data theft and how it has been handled, and we all gave a sigh of relief when obviously the data was found. But I was very frustrated to hear that the VA was not going to be providing the credit monitoring to veterans whose credit may be at risk, and I read the letter from the FBI and know that they say it is a high level of certainty that the data was not accessed. But, frankly, I would not bet my credit on it. And, more importantly, because the VA still does not have an adequate security system, I really think until that is fixed, the VA should keep its commitment to providing veterans with the credit monitoring, and I hope that we can change that direction and move forward on that. I will ask you about that later.

I also share the concern of the Chairman and the Ranking Member about the past failures with data security. We know that the IG has warned time and time again that the systems were not se-

cure about the lack of protection for this vital, sensitive information about health care and benefits. And these are really institutional problems within the VA, and it is going to take more than just words about it. We are going to have to really hear some very concrete plans, and I hope to ask questions about that at this morning's hearing. And I appreciate your being here so we can really get to the heart of why this investigation took so long to begin, and what changes have been made and what the future plans are to make sure that this problem does not happen again.

Mr. Secretary, as we talked about when you came in, I hope that we can also take a few minutes to talk about your recent trip to Walla Walla 2 weeks ago when you came through my State on a series of campaign stops and stopped in Walla Walla. You made an announcement—actually both in Northwest Washington about a Northwest Washington CBOC and the Walla Walla hospital. And as you know, your visit to our State raised more questions than it answered, and I hope that I can have the opportunity to really define what some of that meant, because I know the people in Walla Walla. They are committed; their community is committed; the business community is committed; the veterans community is committed. They have really worked hard to have a seat at the table and want to know what the details are because that is really what matters.

I did send you a letter. I got an answer to it last night, but I still feel that there are a number of questions that are unanswered, and I hope to get those answers today as well.

So thank you, Mr. Chairman.

Chairman CRAIG. Patty, thank you very much.

Now let's turn to Senator Ken Salazar.

Ken.

STATEMENT OF HON. KEN SALAZAR, U.S. SENATOR FROM COLORADO

Senator SALAZAR. Thank you very much, Mr. Chairman, and happy birthday to you.

Chairman CRAIG. Thank you.

Senator SALAZAR. And thank you, Senator Akaka, for holding this hearing.

I also want to thank Tim McClain for the service that he has performed for the VA, and I have very much enjoyed working with him. Sometimes I think when we come to these hearings, it seems that we get into combat, if you will, with the VA on issues that are of concern to Members of this Committee. But I think it is also important, from time to time, to remember that there is a lot of good that goes on with the VA.

I had a long conversation with Under Secretary Perlin yesterday about the latest article in Business Week, and I think it demonstrates that there is a lot of good in the VA. And I think that has come about through the joint efforts of this Committee and the Congress working closely with the VA.

I am very appreciative of the fact that we are looking at the issue of security breaches at the VA. We all breathed a very deep sigh of relief when the FBI recovered the computer. We were all very, very lucky on that incident, but I think the central question

still remains. It was a very troubling incident. I know that Secretary Nicholson shares that concern, and I am very hopeful that today we will hear more from Secretary Nicholson about how we make sure that this problem does not occur again. It has always been my view when these major mistakes occur and people's lives are affected that what we have to do is make sure that you prevent the problem from ever happening again. And I am hopeful that the ideas and policy directions that Secretary Nicholson is taking in the Department will address these issues effectively.

Thank you, Mr. Chairman.

Chairman CRAIG. Ken, thank you very much.

Before I turn to the Secretary, let me thank you all for your kind wishes. In the aging process, there is also some humor, and it happened yesterday. We were in the Speaker's meeting room prior to the final ceremony on the 75th anniversary of the VA in the Rotunda. There was a gentleman there from Maryland who is 104 years old. He fought in World War I. He enlisted when he was 16 years old to serve in the Navy and is in just amazingly good shape, but he could not hear very well. And when I bent over to say hello to him, he looked up at me, and he said, "And you fought in World War II." And I had to remind him that I was not yet born.

[Laughter.]

Chairman CRAIG. So that is part of the positive side of this memory as we work through the aging process.

Anyway, with that, Mr. Secretary, thank you again for coming before the Committee. You have heard our Members' concern about the good news and the bad news and where we go from here. And I think that is going to be what this Committee focuses on now and into the future as we work with VA to get this right and prevent this problem from happening again.

Please proceed.

STATEMENT OF HON. R. JAMES NICHOLSON, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY ROBERT HOWARD, SENIOR ADVISOR TO THE DEPUTY SECRETARY; TIM McCLAIN, GENERAL COUNSEL; AND ROBERT HENKE, ASSISTANT SECRETARY FOR MANAGEMENT, DEPARTMENT OF VETERANS AFFAIRS

Secretary NICHOLSON. Well, thank you, Mr. Chairman, and let me add my greetings and happy birthday to you. I recall that incident yesterday slightly differently, however. He asked you if you fought in World War I.

[Laughter.]

Chairman CRAIG. Yes, I know.

[Laughter.]

Chairman CRAIG. Something about both—I did not want to suggest that his ears were failing and his eyes were failing.

Secretary NICHOLSON. I appreciate being here before you and the Members of the Committee to follow up on what has occurred with the Department of Veterans Affairs since the unfortunate theft of data from the home of a VA employee on May 3rd. I appeared before you at a hearing on May 25th to tell you what I knew about this situation at that time. Since then much has happened and, as you know and have noted, on Thursday, June 29, 2006, I an-

nounced that Federal law enforcement authorities had recovered the stolen laptop and external hard drive.

The FBI's forensic examination of the recovered laptop and hard drive is complete, and the FBI has a high degree of confidence, based on the results of the forensic tests, and other circumstantial information gathered during the investigation that the data contained in that equipment was not accessed or compromised in any way.

This is good news for the VA, most importantly for our veterans and our active-duty military personnel, and we believe should alleviate the concerns that they may have. But it is important that we remain vigilant. And for that reason, we will be retaining the services of a company that specializes in data breach analysis to monitor this situation.

I know that the Members of this Committee have digested the VA Inspector General's report on events related to the data breach. That report is accurate, and it is harshly critical of the situation that has existed at the VA for years where we simply did not have in place proper procedures, regulations, guidelines, and directives. Nor did we have a culture of data security that should have precluded an occurrence like this. And once the event occurred, we did not show sufficient urgency in dealing with it. As you know, I was not informed of the theft until nearly 2 weeks after it had occurred.

So I concur with the recommendations contained in the Inspector General's report and am fully committed to seeing them implemented in the shortest possible time line. Last October, I approved a major restructuring of information security within the Department—far, far before this incident occurred and reached the light of day. This restructuring ordered the centralizing of almost all of the information technology within the Department to come under the Chief Information Officer. This process was and, of course, still is underway and will greatly facilitate control, training, responsibility, and accountability. This consolidation of IT has been accelerated as a result of this incident.

There have been several changes that have already been implemented, and as we continue this effort, we can make the VA the "Gold Standard" in the area of information security, just as we have done in the area of electronic medical records. The VA is the recognized leader in electronic health records, and I appreciate that being noted in the recent article in Business Week. VA is also the recognized leader in health safety and is setting the standards for others to follow. I am committed to doing the same in the area of information security.

We have developed a plan with corrective actions and execution time lines necessary to fix the deficiencies cited in the IG report. It is a multi-phased effort which includes actions in the technical area, such as encryption processes and tools, actions in the management area, such as a complete overhaul of policies and directives, and actions focused on operational area, such as procedures and tools for monitoring the extraction of sensitive information.

We will, of course, be pleased to brief the Committee in greater detail on that at your convenience.

On June 28, 2006, I issued a memorandum delegating to the VA Chief Information Officer all authority and responsibilities given to

me by the Federal Information Security Management Act, or FISMA. This delegation does not relieve me of the ultimate responsibility, but it does empower the CIO with the authority he needs to do his job.

This delegation restructures responsibilities and authorities for information security at the VA, bringing them together in one individual. It also is the first step in bringing about the cultural changes within the VA generally, and more particularly, within the arena of information technology. That must occur. I have made it clear to all senior managers in the Department that information security, cyber security, and the reorganization of the Office of Information Technology are top priorities. These senior leaders know that every employee must be committed to ensure the safety of veterans' personal information. Performance evaluations and executive bonuses will reflect the leaders' and employees' level of commitment.

When I commit to becoming the "Gold Standard," I mean VA must be the best in the Federal Government in protecting personal and health information, training and educating our employees to achieve that goal. The culture must put the custody of veterans' personal information first—over and above expediency. And I expect nothing less.

The IG report has highlighted serious deficiencies. We have a plan for transformation. I realize, however, the recommendations contained in this report are just a start. Achieving our goal of leadership will require much more.

I have reached outside our ranks and enlisted the assistance of leading experts in the field of data security to assist us in defining our path. With their guidance and VA resources, we will become the system for all other agencies to emulate.

Training in the area of information and cyber security will be a vital component of our transformation. To ensure quality and consistency in such a broad-based training program, I have directed the establishment of a new Office of Cyber and Information Security Training within the Office of Information Technology.

This office will be responsible for developing and implementing a training program which will begin with new employee orientation and continue through such programs as Leadership VA, the Senior Executive Service Candidate Development Program, and the Senior Leadership Academy. I expect a continual emphasis on information security throughout an employee's career.

Excellence in information security will take the full commitment of VA's senior leadership, both political appointees and career senior executives. It will also take money, and we will seek the budgetary resources we need for success from the Administration and from you, the Congress. And it will take time, but my sense of urgency is clear.

Measurable progress will require a steady and consistent message for—and from—all who work for this agency.

Industry experts will help our own IT professionals develop program changes and validate our time lines. Employees will be held accountable for safeguarding the sensitive information entrusted to us by veterans and other beneficiaries. Even now we are conducting an inventory to determine appropriate access needs for ev-

eryone within VA. And we will be instituting background checks appropriate to those access levels.

In fact, it is our people that will make all of this happen. There is nothing more important than having people with training and character to assume the responsibility to implement the changes needed.

Mr. Chairman, unfortunately a very bad thing happened. A monumentally awful thing, and I am outraged by it and by the slow response of some in our Department. But I am the responsible person, and it is to me that you are entitled to look to see that this is fixed. It will not be easy, and it will not be overnight. But I am absolutely convinced that we can do it. As I have said, I think we can turn the VA into the model for information security, just as it has become the model for health care in the United States.

Finally, Mr. Chairman, thank you for your kind words for Tim McClain. We wish him well and will miss him.

That concludes my testimony, and I would be pleased to answer any questions the Committee may have.

[The prepared statement of Secretary Nicholson follows:]

PREPARED STATEMENT OF HON. R. JAMES NICHOLSON, SECRETARY, DEPARTMENT OF VETERANS AFFAIRS

Mr. Chairman and Members of the Committee.

Thank you for the opportunity to appear before you to follow up on what occurred within the Department of Veterans Affairs since the unfortunate theft of computer equipment containing VA data from the home of a VA employee on May 3rd. I appeared before you at a hearing on May 25th to tell you of what I knew about this situation at that time. Since then, much has happened.

On Thursday, June 29, 2006, I announced that Federal law enforcement authorities had recovered the stolen laptop and external hard drive. The FBI's forensic examination of the recovered laptop and hard drive is complete. The FBI has a high degree of confidence—based on the results of the forensic tests and other information gathered during the investigation that the data contained on that equipment was not accessed or compromised.

This is good news for our veterans and active duty military personnel and should alleviate any concerns they may have. But, identity theft is the fastest growing white-collar crime in this country, and it is important that we remain vigilant. For that reason, we will be retaining the services of a company that specializes in data breach analysis to monitor this situation.

I know the Members of this Committee have digested the VA Inspector General's report on events related to the data breach.

I concur with the recommendations contained in the Inspector General's report, and am fully committed to seeing them implemented in the shortest possible time. Last October I approved a major restructuring of information security within the Department, centralizing almost all of it under the Chief Information Officer. This process was, and of course, still is underway and will greatly facilitate control, training, responsibility and accountability. This consolidation of IT has been accelerated as a result of this incident. There have been several changes that have already been implemented, and, as we continue this effort, we can make VA the "Gold Standard" in the area of information security. VA has made great strides forward in the area of health care and today is the recognized leader in health records and safety and is setting the standards for others to follow. I am committed to doing the same in the area of information security.

