HOW SECURE IS PRIVATE MEDICAL INFORMATION? A REVIEW OF COMPUTER SECURITY AT THE HEALTH CARE FINANCING ADMINISTRATION AND ITS MEDICARE CONTRACTORS

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MAY 23, 2001

Serial No. 107–29

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

72–833CC WASHINGTON : 2001

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 ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

JAMES C. GREENWOOD, Pennsylvania, *Chairman*

MICHAEL BILIRAKIS, Florida
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
Vice Chairman
CHARLES F. BASS, New Hampshire
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

PETER DEUTSCH, Florida
BART STUPAK, Michigan
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
CHRISTOPHER JOHN, Louisiana
BOBBY L. RUSH, Illinois
JOHN D. DINGELL, Michigan,
(Ex Officio)

(II)

CONTENTS

	Page
Testimony of:	
Adair, Jared, Acting Chief Information Officer, Health Care Financing Administration, accompanied by John Van Walker, Senior Advisor for Technology to CIO and Julie Boughn, Director, Division of HCFA Enterprise Standards	9
Neuman, Michael, President and Lead Programmer, En Garde Systems, Incorporated	18
Vengrin, Joseph E., Assistant Inspector General for Audit Operations and Financial Statement Activities, accompanied by Ed Meyers, Director, Information Technology Systems, Office of Inspector General	13
Material submitted for the record:	
Documents referenced during hearing	40

(III)

HOW SECURE IS PRIVATE MEDICAL INFORMATION? A REVIEW OF COMPUTER SECURITY AT THE HEALTH CARE FINANCING ADMINISTRATION AND ITS MEDICARE CONTRACTORS

WEDNESDAY, MAY 23, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m. in room 2322, Rayburn House Office Building, Hon. James C. Greenwood (chairman) presiding.

Members present: Representatives Greenwood, Whitfield, and Tauzin (ex efficio).

Staff present: Amit Sachdev, majority counsel; Tom Dilenge, majority counsel; Gary Dionne, Congressional Fellow; Peter Kielty, legislative clerk; and Edith Holleman, minority counsel.

Mr. GREENWOOD. Good morning. I am James Greenwood, chairman of the subcommittee, and I apologize to our witnesses and to the rest of you for the delay. The chairman of the full committee, Mr. Tauzin, would like to join us. As if often the case, another subcommittee is having a hearing, and he is giving his opening statement at that hearing and should be with us in a few minutes. So if you will—just ask your forbearance for another few minutes, we will commence then.

[Brief recess.]

Mr. GREENWOOD. Well, we are informed that the chairman is on his way, so we will begin. Our hearing will come to order.

Good morning. When Americans think about the future, their greatest concern, according to a recent Wall Street Journal/NBC News survey, is protecting their privacy. What is particularly interesting about this discovery is that America's concern for privacy is greater than concerns about such critical issues as overpopulation, global warming, and even nuclear war. And when it comes to the privacy of health data the findings are even more startling.

Another recent survey has found that one in five Americans believes his health data has been used inappropriately. And one in six have altered their behavior to avoid the misuse of information, even to the point of avoiding necessary medical care.

If we are to address the nagging concerns of our fellow citizens with regard to the privacy of their medical records, then our standards must be very high indeed. Like Caesar's wife, the security of

our Nation's private health records must be above suspicion. It is in the light of these and some disturbing findings that we, in this subcommittee, gathered today to examine this issue, particularly as it affects the tens of millions of elderly and disabled Americans who rely on the Federal Medicare Program.

The question posed today is how secure is the very sensitive and private medical information gathered by the Health Care Financing Administration, better known as HCFA, and its dozens of fiscal intermediaries and carriers who process literally billions of Medicare claims every year?

To begin to answer this question, several months ago I requested that HCFA provide this subcommittee with information and documentation relating to computer security, including all penetration tests or vulnerability audits that have been conducted on its various networks in the past 5 years. Committee staff also met with senior managers at HCFA on a number of occasions since then to review the information provided and to ask follow-up questions.

Before discussing our findings, I want to start by providing some important background and context. HCFA processes and pays more than $170 billion annually in claims for Medicare health benefits, using a large and complex computer network that links health providers, such as nursing homes and hospitals, with billing clearinghouses, fiscal intermediaries, and carriers.

Using a private dial-up telecommunications network provided by AT&T, and provided by IBM prior to mid-1999, known as the Medicare Data Communications Network, or MDCN, Medicare contractors process standard Medicare claims that contain personally identifiable medical information, such as names, addresses, treatment, and diagnosis codes and payment and insurance data.

This sensitive information traverses the MDCN in order to be linked with necessary data bases of information contained by HCFA and its contractors, including beneficiary claim histories, eligibility data, such as social security numbers, and other information stored in HCFA's Common Working File, known as CWF. This computing network has over 75,000 authorized users. And while it is a private-line network, it has connectivity with other HCFA systems that are accessible via the Internet. In addition, AT&T uses this private-line network to provide similar services to roughly 35,000 customers worldwide, including banks, insurance companies, health care companies, and other Government agencies.

Much of what we have learned so far is good news. Compared to many of its fellow agencies in the Federal Government, HCFA has taken a much more proactive approach to cyber security, particularly in the last 2 years. HCFA has conducted numerous tests of its own systems, including penetration tests from both inside and outside of the network. HCFA generally has limited its Internet connections to reduce the possibility of outside attack, and last year reconfigured those connections to further minimize the chance of unauthorized intrusions after a team of hired experts successfully penetrated its so-called secure network via the Internet.