We are formulating an action plan that is a multi-phased effort which includes actions in the technical area such as encryption processes and tools; actions in the management area such as a complete overhaul of policies and directives; and actions focused on operational areas such as procedures and tools for monitoring the extraction of sensitive information.

On June 28, 2006, I issued a memorandum delegating to the VA Chief Information Officer (CIO) all authority and responsibilities given to me by the Federal Information Security Management Act (FISMA.) This delegation does not relieve me of

the ultimate responsibility but it does empower the CIO with the authority he needs.

This delegation restructures responsibilities and authorities for information security at the VA, bringing them together in one individual. It also is the first step in bringing about the cultural changes within VA generally, and more particularly, within IT at VA, that must occur. I have made it clear to all senior managers in the Department that information security, cyber security and the reorganization of the Office of Information Technology (OIT) are top priorities. These senior leaders know that every employee must be committed to ensure the security of veterans' personal information. Performance evaluations and executive bonuses will reflect the leaders' and employees' level of commitment.

When I commit to becoming the "Gold Standard," I mean VA must be the best in the Federal Government in protecting personal and health information, training and educating our employees to achieve that goal. The culture must put the custody of veterans' personal information first . . . over and above expediency. I expect nothing less.

The IG Report has highlighted serious deficiencies. We have a plan for transformation. I realize, however, the recommendations contained in this report are just a start. Achieving our goal of leadership will require much more.

I have reached outside our ranks and enlisted the assistance of leading experts in the field of data security to assist us in defining our path. With their guidance and VA resources, we will become the system for all other agencies to emulate.

Training in the area of information and cyber security will be a vital component of our transformation. To ensure quality and consistency in such a broad-based training program, I have directed the establishment of a new Office of Cyber & Information Security Training within the Office of Information Technology.

This office will be responsible for developing and implementing a training program which will begin with new employee orientation and continue through such programs as Leadership VA, the SES Candidate Development Program and the Senior Leadership Academy. I expect a continual emphasis on information security throughout an employee's career.

Excellence in information security will take the full commitment of VA's senior leadership, both political appointees and career senior executives. It will take time, but my sense of urgency is clear.

Measurable progress will require a steady and consistent message for—and from—all who work for this agency.

Industry experts will help our own IT professionals develop program changes and validate our time lines. Employees will be held accountable for safeguarding the sensitive information entrusted to us by veterans and beneficiaries. Even now we are conducting an inventory to determine appropriate access needs for everyone within VA. And we will be instituting background checks appropriate to those access levels.

In fact, it is our people that will make all of this happen. There is nothing more important than having people with training and character, who assume the responsibility to implement the changes needed.

Mr. Chairman, unfortunately a very bad thing happened. A monumentally awful thing. I am outraged by it and the slow response of some of our Department. But I am the responsible person, and it is to me that you are entitled to look to see that this is fixed. It won't be easy, and it won't be overnight, but I am absolutely convinced that we can do it. As I've said, I think we can turn VA into the model for information security, just as it has become the model for health care in the United States, as most recently attested to in an article in Business Week magazine dated July 17th.

Mr. Chairman, that concludes my testimony. I would be pleased to answer any questions that the Committee may have.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. AKAKA TO HON. R. JAMES NICHOLSON

Question 1. Based on the FBI's findings that it is unlikely that the data on the hard drive was compromised, VA has withdrawn its plan for providing free credit monitoring for those whose personal information was on the stolen equipment. VA has stated it will continue with a contract for data breach analysis. Please detail when the contract will start and exactly what services will be contracting for.

Answer. Failed to respond within allotted time.

Question 2. As a result of the data breach analysis contract, if a breach is identified concerning a veteran's credit or identity, does VA intend to then provide credit monitoring to that veteran? What is VA's response plan?

Answer. Failed to respond within allotted time.

Question 3. The IG report identified thirteen different memorandums and directives that have been issued in response to the data theft. The report stated they found a patchwork of policies pertaining to information security that were fragmented and difficult to locate. What is VA doing to standardize and simplify the policies and procedures that pertain to protecting personal and proprietary data so that they are clearly understood by all VA employees and contractors?

Answer. Failed to respond within allotted time.

Question 4. The IG recommended that the Secretary take "whatever administrative action" deemed appropriate in connection with individuals involved in "the inappropriate and untimely handling of the notification of stolen VA data." In your response to IG, you indicated that you had directed administrative investigations for some employees and for some political appointees on your immediate staff. Please explain about the administrative investigations—who is carrying them out, how they are being conducted, and what the current status is of their progress? With respect to those on your immediate staff, what is the timetable for the completion of these reviews?

Answer. Failed to respond within allotted time.

Question 5. The IG identified that there is a problem with position level designations not being done or being inaccurate for VA and contract employees. They also identified a problem of background checks for those with access to sensitive data. Please explain the size of the problem, how long it will take to fix it, and how much it will cost.

Answer. Failed to respond within allotted time.

Question 6. How long does VA intend on maintaining the call centers to answer data theft questions from veterans and their families?

Answer. Failed to respond within allotted time.

Chairman CRAIG. Mr. Secretary, thank you very much for that testimony.

Now let us turn to the Honorable George Opfer, Inspector General, Department of Veterans Affairs. George, welcome to the Committee.

STATEMENT OF HON. GEORGE J. OPFER, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY JON A. WOODITCH, DEPUTY INSPECTOR GENERAL; AND MAUREEN REGAN, COUNSELOR TO THE INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS

Mr. OPFER. Thank you, Mr. Chairman and Members of the Committee. Thank you for the opportunity to testify on the results of our reviews of the issues related to the loss of VA information concerning the identity of millions of veterans.

As you know, on May 3rd, the home of a VA employee was burglarized resulting in the theft of approximately 26.5 million personal identification information on veterans and active-duty military personnel. The Secretary was not informed until May 16th. Congress and the veterans were not informed until May 22nd. Since then, this Committee, as well as other committees and Members of Congress, have expressed considerable interest in the incident involving the theft and loss of the data.

When I testified before this Committee on May 25th, I described the OIG approach as three-pronged: An ongoing criminal investigation which is still continuing regarding the theft of the data; an administrative investigation into the handling of the incident once it was reported to VA; and a review of the policies and procedures in VA regarding information security and the process that was used to try to safeguard data.

I am pleased to acknowledge that through the diligent and coordinated efforts of the VA OIG, the FBI, and the Montgomery County police, the stolen data was successfully recovered on June 28th. Based on the facts that we have gathered during this criminal investigation and the computer forensics examinations, we are highly confident that the data has not been compromised.

My July 11th report addresses whether or not the employee had authorization to access the data, take the data home, whether management responded appropriately to the reported theft, and whether VA policies and procedures were adequate to protect the VA information. The report also discusses long-standing information security weaknesses in VA.

Because this employee was responsible for projects involving all aspects of VA, he was authorized to have access to VA databases. However, at the time of the burglary, his supervisors were not aware that he had taken the data home or was working on a self-initiated project. In addition, this data was not password-protected or encrypted in any way. Although a senior manager in the Office of Policy, Planning, and Preparedness was informed of the possible loss of VA data on May 3rd, it was not communicated up the chain of command to the Chief of Staff until May 9th. This is 6 days after the incident had been reported. Poor communication, partially resulting from a dysfunctional working relationship among senior executives, contributed to this delay. The lack of urgency was also impacted by a false assumption that other parts of VA had the responsibility to investigate and report this incident and make the required notifications.

On May 10th, a day after learning of the incident, the Chief of Staff requested legal advice from the General Counsel's office. He decided to wait for that legal advice before notifying the Secretary. Yet during the 6 days that transpired afterwards, there was no follow-up to determine the status of that request. The Chief of Staff notified the Deputy Secretary on May 10th, and he, too, decided not to notify the Secretary until more information was gathered.

The information security officials with responsibility for receiving, assessing, or notifying higher level officials of the data loss reacted with indifference and little sense of urgency. Efforts to investigate the matter were further impeded by errors and omissions in the original incident report.

Twelve days after receiving the incident report, no meaningful progress was made in determining the magnitude of the event. Coincidentally, the incident ended up being referred back down to the individual who originally referred it in the first place.

We were able to determine in the OIG after one interview with the employee the significance of the stolen data. I immediately notified the Chief of Staff on May 16th. The Chief of Staff notified the Secretary shortly after my call. It is unexplainable to us from the period of May 3rd through the 16th why no one in the chain of command reinterviewed the employee to determine the extent of the damage of the potential data loss.

VA policies and procedures were not adequate in preventing the loss. We found that employees were not sufficiently trained, required background checks were not performed, contracts needed

better safeguards to protect data, and incident-reporting procedures needed improvement.

Since the incident, the Secretary has taken many positive steps toward strengthening the policies to prevent similar disclosures. We have made additional recommendations to the Secretary. Our report covers many recommendations aimed at taking appropriate administrative action and establishing an effective, comprehensive policy that will safeguard protected information.

The Secretary has agreed with our findings and recommendations in the report and has provided an acceptable improvement plan.

In closing, I would like to assure the Committee that we will follow up on the implementation of all these recommendations until they are fully completed. Mr. Chairman and distinguished Members of the Committee, thank you again for the opportunity to appear, and I would be pleased to answer any questions.

[The prepared statement of Mr. Opfer follows:]

PREPARED STATEMENT OF HON. GEORGE J. OPFER, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS

INTRODUCTION

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on the results of the Office of Inspector General (OIG), Department of Veterans Affairs (VA), review of issues related to the loss of VA information involving the identity of millions of veterans. I am accompanied by Jon Wooditch, Deputy Inspector General, and Maureen Regan, Counselor to Inspector General.

As you know, on May 3, 2006, the home of a VA employee was burglarized resulting in the theft of a personally owned laptop computer and an external hard drive, which was reported to contain personal information on approximately 26 million veterans and U.S. military personnel. The VA Secretary was not informed of the incident until May 16, 2006, almost 2 weeks after the data was stolen. The Congress and veterans were notified on May 22, 2006. Since then, the Senate Veterans' Affairs Committee, as well as other Congressional committees and Members of Congress, have expressed considerable interest in how this incident occurred and in how VA management responded after being notified of the loss of data.

When I testified before this Committee on May 25, 2006, I described the OIG's involvement as a three-pronged approach including: (1) a criminal investigation, (2) an administrative investigation of the handling of the incident once reported to VA, and (3) a review of VA policies and procedures for using and safeguarding personal and proprietary data. I am pleased to announce that we completed the administrative investigation and the review of policies and procedures, and issued our final report on July 11, 2006.

More importantly, I am also pleased to acknowledge that through the diligent and coordinated efforts of the VA OIG, the Federal Bureau of Investigation, and the Montgomery County Police Department in Maryland, the stolen data was successfully recovered on June 28, 2006. Based on all the facts gathered thus far during the criminal investigation, as well as the results of computer forensics examinations, we are highly confident that the data was not compromised after the burglary. I would also like to point out that we are continuing to pursue the criminal investigation into the burglary.

The July 11, 2006, report essentially addresses whether the employee had authorization to access and take the data home, whether management responded appropriately to the incident, and whether VA policies and procedures were adequate to protect information. The report also discusses long-standing information security weaknesses in VA, even though OIG reports have repeatedly made recommendations for corrective action.

EMPLOYEE NOT AUTHORIZED TO TAKE DATA HOME

Because the employee was responsible for planning and designing analytical projects and supporting surveys involving all aspects of VA policies and programs, he was authorized access to, and use of, VA databases. The employee explained that much of the data that he had stored on the stolen external hard drive was for his

"fascination project" that he self-initiated and worked on at home during his own time. Because of past criticism on the reliability of the National Survey of Veterans, his project focused on identifying approximately 7,000 veterans who participated in the 2001 survey, in order to compare the accuracy of their responses with information VA already had on file. He began the project in 2003, but could not recall spending time working on it during 2006.

To conduct this project, the employee took home vast amounts of VA data and loaded it on an external hard drive. The stolen laptop did not contain VA data. The employee reported that the external hard drive that was stolen likely included large record extracts from the Beneficiary Identification and Records Locator Subsystem that contained records on approximately 26 million living veterans. The extract contained veterans' social security numbers, names, birth dates, service numbers, and combined degree of disability. He also reported that the stolen hard drive likely contained an extract of the Compensation and Pension file, containing personal identifiers of over 2.8 million living veterans.