HCFA also is in the process of upgrading its internal systems to reduce the systemic vulnerabilities in its desktop operations, which should be complete by the end of this fiscal year. Moreover, HCFA recently embarked upon an initiative to review and upgrade the se-

curity of its Medicare contractors to ensure compliance with current Federal requirements, something that has not been done in a comprehensive manner in a very long time.

The subcommittee has just begun to look at these contractor systems and will continue to monitor HCFA's efforts to improve their overall security. I also should point out that the new Secretary of the Department of Health and Human Services has made improved computer security at HCFA a top priority and has proposed a new $30 million fund to help pay for it.

HCFA and several of its Medicare contractors also have reported to this committee that they are unaware of any significant intrusions into their systems by unauthorized individuals, which is surely good news, although it is important to keep in mind that there could have been intrusions that went undetected, as was the case with several of the intrusions perpetrated by the ethical hackers hired by HCFA and the Inspector General, which we will talk about today.

The news, however, is not all good. Audit after audit, even the most recent, continue to reveal significant computer security problems at HCFA and its Medicare contractors, vulnerabilities that continue to place personally identifiable medical information at risk of unauthorized access, disclosure, misuse or destruction. While much has been done to limit the possibility of the truly outside attack by the World Wide Web, this threat still exists, as several of our witnesses today will describe.

For example, in 1999, HCFA issued a contract to En Garde Systems to conduct ethical hacking in the form of external penetration tests to determine whether the MDCN was secure from attacks from hackers on the Internet. I am pleased that En Garde Systems is before the subcommittee today as a witness, and I am releasing a redacted version of the 1999 test results. In that test, En Garde was easily able to exploit a vulnerability in HCFA's web site to get access to the MDCN and then HCFA's internal computer network.

This was rightly viewed as a serious security breach, and at that time En Garde recommended that HCFA reconfigure its computers to discontinue the linkage between the Internet and the secured, private MDCN, the connection that HCFA used to load information onto its web sites. While HCFA made some changes to address this vulnerability at that time, the agency did not follow through on the major En Garde recommendation until pressed by this committee, informing us just yesterday that it has disconnected this particular Internet connection. While that certainly is progress, still more must be done to reduce the risks imposed by external sources.

In addition, the threat from internal sources is great and includes the 75,000 employees of HCFA, its contractors, and certain nursing homes that have authorized access to the Medicare Transaction Network. More must be done and soon to minimize this risk as well. HCFA must improve the basics of security management. It lacks complete security plans, risk assessments, and accreditations for many of its major systems and applications. It fails to enforce strong passwords through the use of available automated tools and fails to block its own employees from downloading Internet hacker tools that could be used to exploit the known

vulnerabilities in its internal systems, as two separate auditors did in tests conducted over the past year.

I was pleased to learn just yesterday that the Department of Health and Human Services, which oversees HCFA, plans to issue for comment a new policy shortly, at our urging, that will require its operating divisions to regularly scan their systems for weak passwords, something that CDC, for example, already has been doing but that HCFA does not currently do.

HCFA has also failed, in my opinion, to implement an adequate testing regime to ensure the security of the Medicare system. While many audits and penetration tests have been done over the years, the restrictions imposed by HCFA on both the scope and nature of these tests limit their overall effectiveness in evaluating the real security posture of the agency's various systems and networks.

For example, ever since a 1997 penetration test conducted by the IG's auditors resulted in the penetration of HCFA's mainframe in the altering of Medicare payment information, HCFA has refused to permit the IG's auditors to conduct similar in-depth testing. In addition, HCFA oftentimes has been slow to implement needed corrective actions following poor test results, and has not consistently tested the efficacy of the corrective actions once implemented.

HCFA also needs to do a better job overseeing its Medicare contractors, as well as those contractors such as IBM and AT&T that provide critical network services utilized by HCFA and its business partners. For too long, it would appear, HCFA has allowed these contractors to essentially assess themselves without sufficiently rigorous independent testing.

The committee's review has found only one set of penetration tests ordered by HCFA back in 1998 and covering just four of HCFA's more than 55 Medicare contractors. Since that time, and despite some significant findings, HCFA has not conducted further tests of its contractors, leaving that task to the Department's Office of Inspector General, which conducts annual assessments of financial controls at HCFA and its major Medicare contractors. But these IG audits, as the IG notes in its testimony today, are fairly low-level tests due to restrictions imposed upon them and are not meant to really test the adequacy of computer security.

Even so, in every year since 1996, the IG has identified computer security controls to be a, "material weakness" at both HCFA's Central Office and its Medicare contractors. HCFA either needs to step up its own testing of these contractors or work to ensure that the IG is permitted to conduct full-scale testing of these contractor systems.

I am also concerned that HCFA has not yet insisted that AT&T and IBM, which respectively run the private network upon which the MDCN runs and the HCFA web servers, agree to a thorough testing of the interconnectivity between these networks, HCFA, and the Internet and between the more than 35,000 AT&T customers that utilize the private network in addition to HCFA.

Clearly, HCFA has dragged its feet when it comes to assuring the security of these systems. Back in 1998, En Garde Systems sensibly recommended that HCFA conduct several distinct tests of those systems to evaluate their security given the incredible trust HCFA places upon them. Two and a half years later, only one of

these tests has been conducted, and despite identifying serious problems, no further testing has been done. As the committee found, neither HCFA nor AT&T has yet tested the security of the MDCN to determine whether one HCFA partner could gain unauthorized access to HCFA internal systems via the MDCN connection or whether one of AT&T's 35,000 other customers that utilize this same network could do the same.

Oral assurances are one thing, test results are another. So how secure is confidential and personal Medicare information? Clearly, it is not secure enough. While HCFA is to be commended on its success in making its data more secure than many other types of sensitive data collected by the Federal Government, it is less secure than it can or should be.

Accordingly, today I call upon HCFA to take the following actions: One, HCFA must step up its efforts to implement the outstanding corrective actions necessary to address known vulnerabilities in its own systems; two, HCFA must demand that its contractors submit to independent testing of their systems, including those test of the AT&T and IBM networks that were recommended more than 2½ years ago; three, HCFA must aggressively carry out its plan to review and upgrade the security of its Medicare contractors and be prepared to fund needed corrective actions; four, HCFA must build into its security management a more regular and vigorous process of scanning its networks for vulnerabilities, improve configurations, and weak passwords; and five, HCFA must quickly evaluate the security of its remote access and dial-up capabilities and enhance that security where necessary. I understand the contract for these services is about to expire, and it is my strong recommendation that the new contract reflect these recommendations.

I look forward to working with HCFA, this new Administration, and with members on both sides of the aisle to improve the protection afforded to this highly personal information of Medicare beneficiaries. When it comes to such sensitive data, we can never be too vigilant.

I will now recognize the chairman of the full committee, Mr. Tauzin, for his opening statement.

Chairman TAUZIN. Thank you, Mr. Chairman. First, let me assure the witnesses today and our guests that the lack of attendance of members at this hearing should not be taken as any sign of a lack of interest in this important subject. There is an important hearing going on downstairs on the issue of online fraud, which is very similar, in some respects, to our concerns as regards the issues of security of the HCFA systems. And there are other distractions, such as that occurring on the Senate today, that is occupying quite a few members this morning, as everybody considers fallout from what might happen this afternoon.

But I can assure there is huge interest and support for you, Mr. Chairman, and this inquiry among the committee members on both sides of the aisle. And I want to join you in the list of recommendations you have made today to HCFA. The protection of privacy and private information in the HCFA systems is a critical issue. It is not only critical for the security of those funds and those systems, which are critical to many millions of older Americans and ill

Americans, it is also equally critical in terms of the privacy rights of Americans whose sensitive medical histories, medical treatments, and medical information can be at risk.

We recently held hearings with the Secretary of the health agency regarding the ongoing decisions regarding health insurance—health information, rather, privacy. And those privacy rules are currently under review to make sure that we get them right. It will do little good for us to have privacy rules at a health agency and privacy laws in general if the Internet and computer systems that contain those data banks and upon which that information is moved is available to hackers and intruders and people who would create mischief with that information. It is critical that this hearing continue to produce oversight, the kind of extraordinary and sensitive, constant review and attention to the questions of privacy in these systems.

Last month, the subcommittee held a hearing that showed just how easily it was for Federal computer systems to be penetrated by hackers. At that hearing, we saw first hand just how easily a team of 20-something ethical hackers could, in minutes, hack into Government computers, crack passwords, and escalate their privileges to allow them not only to get into a computer system but to take control of it and to take control of entire computer networks. That was one frightening hearing. I hope those of you who are here today, if you were not present for that hearing, will go back and read some of the testimony given that day.

Anybody watching how easily those hackers got into those systems and controlled those systems and what they said they could do once they controlled them, how they could take control, for example, of the microphones and record any conversations in the room where the computer is located. If you had a camera on your computer, how they could take control of the camera and actually view anything going on in the room where the computer is located. Anybody who saw that demonstration had to be extraordinarily concerned about the security of systems where sensitive, private information is stored and transmitted.

Today's hearing will continue our investigation into Federal computer security and will highlight the results of the committee's review of the Health Care Financing Administration, or HCFA. Like Chairman Greenwood, I am pleased, first of all, to learn that HCFA is doing a better job than many other agencies in working to address computer security vulnerabilities. But let us be honest, HCFA has to do a better job than most other Federal agencies. The information is much more sensitive than many other Federal agencies.

And the information you have backs up a Federal support system that is critical to the health care of millions of Americans—our own moms and dads and grandparents and aunts and uncles and soon brothers and sisters and ourselves. And we can't permit HCFA to have anything less than the best when it comes to security in these systems.

Now, the bottom line is that it is not going to be enough for HCFA to make sure its own systems are properly protected, because oversight testing of Medicare contractors and their systems are equally important. It is not enough to say that HCFA can take

the assurances of IBM and AT&T that their systems are secure. We need to know that they have been tested, and we need to know that HCFA is taking great steps to make sure that those assurances are real. It is not that we think that contractors are incompetent or deceptive; it is simply we cannot and should not take anybody's word for it. If you are going to contract with separate systems to carry this data and to help administer the program, the Government agency has an obligation that it cannot waiver from in its self-knowing that those systems are secure, not taking anybody's word for it.