While the employee had authorization to access and use large VA databases containing veterans' personal identifiers in the performance of his official duties, his supervisors and managers were not aware that he was working on the project, and acknowledged that if they had, they would not have authorized him to take such large amounts of VA data home. By storing the files on his personal external hard drive and leaving it unattended, the employee failed to properly safeguard the data. While the employee stored the laptop and the external hard drive in separate areas of the house, he acknowledged that he took security of the data for granted.

The loss of VA data was possible because the employee used extremely poor judgment when he decided to take personal information pertaining to millions of veterans out of the office and store it in his house, without encrypting or password-protecting the data. This serious error in judgment is one for which the employee is personally accountable. The Department proposed administrative action prior to issuance of our report.

MANAGEMENT RESPONSE TO THE INCIDENT WAS NOT APPROPRIATE OR TIMELY

The burglary was reported to the local police on May 3, 2006. When the employee discovered that the computer equipment was among the items stolen, he immediately notified VA management in the Office of Policy, Planning, and Preparedness (OPP&P), including Security and Law Enforcement personnel, that the stolen computer equipment contained VA data.

Mr. Michael McLendon, Deputy Assistant Secretary for Policy, was one of the managers notified on May 3, 2006. However, it was not until May 5, 2006, that the Information Security Officer (ISO) for OPP&P interviewed the employee to determine more facts about the loss. The ISO reported that the employee was so flustered that the ISO decided not to discuss the matter; rather he asked the employee to write down what data was lost. The employee's written account of the lost data was an identification of database extracts with little quantified information concerning the significance or magnitude of the incident. This is important because this report served as the basis for all further notifications in VA up to, and including, the Deputy Secretary.

Mr. McLendon received the report of the stolen data on May 5, 2006. Instead of providing the report to higher management, Mr. McLendon advised his supervisor, Mr. Dennis Duffy, Acting Assistant Secretary for Policy, Planning, and Preparedness, of his intent to rewrite the report because it was inadequate and did not appropriately address the event. He submitted his revised report to Mr. Duffy on May 8, 2006.

Our review of Mr. McLendon's revisions determined that his changes were an attempt to mitigate the risk of misuse of the stolen data. He focused on adding information that most of the critical data was stored in files protected by a statistical software program, making it difficult to access. This, however, was not the case because we were able to display and print portions of the formatted data without using the software program. Mr. McLendon made these revisions without consulting with the programming expert on his staff or with the employee who reported the stolen data. Mr. Duffy provided the revised report to Mr. Thomas Bowman, VA Chief of Staff, on May 10, 2006. Mr. Duffy also did not attempt to determine the magnitude of the stolen data nor did he talk to the employee.

Mr. McLendon also did not inform his direct supervisor, Mr. Duffy, when he learned of the incident on May 3, 2006. Mr. Duffy advised us that he did not learn of the theft until Friday morning, May 5, 2006, when he spoke with the OPP&P ISO, in what Mr. Duffy described as a rather "casual hallway meeting."

Mr. Duffy did not discuss the matter initially with Mr. McLendon, noting that there had been a long and very strained relationship with him. Mr. Duffy said that Mr. McLendon had a very strong belief that, as a political appointee, he reported in some fashion to the Secretary and that there was no need for a "careerist" to supervise him. Mr. McLendon characterized the office as one of the most dysfunctional organizations in VA, and that it was one of the most hostile work environments he ever worked in.

Mr. Duffy said he just did not perceive this as a crisis. In hindsight, he added that his greatest regret is that he "failed to recognize the magnitude of the whole thing." Both Mr. Duffy and Mr. McLendon bear responsibility for the impact that their strained relationship, which both acknowledged, may have had on the operations of the office in handling this incident.

We also concluded that Mr. John Baffa, Deputy Assistant Secretary for Security and Law Enforcement, who was notified of the incident on May 4, 2006, also failed to take appropriate action to determine the magnitude and significance of the stolen data.

Shortly after Mr. Bowman received the report from Mr. Duffy on May 10, 2006, he provided it to Mr. Jack Thompson, Deputy General Counsel, and asked him to provide legal advice on the agency's duties and responsibilities to notify individuals whose identifying information was compromised. On May 10, 2006, Mr. Bowman also informed Mr. Gordon Mansfield, Deputy Secretary. While the Deputy Secretary does not recall discussing the magnitude of the number of veterans affected by the theft, he too decided not to raise the issue to the Secretary until they knew more information on what VA's legal responsibilities were and more about the magnitude of the problem. Once again, no attempt was made to contact the employee who reported the theft to determine the magnitude of the stolen data.

The OIG was able to determine the extent of the stolen data after one interview with the employee on May 15, 2006. As soon as I learned of the magnitude of the incident on the morning of May 16, 2006, I immediately notified the Chief of Staff that the stolen data most likely contained personal identifiers on approximately 26 million records. The Chief of Staff then notified the Secretary.

The delay in notifying the Secretary was spent waiting for legal advice from the Office of General Counsel (OGC). This 6-day delay can be attributed to a lack of urgency on the part of those requesting this advice and those responsible for providing the response. This is not to say that everyone who was notified of the incident failed to recognize its importance, but no one clearly identified it as a high priority item and no one followed up on the status of the request until after I notified the Chief of Staff on May 16, 2006.

INFORMATION SECURITY OFFICIALS ACTED WITH INDIFFERENCE AND LITTLE SENSE OF URGENCY

On May 5, 2006, the OPP&P ISO forwarded information concerning the theft to the District ISO, who is responsible for coordinating ISO activities among VA Central Office staff offices. He also submitted it to the Security Operations Center (SOC), which has responsibility for assessing and resolving reported information security incidents. However, the OPP&P ISO's incident report had significant errors and omissions, and information security officials did not adequately attempt to identify the magnitude of the incident or elevate it until May 16, 2006.

At nearly every step, VA information security officials with responsibility for receiving, assessing, investigating, or notifying higher level officials of the data loss reacted with indifference and little sense of urgency or responsibility. At no time did the District ISO or SOC attempt to interview the employee who reported the data stolen to clarify omissions in the OPP&P ISO's report or to gain a better understanding of the scope and severity of the potential data loss. While the District ISO elevated the matter to Mr. Johnny Davis, Acting Associate Deputy Assistant Secretary for Cyber Security Operations, this occurred as another "hallway conversation," and he was not provided any details on the nature of the missing data. No further notifications were made up the chain-of-command.

Twelve days after receiving the original incident report, the SOC had made no meaningful progress in assessing the magnitude of the event and, ironically, had passed responsibility to gather information on the incident back to the OPP&P ISO to review it as a possible privacy violation, an area outside the jurisdiction of the SOC. The OPP&P ISO also serves as the Privacy Officer (PO).

POLICIES AND PROCEDURES DID NOT ADEQUATELY SAFEGUARD PROTECTED INFORMATION

The potential disclosure of Privacy Act protected information resulting from the theft raised the issue of whether VA policies adequately safeguard information that is not stored on a VA automated system. Based on our review of VA policies that existed at the time of the incident; policies that have been issued since the incident; and interviews with VA employees, Chief Information Officers, POs, and ISOs; we concluded that VA policies, procedures, and practices do not adequately safeguard personal or proprietary information used by VA employees and contractors.

We found a patchwork of policies that were difficult to locate and fragmented. None of the policies prohibited the removal of protected information from the worksite or storing protected information on a personally owned computer, and did not provide safeguards for electronic data stored on portable media or a personal computer.

The loss of protected information not stored on a VA automated system highlighted a gap between VA policies implementing information laws and those implementing information security laws. We found that policies implementing information laws focus on identifying what information is to be protected and the conditions for disclosure; whereas, policies implementing information security laws focus on protecting VA automated systems from unauthorized intrusions and viruses. As a result, VA did not have policies in place at the time of the incident to safeguard protected information not stored on a VA automated system.

Although policies implemented by the Secretary since the incident are a positive step, we determined that more needs to be done to ensure protected information is adequately safeguarded. We found that VA's mandatory Cyber Security and Privacy Awareness training are not sufficient to ensure that VA and contract employees are familiar with the applicable laws, regulations, and policies. We also found that position sensitivity levels designations for VA and contract employees are either not done or are not accurate. In addition, we found that VA contracts do not contain terms and conditions to adequately safeguard protected information provided to contractors.

We determined that VA needs to enhance its policies for identifying and reporting incidents involving information violations and information security violations to ensure that incidents are promptly and thoroughly investigated; the magnitude of the potential loss is properly evaluated; and that VA management, appropriate law enforcement entities, and individuals and entities potentially affected by the incident are notified in a timely manner.

INFORMATION SECURITY CONTROL WEAKNESSES HAVE PERSISTED FOR YEARS

For the past several years, we have reported vulnerabilities with information technology security controls in our Consolidated Financial Statements (CFS) audit reports, Federal Information Security Management Act (FISMA) audit reports, and Combined Assessment Program (CAP) reports. The recurring themes in these reports support the need for a centralized approach to achieve standardization, remediation of identified weaknesses, and a clear chain-of-command and accountability structure for information security. Each year, we continue to identify repeat deficiencies and repeat recommendations that remain unimplemented. These recommendations, among other issues, highlight the need to address security vulnerabilities of unauthorized access and misuse of sensitive data, the accuracy of position sensitivity levels, timeliness of background investigations, and the effectiveness of Cyber Security and Privacy Awareness training. We have also reported information technology security as a Major Management Challenge for the Department each year for the past 6 years.

CONCLUSION

Because the employee was responsible for planning and designing analytical projects and supporting surveys involving all aspects of VA policies and programs, he was authorized access to, and use of, these and other large VA databases. However, at the time of the burglary his supervisors were not aware of the employee's self-initiated project and, as such, had no official need or permission to take the data home. In addition, the employee reported that the data stored on the stolen external hard drive was neither password-protected nor encrypted.

Although senior managers and other OPP&P staff were informed of the possible loss of data on May 3, 2006, the incident was not communicated up the chain-of-command until the VA Chief of Staff was notified 6 days later. Poor communication, partially resulting from a dysfunctional working relationship among senior OPP&P

executives, contributed to the delay. While there was considerable rhetoric among management concerning the need to identify the extent and scope of the stolen data, there was virtually no follow-up with the employee to obtain results. Also, the lack of urgency in addressing this issue was impacted by the false assumption that the SOC had the responsibility to investigate the incident and make all required notifications.

On May 10, 2006, Mr. Bowman requested legal advice from OGC. Yet, during the 6 days following this request, Mr. Bowman did not follow up to determine the status of the request, or task anyone to develop a more definitive description of how many veterans' records may have been stolen. Although Mr. Bowman acknowledged he knew the data stolen could potentially affect millions of veterans, he demonstrated no urgency in notifying the Secretary of the incident and decided to wait for OGC's response before doing so.

Mr. Bowman also notified Mr. Mansfield on May 10, 2006, but Mr. Mansfield too decided not to raise the issue to the Secretary until they knew more information on what VA's legal responsibilities were and more about the magnitude of the problem.

At nearly every step, VA information security officials with responsibility for receiving, assessing, investigating, or notifying higher level officials of the data loss reacted with indifference and little sense of urgency or responsibility. Efforts to investigate the incident were further impeded by errors and omissions in the ISO's incident report and were delayed due to ineffective coordination between the OPP&P ISO and the SOC. Twelve days after receiving the original incident report, the SOC had made no meaningful progress in assessing the magnitude of the event and had attempted to pass responsibility to gather information on the incident back to the OPP&P PO. Coincidentally, this is the same individual who referred the matter to the SOC in the first place, which he did in his dual capacity as ISO for OPP&P.

The OIG was able to determine the magnitude and extent of the stolen data after one interview with the employee on May 15, 2006, and I notified the Chief of Staff on the morning of May 16, 2006. The Chief of Staff notified the Secretary shortly after my call. It is unexplainable why no one in the management chain-of-command ever attempted to re-interview the employee to gain a better understanding of the scope and severity of the potential data loss, prior to my call.

While no policy was violated in the handling of the incident, staff and senior managers who were notified of the theft failed to take appropriate action to determine the magnitude of what was stored on the stolen external hard drive, or whether it was properly safeguarded. The failure to determine this resulted in not recognizing the potential significance on VA programs, operations, and veterans. Since the local police were not told for 13 days that VA data was stolen during the burglary, valuable forensic evidence was most likely lost. The delay also prevented the burglary from receiving the urgency it warranted from Federal law enforcement agencies.