So I want to strongly encourage you to go much further in this area than you have gone so far. And I want to congratulate Chairman Greenwood for the very clear successes that his investigation has already produced in terms of pressing the Department and HCFA to make certain improvements in the management of security at HCFA prior to this hearing today.

I don't think, Mr. Chairman, this subcommittee can rest until you and I and members can stand before any camera in America and say that we are personally satisfied the medical information of our constituents is adequately protected and that the systems that back up the health security of our families is adequately protected and that the solvency and financial security of those funds is not threatened by hackers, whom we saw in this room, given the chance, that come in and totally destroy sanctity and solvency of those funds. Now, until we can personally do that, until you have done your job to personally assure yourselves of that and satisfied us that it is also true, this committee has to keep up its vigilant attention on this issue.

Thank you, Mr. Chairman.

[The prepared statement of Hon. W.J. "Billy" Tauzin follows:]

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Mr. Chairman, and let me commend you for holding this very timely hearing on a topic of such great importance to the American people—the protection of their privacy and their private information.

Due in part to the Internet, Americans today are paying greater attention to privacy protections. But I don't think that many people realize the extent to which the ongoing debate over *privacy* is so closely related to the issue of *computer security*. That is one reason why this Committee has been conducting an investigation into the adequacy of Federal efforts to protect our nation's cyber infrastructure and the vast amounts of sensitive data stored on Federal computers.

Last month, the Subcommittee held a hearing that showed just how easily Federal computer systems could be penetrated by hackers. At that hearing, we saw first hand just how easily a team of 20-something "ethical hackers" could, in minutes, hack into government computers, crack passwords, and escalate their privileges to allow them to get control of entire computer networks.

Today's hearing continues our investigation into Federal computer security and highlights the results of the Committee's review of the Health Care Financing Administration, or HCFA. Like Chairman Greenwood, I am pleased to learn that HCFA has been doing a better job than many other agencies in working to address computer security vulnerabilities. But HCFA is an agency that *must* do better than most agencies.

The security of the Medicare claims system is a matter that HCFA and all of us must take very seriously—for it is one of the most critical Federal assets, containing vast amounts of personally identifiable private medical information. And there is no doubt that HCFA can and must do better in this area. This hearing will explore the very real security vulnerabilities that face HCFA, and the serious management challenges the agency must address in order to properly secure the computer networks that make the Medicare claims system work.

Let me highlight just one of these issues, namely HCFA's failure to conduct sufficient oversight and testing of its Medicare contractors and the contractors such as IBM and AT&T that provide critical network services to HCFA. I share Chairman Greenwood's concerns that HCFA has not been aggressive enough in pushing these contractors to allow independent tests of their systems. In an area as sensitive as this one, we simply cannot take their assurances of security at face value—not because they are incompetent or deceptive, but simply because they may not be as secure as they would like to think.

I want to strongly encourage the agency to go further in this area, not just with respect to its contractors' networks, but also its own. Without rigorous, independent testing, we simply cannot assure the American people that their private medical information is indeed protected.

Finally, I want to congratulate Chairman Greenwood for the clear successes this investigation already has produced in terms of pressing the Department and HCFA to make certain improvements to the management of security at HCFA prior to this hearing today.

I look forward to the testimony from our witnesses today, and continuing to work with HCFA and this Committee as it works to address these concerns.

Mr. GREENWOOD. I thank the chairman for his opening statement and welcome the witnesses. There is an amendment to our witness list. Ms. Michael McMullan, the Acting Deputy Administrator of HCFA will not be testifying, but we do welcome Ms. Jared Adair, the Acting Chief Information Officer of the Health Care Financing Administration. She is accompanied by Mr. John Van Walker, the Senior Advisor for Technology to the HCFA CIO, and Julie Boughn, Director of the Division of HCFA Enterprise Standards.

We are also pleased to have with us, Mr. Michael Neuman, president and lead programmer of En Garde Systems, Incorporated, as well as Mr. Joseph Vengrin, Assistant Inspector General for Audit Operations and Financial Statement Activities, who is accompanied by Mr. Ed Meyers, Director, Information Technology Systems of the Office of Inspector General at the Department of Health and Human Services.

Welcome to all of you. You are, I believe, aware that the committee is holding an investigative hearing, and when doing so has had the practice of taking testimony under oath. Do you any of you have objections to testifying under oath?

Seeing none, the Chair then advises you that under the rules of the House and the rules of the committee you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony?

In that case, would you please rise and raise your right hand, and I will swear you in.

[Witnesses sworn.]

Mr. GREENWOOD. Thank you. You may be seated. You are now under oath. And we would like to proceed, I believe, beginning with an opening statement from Ms. Adair for 5 minutes. Welcome.

TESTIMONY OF JARED ADAIR, ACTING CHIEF INFORMATION OFFICER, HEALTH CARE FINANCING ADMINISTRATION, ACCOMPANIED BY JOHN VAN WALKER, SENIOR ADVISOR FOR TECHNOLOGY TO CIO AND JULIE BOUGHN, DIRECTOR, DIVISION OF HCFA ENTERPRISE STANDARDS; JOSEPH E. VENGRIN, ASSISTANT INSPECTOR GENERAL FOR AUDIT OPERATIONS AND FINANCIAL STATEMENT ACTIVITIES, ACCOMPANIED BY ED MEYERS, DIRECTOR, INFORMATION TECHNOLOGY SYSTEMS, OFFICE OF INSPECTOR GENERAL; AND MICHAEL NEUMAN, PRESIDENT AND LEAD PROGRAMMER, EN GARDE SYSTEMS, INCORPORATED

Ms. ADAIR. Thank you.