We found that VA's policies and procedures for safeguarding information and data were not consolidated or standardized to ensure all employees were following all applicable requirements in a similar fashion, and that policies and procedures were not adequate in preventing the loss of the data. We also found that VA employees and contractors were not adequately trained and reminded of the policies and procedures to follow to safeguard personal or proprietary information, sensitivity level designations were not always accurate, information and data provided to contractors need to be better safeguarded, and VA incident reporting procedures and controls need improvement.

Since the incident VA managers have attempted to strengthen policies, procedures, and controls to prevent similar disclosures, but additional actions need to be taken to safeguard protected information and VA's automated systems.

Our CFS audits, FISMA audits, and individual CAP reports of VA medical facilities and regional offices all highlight specific vulnerabilities that can be exploited, but the recurring themes in these reports are the need for a centralized approach to achieve standardization in VA, remediation of identified weaknesses, and accountability in VA information security. Specific recommendations were not made in our July 11, 2006, report because 17 recommendations are listed in previously issued OIG reports and are being followed up on separately.

RECOMMENDATIONS

We recommend that the Secretary:

• Take whatever administrative action deemed appropriate concerning the individuals involved in the inappropriate and untimely handling of the notification of stolen VA data involving the personal identifiers of millions of veterans.

• Establish one clear, concise VA policy on safeguarding protected information when stored or not stored in VA automated systems, ensure that the policy is readily accessible to employees, and that employees are held accountable for non-compliance.

• Modify the mandatory Cyber Security and Privacy Awareness training to identify and provide a link to all applicable laws and VA policy.

• Ensure that all position descriptions are evaluated and have proper sensitivity level designations, that there is consistency nationwide for positions that are similar in nature or have similar access to VA protected information and automated systems, and that all required background checks are completed in a timely manner.

• Establish VA-wide policy for contracts for services that requires access to protected information and/or VA automated systems, that ensures contractor personnel are held to the same standards as VA employees, and that information accessed, stored, or processed on non-VA automated systems is safeguarded.

• Establish VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems, including specific timeframes and responsibilities for reporting within the VA chain-of-command and, where appropriate, to OIG and other law enforcement entities, as well as appropriate notification to individuals whose protected information may be compromised.

The Secretary agreed with the findings and recommendations in our report and provided acceptable improvement plans.

CLOSING

In closing, I would like to assure the Committee that we will follow up on the implementation of these recommendations until they are completed. Mr. Chairman and other distinguished Members of the Committee, thank you again for this opportunity and I would be pleased to answer any questions.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. AKAKA TO HON. GEORGE J. OPFER

Question 1. Please provide an explanation for the apparent breakdown within the Office of Information and Technology in responding to this incident.

Answer. The breakdown was attributable to a number of factors, not the least of which was the lack of a single coherent policy for investigating incidents in which protected information was inappropriately disclosed, lost, or stolen. Existing VA policies focused more on incidents involving the breach or attack into VA's automated systems, and less on Privacy Act violations. Also, the incident report initially filed contained errors and omissions which made it difficult to determine if this was an information system or privacy violation. The distinction was not made for 12 days.

Question 2. Please provide any details on the specifics of the FBI's forensic examination of the stolen hard drive.

Answer. It is my understanding that when you copy or access computer files, there is evidence of it in the form of a time/date stamp. The FBI computer forensics examinations did not reveal any date stamp on any of the stolen files after May 2, 2006, the day before the burglary. The FBI cannot give 100 percent assurance because there are highly technical ways to access or copy files without leaving a time/date stamp. However, we do not believe the thieves possessed the necessary technical skills for the following reasons.

• The string of burglaries around the same time and in the same general area suggests that the thieves were targeting items such as laptops and other computer equipment that are in demand and could be easily sold. The fact that the computer equipment was purchased off the street for such a negligible amount indicates that the individual selling it was unaware of what was contained on the hard drive.

• Multiple computer disks with VA files, which were used to download the VA data onto the external hard drive, were in the employee's house but not taken during the burglary. This suggests that the computer equipment and not the data was the target of the theft.

Given all these factors, we are highly confident that the data was not accessed.

Chairman CRAIG. Well, Mr. Secretary and Inspector General, I am sure we can dwell on the past, and we have just heard a recapitulation of the past and the failures of the system and the per-

sonnel involved to deal with this in a timely fashion. Or we can focus on the future and where we go from here.

By your own expression and by the consistent expression of observers of the past, this system had shortfalls, could fail, did fail. So let me proceed with those thoughts in mind to a series of questions of how we go forward.

First and foremost, Mr. Secretary, you say you are retaining a company for the purpose of monitoring information or breach flows. Is that a result of the lack of absolute confidence that the information was not breached or a risk that there could have been some breaches?

Secretary NICHOLSON. More the former, Mr. Chairman. There is a company out there—and there may be more than one—that has a proprietary software that analyzes large banks of data and looks for correlations of incidents and can by doing that determine these identity thefts are being sourced from a common data bank.

One company that we are very familiar with and have talked to in great detail is called ID Analytics. ID Analytics subsequently donated its services to VA at no cost. But that gives us, a suspenders-and-belt sort of feeling that, while the FBI has told us that they say with a very high degree of probability this has not been compromised, they do not say it is 100 percent. So by engaging this company, it gives us another line of reconnaissance, if you will, to see if anything would start popping up that could be traced back to this bank of data. If that happened, then we can take actions with respect to monitoring and so forth, notifications.

Chairman CRAIG. Do you know or have a general idea of what this monitoring will cost? And do you have the money to accomplish that?

Secretary NICHOLSON. I do have a general idea of what it will cost, and we do have the money, yes. It is, I can say, we are bidding it, so we would like to protect our position.

Chairman CRAIG. That is why I asked the way I asked.

Secretary NICHOLSON. It is relatively inexpensive. It is surprisingly inexpensive.

Chairman CRAIG. OK. Mr. Secretary, you have begun to outline for us a great deal of what you are putting into place as a result of this failure, and before asking this series of questions, I think it is tremendously important for this Committee to gain from you and from VA a detailed plan as to what you plan to do and how you plan to implement it for a lot of reasons.

First of all, you have said it will take time, and that is appropriate, to get it right and to develop a consistency inside VA and a culture and a protocol and all of that. And my guess is it will be a time in which you may be long gone from here, as may I and others. But it is important for this Committee and those of us who will monitor it—because we will—to understand that procedure, that process, for a couple of reasons: To be critical of it, yes, to be observant of it, to monitor it, to check it along the way, to work with VA to make sure this happens. As you know, the House is moving, I think today, to mark up legislation directing and mandating a certain procedure.

So having said all of that, does this plan give veterans, in your opinion, the assurance they deserve that information and cyber security has become your top priority?

Secretary NICHOLSON. I would say unequivocally yes to that. You know, this is the order of the day at the VA, and since this has occurred, I have traveled out and about and talked to hospital directors and regional office directors, and they have the word. They have the sense of urgency.

But, it is still in the nascent stage; you know, we are talking and we are getting the talk right, and we are beginning to confront the culture. But there is a great deal now that has to be done. I mean, the real implementation, then transformation has to be done.

But I would point out—and I think it is fair to do that and to give acknowledgment of it, that we started—last October we started a major change in this agency, and that was a very big decision I made, resisted in many quarters of the vast organization, because it is bringing about a big change. On October 1st, some 5,050-some people will be moved and over $400 million will be moved to the CIO, consistent with the centralization of responsibility and control over information technology and information security.

Chairman CRAIG. I will come back with additional questions. Let me turn to Senator Akaka.

Senator AKAKA. Thank you very much, Mr. Chairman.

Mr. Secretary, I am sure that you appreciate that, as a result of the data theft, veterans' confidence in VA has been low. The veterans my office is hearing from are not certain about VA and what VA is trying to do to help them, and it gives me a feeling that they will not be easily reassured.

As I am sure you know, many veterans organizations are opposed to the decision to not provide credit monitoring, and so my question to you is: What is the status of that about credit monitoring? You did mention that you will retain from the private sector a company that will continue to monitor this situation. Can you give me a status of that?

Secretary NICHOLSON. Yes, I can, Senator. The decision was made both at OMB with engagement by us, the VA, that the credit monitoring that was moving forward as a result of the recovery of the data and the FBI's prognosis that it was not compromised caused us to conclude that individual monitoring was not necessary at this time. And then we were affirmatively going to engage this data bank monitoring. And that is the case, and we have had conversations with the VSOs. Some of them do oppose our decision, and some concur with it, think that it would be a waste of $160 million at this time based on the FBI's analysis.

Senator AKAKA. Is the company that you are retaining to continue this monitoring of the situation the same group that was dealing with the credit monitoring?

Secretary NICHOLSON. No, sir. It is a different company. There may be other companies. We are putting it out for proposal, you know, a request for bids. But we know of the one, we have talked to them.

Senator AKAKA. Thank you.

Mr. Opfer, your investigation found that a number of senior VA officials did not seem to have a sense of urgency in reporting the

missing data to the Secretary who has, again, said that he did not know about it until 2 weeks after the theft. Do you have any explanation for that?

Mr. OPFER. Yes, Senator. Most of the senior officials that we interviewed seemed to be unfamiliar with the databases believed to have been stolen and records that they contained. The initial notification of the incident did not quantify the magnitude of the potential for the loss. And it did not seem to trigger a sense of urgency on the part of any of them to look into it or to take control of the issue to try to determine what potentially could be the harm. Several of them told us that they were working on the mistaken assumption that someone else in VA was going to be following up and doing an investigation and making the notifications to higher management and that they were waiting for additional information. It really comes down to a failure to recognize the magnitude of the potential loss and taking control of the issue and trying to determine exactly what potentially could have been compromised by the employee losing that data.

Senator AKAKA. Mr. Secretary, I am sure you appreciate one of the concerns that Congress has is that we learned of the data loss only shortly before hearing about it on CNN and other media outlets. If you had to do it over again, once you learned of the data breach, would you at least have come to the leadership of the Veterans's committees and let us know about the problem earlier?

Secretary NICHOLSON. That is a good question, Senator. Here was the dilemma: After I did learn about it, of course, I immediately informed the White House about it, and then, the Department of Justice and the FBI and a lot of very senior people got involved in it. But one of the dilemmas was if you go public with this, you will inform whoever has that of what they have, thinking they may not know what they have. As it turned out, as I have often said, through good law enforcement and the grace of God, they did not know what they had and we got it back. They fenced it and somebody turned it in for the reward.

But that was the dilemma, and on the eve of the day—that is, the 21st of May—we had a very big powwow about that, and there were pros and cons. I made the decision that we needed to inform you, the veterans, that this had happened. And so on the 22nd, we did it.

Senator AKAKA. Thank you very much. Before I give it up, I want to add my gratitude to General Counsel McClain for your service and I want to wish you well.

Mr. MCCLAIN. Thank you, Senator.

Senator AKAKA. Thank you, Mr. Chairman.

Chairman CRAIG. Thank you, Danny.

Senator Murray.

Senator MURRAY. Thank you very much, Mr. Chairman, and I do want to follow up Senator Akaka's question on credit monitoring. But before I do that, I wanted to return to the question about your trip to Walla Walla, because as you know, I have a community that cares deeply about this. They have followed the process very, very closely, and they want to have a real voice in the process. And I specifically wanted to ask you about the plan to involve the local community. They have followed the CARES process very, very

closely. They expect that the VA will follow it, too, and that means sending a plan to the local advisory committee for review. Can you commit to us that you will follow the CARES process and work with that Local Advisory Panel?

Secretary NICHOLSON. Yes, I can, Senator Murray. We have followed it, and we have been through the first two stages, and our analysis based on that, I make those decisions. I made a decision on Walla Walla that we would keep that campus open. And the purpose of my visit there was to tell them—the community, the patients, and the staff, all of whom had anxiety—about whether or not we were going to close this. For the benefit of the others, it is a very small VA hospital complex. And I made a decision to keep it open, and that was my purpose of going there.

Now, we are going to go into the third stage, which is being justifiable to keep it open. What will it look like? And as you know, when I went there, I assured them that we were going to have a new ambulatory outpatient clinic facility there. We have other issues that we will be dealing with, and we will be engaging the Local Advisory Panel on those issues, such as long-term care, inpatient medicine and inpatient mental. We have those capabilities there, but as you know, the populations are very small. For example, the average daily census in the nursing home is 22, in the mental health it is 18, and in medicine it is 10.

Senator MURRAY. OK. But you will follow the LAP process so that that plan will go to the LAP committee and they will have their official——

Secretary NICHOLSON. Yes.

Senator Murray [continuing].—responsibility to have a response back?

Secretary NICHOLSON. Yes, we will.

Senator MURRAY. The questions that are raised are really—I mean, we have been dealing with for a long time. There aren't any facilities in the local community to outsource this to. And maybe more to the point, as you know, your announcement came as a surprise because many of us have been working very, very closely on this for a number of years now with the community and did not know that you were coming out there. I am glad that you have taken the first step to do that, and now the second step to continue the LAP process and send the plan.

But could I get your commitment to come in and talk with me, bring your staff, so that I can talk with you about the proposal and learn where we are going to go from here?

Secretary NICHOLSON. Yes, indeed. Sure, we will do that.

Senator MURRAY. OK. I would really appreciate that because this is obviously a very involved community. Senator Craig has been out there. He knows as well as I do, and we would like to work with you to get us to where we need to be. I would appreciate that.

I also wanted to ask you about Bellingham because when you were there, we were told that you committed to bringing a VA clinic to Northwest Washington and that some kind of announcement would be coming within the week. And I have been unable to get any clarification from your staff, and I wanted to find out from you here, can you tell me what you said in Bellingham about the new clinic so that we all are on the same page?

Secretary NICHOLSON. I can. What I said to the veterans there with whom I met was that we have made a decision in the CBOC business plan analysis that we would put a new community-based outpatient clinic, CBOC, in Northwest Washington, somewhere between Seattle and the Canadian border. I did not specify where it would be located, and I would be happy, when we have our meeting, to discuss that with you, but we have not made a decision as to where to site it.

Senator MURRAY. But the decision has been made to site one there?

Secretary NICHOLSON. Yes.

Senator MURRAY. Is there a time on that, a time commitment?

Secretary NICHOLSON. We hope to make the decision about where to put it before the end of the year, and then, you know, it usually takes us 6 months or so then to open one.

Senator MURRAY. Well, I appreciate that, and, again, part of the reason there has been such a flare-up over this is that our veterans are very well aware of politics and policy. They care deeply about policy, and the confluence there has really riled a lot of people, as you probably know now from the press. But one of the problems, I think, that I am hearing back and I think you should be aware of is that people are aware that clinics are a promise to veterans and they need to be part of a policy that we are all aware of. And there is a deep concern that many of these promises that are being made for clinics are being made in Republican districts and not in Democratic districts. And maybe it is just a confluence of where things are, but are you aware that since you have been announcing clinics, 80 percent of them are in Republican districts? And I think that has brought some question to whether or not we are going to have politics become part of the VA process. I do not want that to happen. I do not think anybody does. But I just wanted you to be aware that is part of what some of the backlash has been on this.

But I do appreciate your commitment to work with us. As you know, having been in Walla Walla, this is a really caring community. They have worked very hard on this, and I really appreciate your commitment to the LAP process and to having that community continue to be involved. And I will work with you on the western Washington CBOC, and I am really glad that is part of the process that you are going in as well. So thank you very much.

Secretary NICHOLSON. I was not aware of that statistic. I have never done that calculus. In fact, I am quite sure that district is a Democratic district.

Senator MURRAY. It currently is, but, unfortunately, the announcement was made on a political campaign rather than bringing the veterans in who have been following this, believe me, day by day.

Chairman CRAIG. Senator Murray, thank you.

Senator Burr, thanks for joining us, and please proceed with any opening comments you would like to make and questions of the Secretary and the IG.

STATEMENT OF HON. RICHARD BURR, U.S. SENATOR FROM NORTH CAROLINA

Senator BURR. Thank you, Mr. Chairman, and my congratulations on one additional notch on your age. I understand it is your birthday today.

Chairman CRAIG. Thank you so much.

Senator BURR. Mr. Secretary, I really only had one question, but Senator Akaka has stimulated me to make a statement, and I will try to do this as diplomatically and delicately as I can.

Your answer to his question basically said that there was a lengthy debate with a lot of people about whether and when to notify Congress, and you won. I would tell you, just as a Member of Congress and of this Committee, a debate on whether that happens and when is not a debate that needs to happen. Notification of this body is an automatic thing.

You were not served well, I think you have acknowledged that, from a standpoint of the lag time it took for the information to get to you. I also look at what you considered to be a quick decision in this debate at issue, and I consider the lag time between the 16th and the 22nd, the notification of us, as unacceptable. So my intent was not to rehash any old stuff. It is just to make the point that we are partners, and we serve the veterans, you serve the veterans. We each have a piece of the responsibility. Ours is policy and financially. It takes all partners to make it work, and I would hope that in the future, regardless of what area of Government, there would not be a debate about whether or when Congress was included in good news or bad news.

My question is a very simple one. You have gone through an exhaustive process to find what the correct path from here is, and I commend you for that. I think it has been done very thoroughly. What will you do to gain back the trust of veterans? I think that was at the root of Senator Akaka's question. We made an offer to veterans that I think was an offer we had to make—credit monitoring. I was not part of that debate as to whether we continued it or not. But that decision was made. Now the responsibility still falls to you of, over and above, just fixing this system and monitoring to see what happens, how do we gain back the trust of veterans across the country?

Secretary NICHOLSON. Well, Senator, I think you have to earn it and you have to show leadership and commitment and delivery. I travel a lot. I meet with a lot of veterans, and I talk to them about a lot of things. And I would say that generally, because the VA continues to function very well—I mean, I don't know if you were in here when they mentioned about the Business Week article saying that we are not only the biggest, but the best health care system in the United States of America. And a week ago Monday night, Harvard University awarded the VA its top award that it gives every year for the best innovative solutions in Government. And 1,000 entities competed for that. And the VA won, and they had a big banquet up here at the Washington Hilton and awarded that to the VA.

The VA earned that. The VA continues to provide outstanding services, medically and benefits and burials, to veterans. So it is functioning very well. But this is, no question about it, you know,

a real flaw and a very visible one. So we have to earn that back. The best way to do it is every day, you know, getting up, putting on your work clothes, and doing a good job, and then making sure that we get this right, that this does not happen, and that we do indeed become the model for this that we can be depended on.

Senator BURR. Well, I clearly acknowledge to you, I believe we do much more good than we do bad. This is an unfortunate incident. Let me just restate that if there is one organization out there that is unhappy with the course that we have laid out, then it makes our job that much harder to build that trust back, and I would just encourage you today to, as aggressively as you can, bring those groups in that represent those veterans. Find a way to bring their assurance level high enough that it is not just a cutoff mark. And, you know, we all know the realities that we are faced with, and if there is $160 million that we do not have to spend on that, we can put it into health care. That makes tremendous sense. But I think we also have to understand that there is some element of the population out there that we also promised that money to make sure that their identity, their credit was protected. As long as 100 percent of them feel and are told that they should be comforted at what direction we have turned to, I will feel comfortable. But unless we have reached that consensus, I think we still have some work to do.

I thank you for your willingness to come up and share your plans with us. I thank you for your service, especially at a time that it has not been easy as Secretary of the VA. More importantly, I thank the Chairman for, I think, the methodical way that this Committee has worked through this issue trying to find a common solution, and I commend you.

Chairman CRAIG. Thank you, Senator.

Mr. Secretary, General Opfer, let me make a couple of comments and then go into the plan and where you all are going to go. We are tremendously proud of what VA did during Hurricane Katrina, the orderly process of evacuating hospitals and removing people and taking them out of harm's way. You did it because you had a plan and you had practiced it and executed it. You could do it jointly or hospitals could do it individually. And when communications systems broke down, hospitals did it individually.

I was here on 9/11. Most of us were. Chaos reigned supreme on Capitol Hill. Why? No plan of execution, no process, no procedure, and, more importantly, no drilling—no establishment within the system and within the employees—of how you deal with an emergency crisis. We are now doing that. The bells ring around here. People orderly march out. They go to their points of contact. They go to garages. They are quarantined. We practice, we drill. And we are getting better. And even during that, there is a sense of calm now that, if it were real, somehow we would have a way of orderly moving through this and getting out of it. That is how you establish a culture. You do not do it by simply putting it on paper. You work it. You process it. You proceed. You practice it. And you enforce it amongst those who fail to listen. As much as I respect the VA, I also understand the firewalls of a bureaucracy that will resist change.

So let me turn to you, General Opfer. Have you had a chance to review VA's implementation plan that the Secretary talks about? And if so, what are your comments?

Mr. OPFER. Yes, Mr. Chairman. The report that we issued covered a lot of issues raised in the FISMA work, the consolidated financial statement audit, as well as the data loss. We made a number of recommendations to the Secretary, and I am very pleased at the reaction of the Secretary and his commitment toward the recommendations in our reports. The Secretary has concurred with all the findings and the recommendations that we have made and provided us improvement plans.

In his response, he has extended a commitment to strengthening and clarifying all the VA policies which relate to information security and privacy issues, holding employees as well as—I think a very important factor—contractors to the same standards and to make sure that we are correcting the problems found with contracts, so that they all comply with these policies.

Improvement plans provided by the Secretary are responsive to our recommendations, and I think when they are fully completed and fully implemented, they will address the concerns that we raised in the report. The Secretary mentioned an issue which I think is one that we have to overcome. There is a culture problem that we need to address because this change really addresses that we need to have the people, all the employees in VA and contractors, those that use the systems change their culture regarding the use, the storage, and transmission of the data. And I think that the plan will provide us an opportunity, and we will fully review all the recommendations as they are being implemented to make sure that they are fully implemented.

Chairman CRAIG. You have walked into my next question, and that was: Do you have a plan to follow up and to monitor?

Mr. OPFER. Yes, usually what we do—and we will in this case, Mr. Chairman—is we will not close out any of the recommendations until they are fully implemented. For example, implementation of a new policy and procedures without compliance does not do any good. You have to have the compliance with the policies and procedures. So we will not accept that they have established a policy and procedure, we will go out to various facilities to make sure that there is compliance, not only in headquarters, but whether it is in a hospital or another location out in the country. We will aggressively follow up on all those recommendations and make sure that they are in compliance.

In addition, as I mentioned, our FISMA work and consolidated financial statements audits, prior to this issue, I had made a decision that I was going to contract out next year for the FISMA work, and I wanted to use the staff that the IG had that was doing the FISMA work to do additional IT penetration tests and other IT security issues. So this would fall right into it. We will aggressively pursue—and as I am testifying here today, we are doing unannounced penetration tests and other compliance audit reviews, and we will aggressively continue to do those.

Chairman CRAIG. Thank you.

We have been joined by Senator Thune. John, do you have any opening comments or questions before we start the second round?

STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Mr. Chairman, I just want to thank you for holding the hearing, and I want to thank Secretary Nicholson—and good to have you here, Mr. Opfer—for joining us and hopefully shedding some additional light on this very important issue of data security. It is something that veterans in South Dakota—one of the things when I travel in my State, and I am sure you hear this, too—an issue that really got on the radar screen. There is a tremendous concern—it really penetrated the consciousness of our veteran community out there and a real concern. And I guess my whole concern here—and I hope that some of the findings and recommendations and issues that have arisen out of this will give us an opportunity to address this so that it never happens again. So we look forward to working with you on that, and I want to thank you, Mr. Chairman, for holding this hearing.

As we said at the last hearing we had, when initially this was disclosed, we have got a lot of work ahead of us, and so we look forward to getting that done. I will let you go ahead and some of the folks who have been waiting here ask some questions, and I will perhaps ask some questions on the second round. So thank you for holding the hearing.

Chairman CRAIG. Senator Thune, thank you.

Senator Murray.

Senator MURRAY. Thank you, Mr. Chairman.

Let me follow up on the credit monitoring issue again, because I think Senator Burr spoke to the issue that I think is deeply concerning to all of us, that is, reestablishing trust to our veterans. And a promise was made to them, after they felt very violated that their records had been gone, that they would have this credit monitoring for a year. So I think the announcement that they would then not have it has jarred a lot of feelings, well, how do we trust this? I think that is an important point in consideration, and no one wants to spend money unwisely. But I would suggest that it would be wise money spent. I listened very carefully to the plan, and obviously a change of culture with an additional long-term implementation of encryption processes and all the other things that are going to go into making sure that the records are not breached again, leaving those records vulnerable until all of that is accomplished, it seems to me that the credit monitoring would be a wise investment.

But the other issue that I want to raise as well that tells me that we should keep credit monitoring is that we are getting a number of veterans calling us telling us that they are getting called by people who say they are with the VA and asking for personal information in order to protect the veteran's credit. I am very concerned that we have left this population vulnerable to those kinds of individuals, and providing the credit monitoring will give them the ability to say, "I already have protection," and make them much less vulnerable to those kinds of people who will use this incident to go after them.