Mr. GREENWOOD. Good morning.

Ms. ADAIR. Good morning. Chairman Tauzin, Chairman Greenwood, thank you for inviting us here today to discuss the Health Care Financing Administration's information security efforts. Protecting the confidential health information of the Americans who rely on our programs is a critically important responsibility. I assure you we take this duty seriously, and over the last few years we have made substantial improvement.

Beneficiary data are essential to carrying out Medicare's health insurance functions. These data allow us to determine if an individual is enrolled in Medicare and to determine whether a claim should be paid and how much to be paid. As custodians of these data, it is our job to ensure that proper safeguards are in place. Our beneficiaries deserve no less.

We face considerable security challenges due to Medicare's current, complex environment. The complexity of this environment is driven by the increasingly data-intensive nature of modern health care. And because our claims processing contractors are, by law, decentralized. We are proud in the history of the Medicare Program there have been no significant security or privacy breaches of Medicare systems, and there have been no substantial problems with breaches of confidential, beneficiary or provider data. Nevertheless, we remain vigilant in our efforts to protect beneficiary information.

We recognize that although perfect security is unattainable, we must constantly and rigorously improve our defenses. Even the smallest technological change can open us to new threats that cannot always be anticipated. We have worked proactively to identify, correct, and prevent problems. And I want to thank the Office of the Inspector General as well as the General Accounting Office for their assistance in highlighting areas where we can make improvements and in recommending solutions. Their work serves as an important road map for us as we work to improve security.

We have instituted a comprehensive system security program across our entire enterprise, and we continue to make great strides in improving security. For example, we became one of the first nonmilitary Federal agencies to initiate third-party penetration testing of our system. At our agency and at some of our claims processor contractors, we have used ethical hackers to test for potential vulnerabilities before someone actually seeking to do harm could discover them. In addition, we have been conservative in moving to new e-business technology to ensure that adequate protections are in place before using this kind of technology. And we do not share

confidential beneficiary information for marketing or commercial purposes.

We have established baseline security requirements for our claims processing contractors and are assessing how their security measures meet or exceed our requirements. These assessments will be valuable for future security planning. Internally we are improving processes for managing access to data to help ensure that only staff with a legitimate professional need have access to sensitive information and that the data are used appropriately. We look carefully at whether an employee's job entails need-to-know confidential information. Even our senior staff, including the Chief Information Officer and myself, cannot browse this information, because we do not have a need to know.

Additionally, we are increasing awareness of security to the entire agency and to our contractors, reminding them that bad habits, such as sharing passwords, could lead to unintended consequences. Beginning this summer, all HCFA staff will complete annual training on computer security.

We are working hard to protect confidential health data. Our goal is to create multi-layered security defenses that when taken together establish a solid security posture for our agency. We want to work with you and our partners to make sure that we protect this information and fulfill all of our responsibilities to our beneficiaries and the taxpayers.

Thank you for holding this hearing, and I will be happy to answer questions.

[The prepared statement of Jared Adair follows:]

PREPARED STATEMENT OF JARED ADAIR, DEPUTY CHIEF INFORMATION OFFICER, HEALTH CARE FINANCING ADMINISTRATION

Chairman Greenwood, Congressman Deutsch, other distinguished members of the Subcommittee, thank you for inviting me to discuss the Health Care Financing Administration's (HCFA) information technology security efforts and our plans for the future. Protecting the confidential health information of the Americans who rely on our programs is a critical responsibility, and we take this duty seriously. I appreciate the opportunity to share our efforts and plans with you.

Confidential data are essential to carry out many of our business functions. For example, to pay a Medicare claim, we must confirm the beneficiary's eligibility for Medicare benefits, obtain information about secondary payers, review the claims history, and perform other data-intensive activities. Similarly, for a Medicare managed care payment, we have to establish the beneficiary's enrollment, calculate the payment amount, and forward that amount to the plan. In addition, efforts to encourage high quality care require analysis of the treatments and complications that Medicare beneficiaries experience. As manager and custodian of this data, we have a legal and practical responsibility to assure that proper security safeguards are in place for maintaining confidentiality, integrity, and appropriate availability of this data. We take this responsibility seriously, and the public counts on us to do so.

This Committee and Congress recognized this when they passed the Government Information Security Reform Act, focusing attention across the government on information security concerns. While we have not yet experienced any significant breach of our systems' security, we remain vigilant in our efforts to protect beneficiary information. Our staff and partners like the Inspector General (IG) have identified security vulnerabilities within our systems, and we have taken appropriate steps to address them. I want to commend the IG, as well as the General Accounting Office (GAO) and others, for their assistance in highlighting these vulnerabilities and their recommendations for solutions. Their work serves as an important roadmap for us as we work to improve security across our Agency. Moreover, in our recent Chief Financial Officer Electronic Data Processing audit, the IG acknowledged that we have made progress with our security efforts. As a result of increasing use and changing technologies, the demands on our information technology architecture are

greater than ever before, and security risks continue to evolve. Clearly, we must continue to enhance and improve security in order to meet today's needs and tomorrow's challenges.

We recognize that although perfect security is unattainable, we must constantly and rigorously improve our defenses. As the technology we use in administering our programs has grown more complex, old threats have intensified and new security threats have emerged. Even the smallest technological change can open us to new threats, which cannot always be anticipated.

As the Deputy Director of HCFA's Office of Information Services and Deputy Chief Information Officer, I am acutely aware of our computer system security responsibilities. We have worked hard, especially in the past 5 years, to identify, correct, and prevent problems with the security of our computer systems. We have instituted a comprehensive and effective system security program across our entire enterprise, and we continue to make great strides in improving security both in our internal systems and the systems of our external business partners. We have greatly improved our security, and we have concrete plans to improve it further.

BACKGROUND

In the history of the Medicare program, there have been no significant security or privacy breaches with Medicare systems, nor have there been substantial problems with breaches of confidential beneficiary or provider data. However, we face considerable security challenges due to Medicare's current, complex environment. The complexity of this environment is driven by the increasingly data-intensive nature of modern health care as we strive to meet our mission of providing high-quality health insurance coverage to nearly 40 million older and disabled Americans. By law, Medicare fee-for-service claims are processed by about 50 private sector insurance companies who each have their own business processes and variations in the use of Medicare claims processing software, which we are responsible for overseeing. From a technology standpoint, such decentralization requires that we transmit data with contractors to ensure that we bring together up-to-date information on eligibility, enrollment, deductibles, utilization, and other potential insurance payers. We also must share eligibility and managed care enrollment data with the approximately 540 managed care plans providing services to Medicare beneficiaries.

In addition to these demands, we are striving to make information about our programs and services more readily available to Medicare beneficiaries, physicians, and other providers. We need to provide timely solutions and ready access to information for our customers and partners so they can research Medicare benefits, billing rules and procedures, the quality and safety of care, and a host of other subjects. However, we must balance this need with our responsibility to protect sensitive information from unauthorized access, such as preventing "hackers" from violating our internal systems via our public Internet sites. And we must address both of these priorities within the aging nature of our current information technology infrastructure.

We learned a great deal about how to address information technology challenges two years ago when, in partnership with Congress and over one million health care providers across the country, we successfully met the Year 2000 challenge. Now, with our resources no longer committed to that effort, we have resumed efforts to implement legislative changes mandated by the Health Insurance Portability and Accountability Act, the Balanced Budget Act of 1997, the Balanced Budget Refinement Act of 1999, and the Medicare, Medicaid, and SCHIP Benefits and Improvement Act of 2000. We also have initiatives to modernize other areas related to our business functions, including establishing the HCFA Integrated General Ledger Accounting System, to readily support a "clean opinion" on our Chief Financial Officer audit; and we have refocused on the security responsibility that comes with using ever-improving information technology.

INFORMATION SECURITY

In 1997, HCFA's first Chief Information Officer, Dr. Gary Christoph, was hired, and he began an effort to identify security deficiencies in our internal systems. Under Dr. Christoph, we began testing for security problems so we could better realize what problems exist, where they are located, and how we can prevent them. Under this guiding principle, we became one of the first non-military Federal agencies to initiate third-party penetration testing of systems. We used an "ethical hacker" to test for vulnerabilities at our Agency and at some of our claims processing contractors before someone actually seeking to do harm could discover them. It is imperative to uncover these vulnerabilities, and in many cases we agreed with and implemented the contractors' recommendations. In other cases, we analyzed the findings, considered the recommendations, and developed solutions that more appro-

priately fit our business needs while still addressing the underlying vulnerability. In all cases, we recognize the seriousness of any vulnerability and know we must carefully balance security with our other business responsibilities. We do not share confidential beneficiary information for marketing or other commercial purposes. We also have been conservative in moving to new e-business technology, to ensure that adequate protections are in place before we use this type of technology. Moreover, from Fiscal Year 2000 to Fiscal Year 2001, our spending on major information technology security projects increased from $5 million to $11.7 million.

In 1998 we began work on an Enterprise-wide Systems Security Initiative that follows guidance from the National Institute of Standards and Technology and the Office of Management Budget Circular A-130, which established policy for the management of Federal information resources. The central tenet of our initiative is to understand and mitigate the risks to our information in the most cost-effective manner. As you know, this effort slowed when we had to dedicate the vast majority of our information technology staff time and resources to Year 2000 remediation efforts. We resumed focusing on the Security Initiative in 2000, implementing it along two parallel tracks: one track focuses on security inside the Agency, and one examines our external business partners, beginning with the Medicare contractors.

The Security Initiative's implementation at the Medicare contractors began in earnest earlier this year when we published baseline security requirements for the contractors and followed up with an assessment tool to compare how their security measures to our core requirements. The results of those assessments will serve as a valuable work plan for our security efforts in the future.

Our internal HCFA efforts have been ongoing for a longer period of time and we have made substantial progress. We continually assess our internal risks and vulnerabilities and take remedial actions to address them as aggressively as possible within our available resources. For example, we have developed improved procedures and tools for managing access to our data. These efforts help ensure that only staff who have a proper and legitimate professional need have access to sensitive information and that the staff use these data appropriately within our strict guidelines. We look carefully at whether an employee's job entails a "need to know" confidential information. Even our senior staff, including the Chief Information Officer and I, cannot browse this information because we do not have a "need to know." Additionally, we are publicizing our intensified data security efforts to the entire Agency and contractor staff, informing them of their responsibilities, and reminding them that bad habits, such as sharing systems passwords, could lead to unintended consequences. And beginning this summer, all HCFA staff will complete annual training on computer security. We believe that this strong effort to protect sensitive material will itself deter individuals from even attempting to violate our systems.