So I would like to ask you again, Mr. Secretary, where you stand on the individual credit monitoring and how we can perhaps go back to that question.

Secretary NICHOLSON. Again, we made a decision that after the data had been stolen, was, you know, at large, that we should contract and provide credit monitoring for the affected veterans. Then the data was recovered, and the FBI is saying that this data was not compromised. And the cost, given the large population of people, is approximately $160 million. So the facts changed. The situation has changed.

We plan to inform the veterans of that, and we plan to inform the veterans in a letter telling them they can still have their credit monitored by one of the three monitoring agencies, free for a period of, I think it is 90 days by calling them on a 1–800 number. They can still get credit reports three times during the year if they have any concerns, and that we are doing this overarching analysis of this data to——

Senator MURRAY. So is the credit monitoring still available to the veterans? Maybe I misunderstood.

Secretary NICHOLSON. Not in the form that we were going to provide before the data was recovered, no. But all veterans, all citizens are entitled to call one of those credit monitoring companies and get a copy of their credit report and to have a credit alert put on their file for——

Senator MURRAY. But it costs them something.

Secretary NICHOLSON. No, it does not cost them anything.

Senator MURRAY. But you are not going to offer the one year free credit monitoring that originally was involved. Well, can you give this Committee the assurance 100 percent that information was not accessed?

Secretary NICHOLSON. I can only give you, Senator Murray, what the FBI has given us, which is that this data, based on their forensic analysis and the expertise that they have, combined with the circumstantial part of it, which was that this was, again, random burglary that was not seeking this data, and the way it was handled and fenced and somebody bought it and turned it in for a reward——

Senator MURRAY. But it was fenced and someone else had it, so it is—I have not seen the FBI report. Obviously, they have not shared all the details with us. But there still can be a chance that it was accessed by someone who knew what they were doing.

Secretary NICHOLSON. I think that I could not sit here and say to you that it is 100 percent, because the FBI has not told us that.

Senator MURRAY. OK. And we also know that the VA records themselves, still we have not implemented the plan that you have now moved forward. You are moving forward on one, but the records still are not encrypted. There still has not been the change of culture, those kinds of things that we can guarantee people. Correct?

Secretary NICHOLSON. All of our restructuring and reformation and all that are not complete. That is correct. There are many things underway.

Senator MURRAY. And are you aware that some of our veterans are getting called by people saying that they are with the VA and offering services?

Secretary NICHOLSON. I have heard that on a couple of occasions they were being called by the VA because the VA does polling of its beneficiaries continuously, both medically and benefit——

Senator MURRAY. They call and ask for personal information over the phone?

Secretary NICHOLSON. We have discontinued that. It is just authentication information that they are talking to the right person. But we have discontinued that for now because that was causing confusion. But, additionally, it is possible that—I mean, it is not only possible, it is probably happening that veterans are getting calls from people in this fraudulent world because that happens. Last year, I am told that 9 million Americans had their identity stolen.

Senator MURRAY. Right. And, unfortunately, some people are using this incident to then call veterans and ask for their personal information, saying that they are with the VA, which leads me, again, to the conclusion that providing this credit monitoring for a year will give some security to veterans at a time when, whether it was real or not, whether actually the data was used or not, there is a lot of insecurity out there. So I guess I would just ask, Mr. Chairman, if that question could be reconsidered, if we could look at the facts. I think it is a time when we have to reassure our veterans. I do not want to spend the money any more than anyone else does. I certainly do not want to see it come from benefits or health care. But I also know that a climate has been created that could be used by someone who is using it fraudulently, but also when our veterans themselves still do not know that their information is encrypted, and I think that kind of security would be something that we—I hope we can relook at that decision and do it quickly.

Chairman CRAIG. I thank the Senator, and I do not think any of us do not share in your concern. And it is not a perfect world, and I think the reality is—and that is when we began to look at this in a situation where we believed—we knew that the information had been stolen. We did not know that it had been breached yet; that veterans, by simply the multiplier that the Secretary spoke to, some were going to get their ID stolen, whether it was out of this database or whether it was another database; and that how we measured that was going to be critical because the Government is not responsible for a veteran's loss of information if it is not out of this database, and how we break that out, clarify it, and understand it.

So I am to date comfortable with the current monitoring that is underway and planned for the broad sense to try to assure that what we believe is now at hand is valid. And I am willing to live with that for the time being.

If there is any indication that it is not, then I am going to agree that there is a responsibility.

Senator MURRAY. Well, we do have a problem because we have all been out there talking to veterans saying, "Your credit is free monitoring." They may not know that the decision has been rescinded, and, you know, for us to go back out there and say, "Oh, never mind now" is a very difficult situation.

Chairman CRAIG. That is a communications problem that I think we have got to all work collectively at, and I——

Senator MURRAY. Yes, and I am just looking at it, it is just my recommendation that we continue it.

Chairman CRAIG. I appreciate that.

Senator MURRAY. But we will have the discussion.

Chairman CRAIG. Yes.

Mr. Secretary, how do we, how does this Committee, how does VA, and how does a new Secretary 3 years from now or 4 years from now, sit before this Committee and hold up a brochure like this and say, "Today Harvard has announced that the information system of the VA is the best in the Nation and a model for the rest of the Federal Government to follow?" How over the course of the next 3 years do we work with you and a new Secretary to make sure that that announcement day comes? We obviously, by the establishment of VA's electronic medical records success, have it within the system's capability of getting it done. And how do we work with you to assure that same thing will happen system wide in the information world?

Secretary NICHOLSON. Well, that is exactly the goal, Mr. Chairman. You have described it. That is what we talk about, our leadership team, when we talk about the change that we are in. We use the term the "Gold Standard," but that is really what we are talking about. If we can win this annual award for innovations and Government solutions for our electronic medical records, we can do it for our information technology and security systems.

But, you know, it is going to take a very good plan, that is, good architecture. Then it is going to take good implementation and constant monitoring, you know, management, to see that it is functioning the way that it should. And that is the path that we are on.

We have brought in the best, we think, that exists to help us in that architecture to design the kinds of systems that we need. And as I have said in my testimony, we made the threshold decision last October which had to be the predicate for all of this that we have centralized the management of information technology in this vast bureaucracy where it was decentralized all over the world, really, from Maine to Manila. That is all being pulled in, and that was underway because of some of the deficiencies that had been pointed out for several years by the IG.

It is accelerating. We have a sense of urgency about this. This is a terrible event. I do not think that a lot of it is very technical when you talk about the kinds of encryption models that we are going to use and those kinds of things, but a lot of it is common sense of having people inculcated with this culture. And the model that I use, which I am very familiar with, is the military, where to have access to classified information, you have to have a clearance and you have to have a need to know. I think that is a model that we need for access to all this digitized information that we now work with in this agency and so many others. We need to know something about the people to whom we are giving this access because you have to—in the end game—you have to trust them. You cannot keep it from them.

Somebody asked me at one of the hearings how we could let them carry it out, and I held my wallet up, which is larger than this hard drive. But they do not have to carry it out, Mr. Chairman. They can send it out.

Chairman CRAIG. That is right.

Secretary NICHOLSON. So you have to be able to depend on the people, and you have to know something about them, which means give them background investigations, clearances. So it is a composite of all those things. It is going to take a lot of management.

Chairman CRAIG. Have you established a time line? Is that now in place? Or are you far enough along to say here are time lines in which certain things will be accomplished that we in the Congress can—that you can share with those of us in Congress who are focused on this, share with the Inspector General, in a way that we can monitor with you those successes?

Senator Murray talks about a state of confidence. Senator Burr talks about a state of confidence. Senator Akaka talks about a state of confidence. As I said in my opening statement, the state of confidence on Capitol Hill does not exist today because of repeated warnings, repeated observations, and a failure to adhere to that, not on your watch, but on many watches before you. Had that state of confidence been established, and a procedure and a process, prior to your presence as Secretary, there is a strong likelihood that what occurred on the 3rd of May would not have occurred. And so I do not think this Congress is going to be confident, and my guess is that the population that VA serves will not be confident, until that plan is monitored, publicized, implemented, and the implementation phases are monitored and publicized.

When can we expect to see that kind of time line, procedure, and process?

Secretary NICHOLSON. We have that, Mr. Chairman. In fact, it is at Tab 3 of the IG's report, which I am sure you have a copy of.

Chairman CRAIG. OK.

Secretary NICHOLSON. It takes pretty good eyesight because it is——

Chairman CRAIG. That may be my problem at 61 years of age.

[Laughter.]

Secretary NICHOLSON. I was going to say as a World War I veteran——

[Laughter.]

Secretary NICHOLSON. I would refer you to that, and this is a dynamic document, but it does show the functional things that we are doing and time lines that have been affixed to them. And because it is dynamic and it is not all cast in bronze yet, I would not submit it for the record of this hearing. But the IG has it, and it is in the report.

Chairman CRAIG. We have it. That is why I brought it up. This needs to be known.

Inspector General, how do you monitor this time line? It is in your report. You have a process in place now to follow through?

Mr. OPFER. Yes, that would be the process I described before, Mr. Chairman, of any recommendations or findings that we have in the report. We do not clear those recommendations or findings until they have been fully implemented and we have verified that they have been implemented throughout all the facilities in VA. That is part of our follow-up process.

Chairman CRAIG. OK. Thank you.

Senator Thune.

Senator THUNE. Thank you, Mr. Chairman, and I appreciate that line of questioning. That is an issue that I have talked about in previous hearings here, and that is the issue that was raised with the House bill that would centralize everything. And I think we talked about at this hearing the efforts that are being made internally to accomplish some of those same objectives at the VA. And so I am very interested in the Chairman's line of questioning with respect to timing and how that is proceeding.

I also am interested in just getting your reaction, because I think they are debating in the House today, to legislation that would make the CIO at the VA an Under Secretary, and if you think that makes sense, to have someone that has got more, I guess, line authority, someone that can oversee this whole effort that is being made to get this information centralized. And I know you have different models that have been described at previous hearings. The Federated model I think is the one that you are—is that correct? Is that the one that you are pursuing right now?

Secretary NICHOLSON. Yes.

Senator THUNE. But I guess I would be interested in knowing, Mr. Secretary, whether the legislation is something that you would support, whether that is a worthwhile course to proceed with, and any other thoughts you might have about how we just tighten this up so that the information that is there does not have the propensity to be, I guess, lost or stolen like what we experienced here with this last event.

Secretary NICHOLSON. Well, I think that is a very good question, Senator Thune, and we have been working with it. The House is doing that, with all the best intentions of trying to help this, that is, to make the Chief Information Officer an Under Secretary.

I do not think it is necessary. The importance underlying all of this is leadership, the commitment, and sound management. And so the title that you give someone, that is not going to fix anything. It is how it is implemented and in this cultural change that we have been talking about.

So it violates, frankly, my sense of design of an organization because we have three Under Secretaries and each of them have operational responsibility: One is to run a health system; the other is to run a benefits system; and the other is to run a burial system. They are operators. They are in a military context. They are maneuver element commanders. They are out there, they are fighters. And the others, everybody else is a staff supporter. And information technology and information security is a staff function. It is a very important one, but it is still a staff function. And by doing the centralization that we have done and by empowering the CIO,

which I have done—and for some reason it was never done, but I have done it—I have by directive given him not just the responsibility, but the delegated authority commensurate with his responsibilities to manage IT as an Assistant Secretary. And so I do not think it is necessary.

Senator THUNE. Mr. Opfer, are there any other agencies that you are aware of that are doing a good job in the information security—I am sorry—that have—you know, in terms of the way they go about this? I guess what I am asking is, in the Government—and I realize each agency has unique needs and you have got different database requirements and everything else. But are there similarities or differences between the way the VA does and other agencies do it? And are there things that other agencies are doing that we could learn from and perhaps implement?

Mr. OPFER. Senator, I think we would need to look at some of the agencies that have gotten good marks on the FISMA reports, for example. That would be mostly in IT security and the financial statements, I know some of the ones that come to mind to me would be the Social Security Administration; the Department of Education had problems over the years; they have done a very good job in correcting them and the Department of Labor.