Throughout our implementation of the Security Initiative, we have pursued self-testing of our security controls. Periodic recurrent testing can detect new vulnerabilities that have surfaced because of new technology, and reaffirm that old vulnerabilities have not been reopened. We also continue to use third party contractors to conduct "white hat" penetration tests of various portions of our computer network. When we began these tests over 3 years ago, we focused on looking into the Agency from external networks such as the Internet. Recently, we conducted more refined testing by looking internally at our network from the perspective of an authorized HCFA user. This is important because published industry-wide statistics indicate that authorized users or employees are suspected as the largest source of security breaches.

Along with our own self-assessments and contractor testing, audits performed by the IG have aided us in identifying security vulnerabilities in our information systems. For example, the IG found that Agency and contractor employees could have had unauthorized access to confidential information, because passwords were not being administered properly or computer programmers could have had inappropriate access to some files. They also found instances where people could have had inappropriate access to the areas where computers were stored. In each of these instances, we have worked hard to address the vulnerabilities, and we have made significant progress. For example, we have recertified all of the individuals with password access to our systems, purging hundreds of individual passwords from our systems. Additionally, we have secured areas that before permitted inappropriate access to our computer hardware.

Some of these vulnerabilities were easy to address, while others are longer-term projects that require more intensive attention. And we remain open to suggestions of additional ways to improve our security. Information technology continues to evolve, and we will always have to strive to keep our health data secure.

CONCLUSION

We have been working hard to protect confidential health data. Our goal is to build upon a multi-layered series of security defenses, utilizing firewalls, scanning software, intrusion detection, administrative controls, access controls, good authorization procedures, and recurrent security training and education for staff, among other things. Taken together, these layers of protection establish a solid security posture for our Agency. We face major challenges in continuing to implement and improve our computer security program. Over the next fiscal year, we expect to put our security policy statements into action and develop specific standards, including establishing minimum floors for protecting all of our sensitive data.

We want to continue to work with you and our other partners to make sure that we protect this information and fulfill all of our responsibilities as effectively and efficiently as possible. Thank you for your support and assistance, and the opportunity to discuss these important issues with you today. I am happy to answer your questions.

Mr. GREENWOOD. Thank you for your testimony, and thank you for the constructive way that you have approached this relationship.

Mr. Vengrin.

TESTIMONY OF JOSEPH E. VENGRIN

Mr. VENGRIN. We share the committee's concerns regarding the security of Government information systems, and we appreciate the opportunity to testify on the vulnerabilities within the Medicare claims processing system.

As you mentioned, Mr. Chairman, as part of our annual audit of the Health Care Financing Administration financial statements, we contract with independent public accounting firms to test the adequacy of internal controls over Medicare's information system. The purpose of these tests is to determine the nature, timing and extent of audit procedures to be performed during this financial statement review.

Strong internal controls over Medicare systems are essential to ensure the integrity, confidentiality, and reliability of critical data and to reduce the risk of errors, fraud, and illegal acts. However, in the last 5 years we have noted continuing material internal control weaknesses in Medicare systems, particularly those operated by the Medicare contractors.

Material weaknesses are defined as serious deficiencies in internal controls that can lead to material misstatements of amounts reported in HCFA's financial statements. Also, such weaknesses could allow unauthorized access to and disclosure of sensitive information, malicious changes that could interrupt data processing or destroy data files, improper Medicare payments, or disruption of critical operations.

My statement today will summarize the significant problems noted in the fiscal year 2000 financial statement audit. I will not go into some of the background on the Medicare system—you have mentioned that in your opening remarks. We know it is very complicated and complex.

As we previously reported, the internal control environment for the Medicare claims processing operation needs substantial improvement. Our fiscal year 2000 audit identified numerous weaknesses in general controls, which affect the integrity of all applications operating within a single data processing facility and are critical to ensuring the reliability, confidentiality, and availability of

data. Auditors identified 124 general control weaknesses—115 at the sampled Medicare contractors and the remainder at the HCFA Central Office.

Mr. Chairman, over 60 percent of these weaknesses involved two types of general controls: access and entity-wide security. Access controls ensure that system assets are physically safeguarded and that access to sensitive computer programs and data is granted only when authorized. Weaknesses in such controls can compromise the integrity of sensitive information and increase the risk that data may be inappropriately used or disclosed.

Access control weaknesses represent the largest problem area. The most widespread weaknesses concerned poorly controlled passwords, ineffective implementation of system security software, and infrequent reviews of access privileges. We also reported that controls did not effectively prevent access to sensitive data. For instance, computer programmers and other technical support staff had inappropriate access to data files used in the fee-for-service claims process, such as beneficiary history files.

As part of their assessment of access controls, auditors performed low-level internal and external penetration testing at eight contractor sites. This testing revealed additional access control risks. Systems permitted excessive remote access logon attempts. Systems disclosed more information about themselves than necessary. Inadequate password protections permitted unauthorized access to certain computer systems, and insufficient controls over print output queues permitted unauthorized read access to sensitive data. Such weaknesses increase the risk of unauthorized remote access to sensitive Medicare information.