We just recently brought on board the new Deputy Assistant Inspector General in our office. The individual is considered an IT security expert who helped create the program for reviews in the Department of Education. And I think he will help in our role to assist the Department in going along with that. But I think we can look at other agencies. It is not exactly a layover, but look at some of the problems they have had and how they have addressed it. But a lot of it is really making sure that we hold people accountable and have policies and procedures in effect. And we have to realize that we are living in a digital age, and this is constantly evolving. And if we get the policies and procedures in place, we cannot say we have accomplished our mission. We have to review them. Are they still protecting us with the possible threat that we have now?

Senator THUNE. Do you contemplate in your analysis when you do these sorts of reports some of the things that are happening in other agencies? Do you incorporate that?

Mr. OPFER. Yes, we do. I have actually been requested by some of the other Inspectors General and other Departments' Deputy Secretaries, when it is appropriate, to give lessons learned from our perspective, and I have already accepted to go and do that. And the President's Council on Integrity and Efficiency has asked us—they have what they call an IT Roundtable for all the Inspectors General, and we will put on a presentation of what we have learned from our review, and this is to the other IGs of the agencies.

Senator THUNE. Very good.

Thank you, Mr. Chairman.

Chairman CRAIG. Senator Thune, thank you very much.

Well, Mr. Secretary, General Opfer, thank you for your time before the Committee today. I think this hearing was important not just for our record, but for any article or information that may flow from it as to where we are in this very important time and process as we work with you to transform VA into, I hope, a successful and recognizable system that develops the kind of integrity we need in

information and intelligence flow within the agency itself. So remember our goal, Mr. Secretary.

Secretary NICHOLSON. Yes, sir.

Chairman CRAIG. Thank you.

The Committee is adjourned.

[Whereupon, at 11:34 a.m., the Committee was adjourned.]

A P P E N D I X

The Best Medical Care In the U.S.

How Veterans Affairs transformed itself—and what it means for the rest of us

BY CATHERINE ARNST

RAYMOND B. ROEMER, 83, has earned his membership in "the greatest generation." A flight engineer during World War II, his B-24 was shot down over Potsdam during a bombing run. He managed to parachute out, but the jump landed him in enemy territory. Roemer spent 11 months in a German POW camp until he was liberated by General George S. Patton's troops in April, 1945.

A month later he came home to Buffalo with a Purple Heart and a few crushed vertebrae from that parachute jump. He married his high school sweetheart, started a successful metal-fabricating business, and signed up for health benefits with Blue Cross/Blue Shield. He can afford to be treated at any of some 20 well-regarded hospitals in the area, but Roemer has made what what may seem a bizarre choice. He goes to the Veterans Affairs Medical Center in Buffalo, a hulking, gray edifice first opened in 1950. He doesn't go just for his service-related injuries, either. His primary care doctor is at the VA, he fills his prescriptions there, and he uses the hospital for his vision and hearing needs. He even persuaded his 59-year-old son and business partner, Nicholas, a Vietnam War vet, to enroll with the VA.

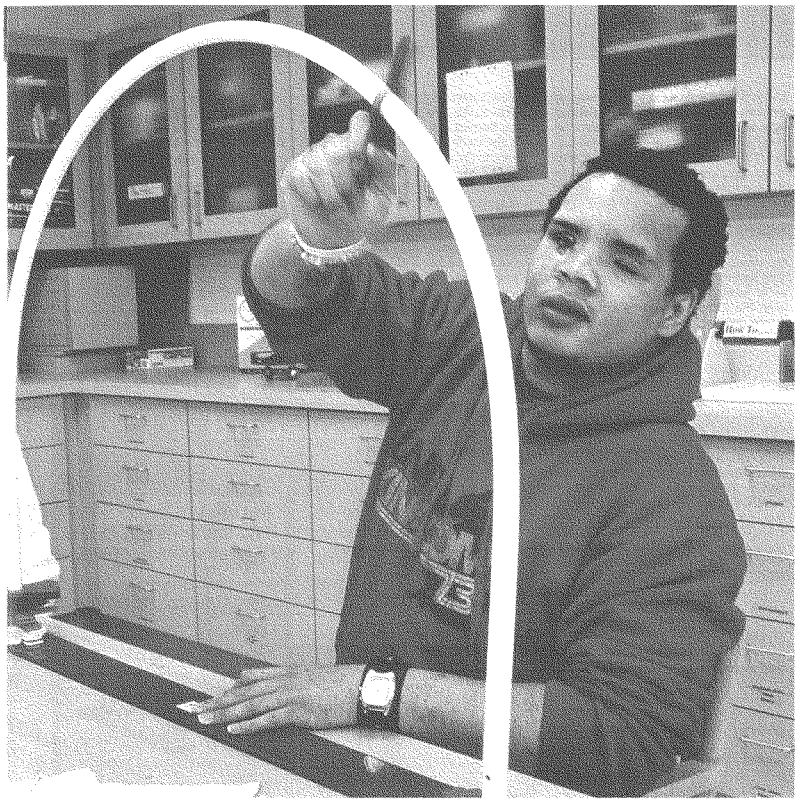
Every day some 1,400 patients pass through the Buffalo VA's unprepossessing entrance, into what many might assume is a hellish health-care world, understaffed, underfunded, and uncaring. They couldn't be more wrong. According to the nation's hospital-accreditation panel, the VA outpaces every other hospital in the Buffalo region. "The care here is excellent," says Roemer. "I couldn't be happier, and my friends in the POW group I belong to all feel the same."

LOWER COSTS, HIGHER QUALITY

ROEMER SEEMS TO HAVE stepped through the looking glass into an alternative universe, one where a nationwide health system that is run and financed by the federal government provides the best medical care in America. But it's true—if you want to be sure of top-notch care, join the military. The 154 hospitals and 875 clinics run by the Veterans Affairs Dept. have been ranked best-in-class by a number of independent groups on a broad range of measures, from chronic care to heart disease treatment to percentage of members who receive flu shots. It offers all the same services, and sometimes more, than private sector providers.

According to a Rand Corp. study, the VA system provides two-thirds of the care recommended by such standards bodies as the Agency for Healthcare Research & Quality. Far from perfect, granted—but the nation's private-sector hospitals provide only 50%. And while studies show that 3% to 8% of the nation's prescriptions are filled erroneously, the VA's prescription accuracy rate is greater than 99.997%, a level most hospitals only dream about. That's

Because the VA treats patients for life, it has an incentive to invest in **preventive care,** reaping the benefit of lower long-term costs. And its **advanced patient-records database** has nearly eliminated drug errors



CURT CAMPBELL/VA

largely because the VA has by far the most advanced computerized medical-records system in the U.S. And for the past six years the VA has outranked private-sector hospitals on patient satisfaction in an annual consumer survey conducted by the National Quality Research Center at the University of Michigan. This keeps happening despite the fact that the VA spends an average of $5,000 per patient, vs. the national average of $6,300.

To much of the public, though, the VA's image is hobbled by its inglorious past. For decades the VA was the health-care system of last resort. The movies *Coming Home* (1978), *Born on the Fourth of July* (1989), and *Article 99* (1992) immortalized VA hospitals as festering sinkholes of substandard care. The filmmakers didn't exaggerate. In an infamous incident in 1992, the bodies of two patients were found on the grounds of a VA hospital in Virginia months after they had gone missing. The huge system had deteriorated so badly by the early '90s that Congress considered disbanding it.

Instead, the VA was reinvented in every way possible. In the mid-1990s, Dr. Kenneth W. Kizer, then the VA's Health Under Secretary, installed the most extensive electronic medical-records system in the U.S. Kizer also decentralized decision-making, closed underused hospitals, reallocated resources, and most critically, instituted a culture of accountability and quality measurements. "Our whole motivation was to make the system work for the patient," says Kizer, now director of the National Quality Forum, a nonprofit dedicated to improving health care. "We did a top-to-bottom makeover with that goal always in mind."

AFTER IRAQ Therapist Daniela Lita with vet Poole, who is recovering from injuries suffered in a roadside bomb attack

Keeping that goal in sight will be challenging as more and more Iraq vets come

home. Some Sunbelt facilities are already overcrowded as the veterans' population ages and moves south. Much also depends on the amount of money Washington is willing to allocate to veterans' care. Kizer complains that budget allocations did not keep pace with inflation for the entire five years he was at the VA.

MIGHTY FORCE FOR CHANGE

THE VA'S RADICAL overhaul has caught the attention of health-care policy wonks, who have in turn sung the system's praises in prestigious medical journals. Last year the Canadian journal *HealthcarePapers* devoted an entire issue to the lessons other systems can take from the VA's transformation.

The biggest lesson? A nationwide health-care network that gets its funding from a single payer can institute mighty changes. Proponents of national health-care reform extrapolate even further. "The VA proves that you can get better results with an integrated, organized, national health-care system," says Dr. Lucian Leape, a professor at the Harvard School of Public Health and a leading expert on hospital safety. "We will not achieve even close to the level of quality and safety we need [in the U.S.] as long as we have individual practitioners and hospitals doing individual things."

The VA is, in many ways, the exact opposite of America's fragmented private-sector system, where doctors work for hospitals as independent contractors, and third-party insurers pay the bills as they see fit. By far the largest health-care network in the U.S., the VA serves 5.4 million patients—double the number it treated 10 years ago. All veterans are eligible for free or low-cost care, paid for out of the federal budget. The 2006 allocation comes to $35 billion.

Not having to rely on piecemeal insurance payments means the VA can finance large-scale improvements such as the electronic medical-records system, up and running in all of its facilities since 2000. In contrast, only some 20% of civilian hospitals have computerized their patient records. Because the VA is a nationwide health-care system, its electronic network is national, which means all of its facilities can share data. When hospitals were evacuated from New Orleans during Hurricane Katrina, the VA's patients were the only ones whose medical records could be accessed immediately anywhere in the country.

The VA's charter also confers some unique advantages. Because it treats patients throughout their lives, it can invest in prevention and primary care, knowing it will reap the benefits of lower long-term costs. Because the government pays the bills, the VA doesn't have to waste time or money on claims-related paperwork. Unlike Medicare, the VA is allowed to negotiate prices with drug companies and other suppliers, and it uses that power aggressively. The consumer group Families USA estimates that Medicare Part D enrollees, on average, pay 46% more than the VA for the same drugs.

The VA also gets to keep any money it saves through cost efficiencies. In the private sector the savings flow back to whoever is paying the bills. And because its doctors are salaried employees, the VA can implement systemwide changes without having to persuade outside doctors to go along. That doesn't mean it's settling for second-rate physicians. Among the VA staff is a Nobel prize winner, and clinical research is conducted throughout the system. The Buffalo VA recently hired one of the city's top surgeons, Dr. Miguel A. Rainstein, as chief of surgery. He had spent 26 years in private practice, where, he concedes, he made a lot more money, but he was ready for a lifestyle change. "I feel the VA has always gotten a bad rap. They have an excellent medical staff here, in surgery and in specialties."

The staff is happier, too, since much of the bureaucracy that once hobbled the organization has been streamlined. Kizer ended Washington's centralized decision-making and set up a military-like organization of 22 regional divisions. And doctors don't have to worry as much

Winning Scorecard

Hospitals in the Veterans Affairs system outpace those in the private sector by many measures

QUALITY of Care

The latest Rand Corp. study found that VA patients, on average, received about two-thirds of the care recommended by national standards, compared with just half for patients at a sample of the nation's other hospitals. Here's the breakdown:

HEALTH INDICATOR	VA SCORE	NATIONAL SAMPLE
Overall	67%	51%
Chronic care	72	59
Lung disease	69	59
Heart disease	73	70
Depression	80	62
Diabetes	70	47
Hypertension	78	65
High cholesterol	64	53
Osteoarthritis	65	57
Preventive care	64	44
Acute care	53	55
Screening	68	46
Diagnosis	73	61
Treatment	56	41
Follow-up	73	58

*SOURCE: VA patients. **PRO patients at non-VA hospitals.
Data: Rand Corp.; Agency for Healthcare Research & Quality

Patient SATISFACTION

For the sixth year in a row, veterans in 2005 were happier than other patients with their health care.

	VA	PRIVATE SECTOR
Inpatient	83*	73
Outpatient	80	75

*Out of 100. Data: American Customer Satisfaction Index

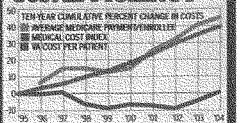
TECHNOLOGY Use

The VA has the most advanced electronic-records system in the U.S.

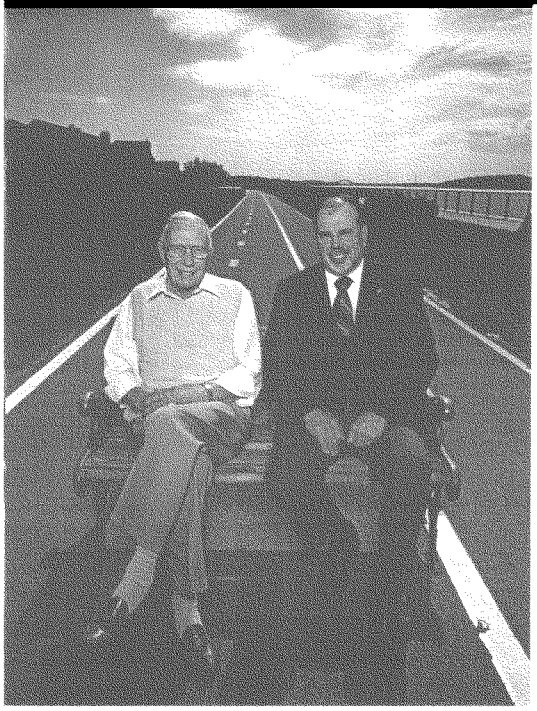
	PERCENTAGE OF HOSPITALS WITH ADVANCED ELECTRONIC RECORDS
VA	94%
Academic medical centers	30
Nationwide	8

Data: Commonwealth Foundation

Cost EFFICIENCY



Data: VA; Health & Human Services; Bureau of Labor Statistics



CHRIS CRISMAN

FATHER AND SON Ray and Nick Roemer can afford private doctors but choose the VA

happening in our hospitals." VistA is a big reason why the VA has held its costs per patient steady over the past 10 years despite double-digit inflation in health-care prices.

VistA has also turned out be a powerful force for quality control. The VA uses the data gathered in its computers to pinpoint problem areas, such as medication errors. The network also allows it to track how closely the medical staff is following evidence-based treatment and monitor deficiencies. Such tracking pays off. When Rand did an extensive study comparing quality of care at the VA with private-sector hospitals, it found that performance measurement played an important role in helping the VA score higher in every category except acute care, where it came in about even.

All of these changes are evident at the Buffalo VA. The patients in its waiting rooms hint at the hospital's special mission—a mixture of frail old men, Vietnam

> "The care here is excellent. **I couldn't be happier,** and my friends in the POW group I belong to all feel the same"
>
> *–Raymond Roemer, World War II vet*

about malpractice lawsuits, since government agencies are somewhat protected. That made it easier for the VA to go out on a limb in 2005 and institute a systemwide policy of apologizing to patients for medical errors—an act of contrition rarely done in the private sector. "Most families just want to hear an apology when a mistake is made," says Dr. Jonathan B. Perlin, Kizer's successor as Under Secretary for Health.

The "Sorry Now" program, as it's called, is an extension of Kizer's plan to transform the VA from an unaccountable bureaucracy into a transparent system that constantly seeks to improve care. "They've adopted a culture of patient safety and quality that is pervasive," says Karen Davis, president of Commonwealth Fund, which studies health-care issues.

The centerpiece of that culture is VistA, the VA's much praised electronic medical-records system. Every office visit, prescription, and medical procedure is recorded in its database, allowing doctors and nurses to update themselves on a patient's status with just a few keystrokes. In 1995, patient records at VA hospitals were available at the time of a clinical encounter only 60% of the time. Today they are 100% available. Some 96% of all prescriptions and medical orders, such as lab tests, are now entered electronically. The national comparison is more like 8%. "One out of five tests in a civilian hospital have to be repeated because the paper results are lost," says Veterans Affairs Secretary R. James Nicholson. "That's not

era vets with ponytails and tattoos, and a scattering of young, clean-cut guys recently back from Iraq. The few women are usually wives since only 7% of veterans are female. A nurse meets with each patient on arrival, updating electronic records so that the doctor can get up to speed immediately. (Patients can also access their own records if they want, a rare option in most medical-records systems.)

At the hospital pharmacy, prescriptions are doled out by robotic devices—one reason the organization is able to hold copays at $8. Each bottle of medicine carries a bar code that is scanned by the computer. If a patient is allergic or takes a conflicting drug, the system will sound an alarm. Similar bar codes are affixed to patient ID bracelets to protect against the

wrong patient getting a procedure, a common mixup in hospitals. The bar code idea was thought up by a VA nurse in Topeka, Kan., who noticed that rental cars were checked in with portable bar code scanners and figured the same technology could be used in hospitals.

ELECTRONIC HOUSE CALLS

DR. JOHN SANDERSON, the Buffalo VA's director of medicine, clicks on to VistA as soon as he enters the clinic each morning to check the progress of his patients. Sanderson is a primary care doctor, so he plays point man in the team of specialists assigned to each vet according to the patient's needs. He meets with an elderly man with severe asthma, takes a quick look at his electronic records, and learns that the patient has not yet had a pneumonia shot. That's a big issue at the VA. The organization has cut hospitalizations by 4,000 patients a year since its pneumonia vaccination rate went from 29% in 1995 to 94% last year.

Sanderson also decides the patient needs to see a pulmonary specialist and arranges an appointment with one on the spot so the vet doesn't have to make a second trip. Such consideration for the patient is evident throughout the hospital. In every department of the giant building hangs a poster with the name, photo, and phone number of the supervisor, inviting patients to call with questions or complaints. The hospital is determined that no patient remain in the waiting room more than 15 minutes. Sanderson would like to get that down to five. After every outpatient visit and inpatient release, a staffer follows up with a call a few days later for feedback on the vet's experience and to make sure there are no problems.

Sanderson is able to spend more time with his patients because he spends less time record-keeping than his counterparts in private practice. That lets him focus on preventive care, and particularly diabetes prevention. Some 23% of the VA's patients have diabetes, and without close monitoring they can go on to develop a range of complications. The VA scored very high in the Rand study on diabetes care—70 out of 100, vs. 57 for the private sector. But to keep patients from developing diabetes in the first place, the VA offers overweight patients the opportunity to join a weight-management program that pairs them with a nutritionist. Few insurers will pay for such prevention in a civilian setting. To Sanderson, preventive care is just one reason he is sure the changes at the VA "have saved thousands of lives over the years."

Staffers in Buffalo embrace the hospital's high level of commitment to patient care in part because many of them are veterans themselves. Diane DiFrancesco, a nurse in the intensive-care unit, is also a flight nurse in the U.S. Air Force Reserve. Her husband, a pilot in the reserves, is on his third tour of duty in Iraq. She has been at the Buffalo VA since 1987, a longevity typical at the facility, where the annual turnover rate is half that of other area hospitals. "People here really want to help the vets," she says. "Once you get used to

PLAYBOOK: BEST-PRACTICE IDEAS

Medical MAKEOVER

The Veterans Affairs health network went from one of the worst in the nation to the best in just 10 years. It has some unique attributes that can't be duplicated at civilian hospitals. Still, other providers—and industries—can learn a lot from the military's rulebook.

HIRE LEADERS WHO LOVE A CHALLENGE When Dr. Ken Kizer became Health Under Secretary in 1994, Congress handed him a mandate to fix the VA, and he ran with it. "There was a universal consensus back then that if there was a single organization that couldn't be changed, it was the VA," he says. "I decided I would make this a model system, a case study for radical change." Kizer is often described as hard-nosed, abrasive, and brilliant. He got the job done in just five years. But Congress forced him out in '99.

ESTABLISH A CULTURE OF QUALITY Kizer decided from the outset that the VA would focus on quality of patient care above all. Every change, from the practice of medicine to the way prescriptions are filled, was redesigned with that goal in mind. "Culture of quality" is not just a meaningless slogan at the VA. Practices and outcomes are evaluated constantly, and staffers throughout the system meet regularly to discuss ways to improve patient care.

IT'S THE TECHNOLOGY, STUPID The VA has by far the most advanced electronic medical-records (EMR) system in the U.S., called VistA. Every one of the VA's facilities is linked to the national database, and every patient protocol and interaction is recorded. The resulting efficiencies and error reductions have more than covered the cost of implementing VistA. Also, the VA now has the data in hand to determine how well it is meeting its quality benchmarks.

it here, it's hard to work anywhere else."

This Band of Brothers mentality goes a long way toward attracting and keeping the VA's unique group of patients. "I've never been very comfortable in hospitals, but I like the idea that the patients here and I have something in common," says Nick Roemer, Ray's son, who first used the Buffalo VA three years ago when he hurt his wrists. He has private insurance but figured it would be cheaper and faster to come to his father's caregiver. "You can talk to people here. They're like you."

The VA's mission brings with it some special burdens, however. Its patients are generally older, poorer, and sicker than those in civilian hospitals; there is also a higher prevalence of mental illness and addiction. And it has large numbers of patients with a malady that is much less common in civilian hospitals: post-traumatic stress disorder (PTSD).

It was the PTSD program that persuaded Steve to enter the fold. A 40-year-old police officer in the Buffalo area who asked that his last name not be used, Steve has been a sergeant in the reserves for 21 years, serving in Afghanistan, Bosnia, and Panama, and Iraq in 2004. When he returned from Iraq, he couldn't sleep and constantly felt anxious. He resisted visiting a VA facility because of negative impressions carried over from the early '90s, but he figured "a civilian doctor would have no clue. They don't understand where we're coming from." At the VA he felt he could be treated properly and comfortably. "To be honest, I don't want to bring it up with anyone outside the vet community." Now he's sending literature about the PTSD services to everyone in his unit who's still in Iraq.

"Once you get used to it here, it's hard to work anywhere else"

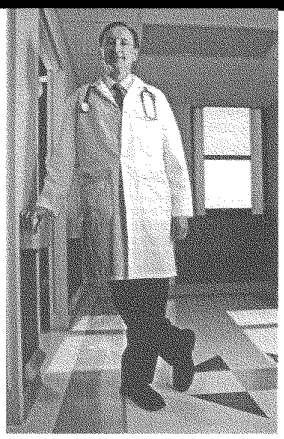
–Diane DiFrancesco, intensive-care nurse at the Buffalo VA Medical Center, where the staff turnover rate is half that of other local hospitals

Those returning vets are one of the biggest challenges looming for the VA. It recently reported that the number of PTSD cases has doubled since 2000, to an all-time high of 260,000. The Iraq war has also left vets with injuries that are horrendous even by wartime measures because battle field medicine can treat traumas that in past wars would have meant certain death. In World War II, there were two to three soldiers wounded for every one killed. In Iraq, 9 to 10 are wounded for each killed.

Marine Corporal Jason Poole, 23, is living proof of the improved chances of survival and the advanced medicine offered by the VA. The native of Bristol, England, now a U.S. citizen, was on his third tour in Iraq in 2004, 10 days shy of coming home, when his patrol was hit by a roadside bomb that left him in a coma for two months. Shrapnel went through his left ear and out his left eye. He was unable to walk, talk, or breathe without a tube. Treated at the brain trauma unit of the VA hospital in Palo Alto, Calif., one of four VA polytrauma clinics for the severely wounded, Poole has had nine reconstructive surgeries in two years. He still gets physical therapy, but he is now walking, talking, and taking classes at a community college. "I've been treated amazingly here," he says. "Everyone has been working so hard for me."

The VA is opening 22 more polytrauma clinics to care for the growing numbers of soldiers with severe injuries. Most will eventually be treated at standard hospitals like the one in Buffalo, and that could send the VA's costs skyrocketing.

It doesn't help that the VA must worry about getting shortchanged by Washington. President George W. Bush wants to hold down costs by raising eligibility requirements for vets. So far, Congress has rebuffed him. That doesn't mean Capitol Hill is always on the VA's side, though. Kizer, the turnaround's architect, was forced out in 1999 when Congress refused to reconfirm him after he closed hospitals in key districts. Dr. Dennis S. O'Leary, president of the Joint Commission on Accreditation of Healthcare Organizations, praises Nicholson and Perlin for sticking with Kizer's reforms. But he warns that "the most common reason hospitals go into the tank is a change in leadership." Since the VA is as affected by politics as any other federal entity, that will always be a concern, he says.



"Thousands of lives" have been saved by the VA's focus on preventive care

–Dr. John Sanderson, director of medicine at the Buffalo VA

It's not a concern yet, and civilians are taking notice of the military way of medicine, with some hospitals using versions of VistA. The VA's other advantages may not be as easy to adapt, but as Harvard's Leape says, "the VA is a dramatic example of what can happen if you have the will and the leadership to make change happen." ■

CHRIS GRIMAN