Entity-wide security programs ensure that security threats are identified, risks are assessed, control techniques are developed, and management oversight is applied to ensure overall effectiveness of the security measures. These programs typically include policies on how and when sensitive duties should be separated to avoid conflicts of interests and stipulate what types of background checks are needed during the hiring process. Inadequacies in the programs can result in inadequate access controls and software change controls affecting mission-critical operations.

We reported that several contractor sites lacked fully documented, comprehensive entity-wide security plans, had inadequate risk assessments and lacked comprehensive security awareness programs. At the HCFA Central Office, we found no security assessment of or security plans for significant application systems, insufficient security oversight of Medicare contractors, and no formal process to remove system access of terminated HCFA employees.

With respect to the shared systems, since fiscal year 1997, we have reported that Medicare data centers have inappropriate access to the source code of one of the shared claims processing systems. This unresolved weakness, Mr. Chairman, was expanded this year to include the Common Working File, which is shared by all Medicare claims processors. Access to source code renders the Medicare claims processing system vulnerable to abuse, such as implementation of unauthorized programs. While HCFA requires contractors to restrict local changes to emergency situations, local

changes are often not subjected to the same controls that exist in the standard change control process.

To briefly conclude, we remain concerned that inadequate internal controls over Medicare operations leave the program vulnerable to loss of funds, unauthorized access to and disclosure of sensitive medical information, and malicious changes that could interrupt the data processing or destroy data files. All of the weaknesses that I have described today are troubling. However, we do not know whether the resulting vulnerabilities have been exploited in terms of compromised medical information, fictitious claims, or diversion of taxpayers' dollars.

On a positive note, to conclude, I would like to report that HCFA Central Office has continued to make substantial progress in implementing enhanced control procedures, specifically in the area of access controls and application change development controls.

I will now entertain any questions. Thank you.

[The prepared statement of Joseph E. Vengrin follows:]

PREPARED STATEMENT OF JOSEPH E. VENGRIN, ASSISTANT INSPECTOR GENERAL FOR AUDIT OPERATIONS AND FINANCIAL STATEMENT ACTIVITIES, DEPARTMENT OF HEALTH AND HUMAN SERVICES

Good morning, Mr. Chairman. I am Joseph E. Vengrin, Assistant Inspector General for Audit Operations and Financial Statement Activities of the Department of Health and Human Services. With me today is Ed Meyers, Director, Information Systems Audits and Advanced Techniques. We share the Committee's concerns regarding the security of Government information systems, and we appreciate the opportunity to testify on the vulnerability of Medicare claim processing systems.

In conducting annual audits of the Health Care Financing Administration (HCFA) financial statements, which are required by the Government Management Reform Act of 1994, we contract with independent public accounting (IPA) firms to express an opinion on the financial statements and report on internal control deficiencies. As part of the body of work underpinning these audits, the IPA firms perform various internal control tests of the Medicare program, including its automated systems. The purpose of these tests is to determine the nature, timing, and extent of audit procedures to be performed during each year's audit.

Strong internal controls over Medicare systems are essential to ensure the integrity, confidentiality, and reliability of critical data and to reduce the risk of errors, fraud, and other illegal acts. However, since fiscal year (FY) 1996, when we first began the financial statement audits, we have noted continuing material internal control weaknesses in the systems, particularly those operated by contractors. Material weaknesses are defined as serious deficiencies in internal controls that can lead to material misstatements of amounts reported in subsequent financial statements unless corrective actions are taken. Also, such weaknesses could allow (1) unauthorized access to and disclosure of sensitive information, (2) malicious changes that could interrupt data processing or destroy data files, (3) improper Medicare payments, or (4) disruption of critical operations. My statement today will summarize the significant problems noted in the FY 2000 financial statement audit.

MEDICARE AUTOMATED SYSTEMS

By way of background, the Medicare program provides health insurance for 39.5 million elderly and disabled Americans at a cost of about $215 billion in FY 2000. The program is administered by HCFA, the largest component of the Department of Health and Human Services. Medicare services are provided through either fee-for-service arrangements or managed care plans.

HCFA relies on extensive computerized operations at both its central office and contractor sites to administer the Medicare program and to process and account for Medicare expenditures. The HCFA central office systems maintain administrative data, such as Medicare enrollment, eligibility, and paid claims data, and process all payments to health care providers for managed care. The fee-for-service claim processing system, the Department's most complex and decentralized system, is operated with the help of more than 50 contractors located throughout the country. There are two types of contractors: Intermediaries process claims from institutions, such as hospitals and skilled nursing facilities, filed under Part A of the Medicare

program, while carriers process Part B claims from other health care providers, such as physicians and medical equipment suppliers. These contractors and their data centers use several "shared" systems to process and pay provider claims. Currently, each intermediary uses one of two shared systems, and each carrier uses one of four shared systems. All of the shared systems interface with HCFA's Common Working File system to obtain authorization to pay claims and to coordinate Medicare Part A and Part B benefits. This fee-for-service network processed over 890 million claims totaling $173.6 billion during FY 2000.

Generally, Medicare claim processing begins when a health care provider submits a claim to a contractor. The claim is entered into a shared system which captures, edits, and prices the claim. Once the claim has passed all shared system edits and has been priced, it is submitted to the Common Working File for validation, verification of beneficiary eligibility, and payment authorization.

SYSTEMS CONTROL WEAKNESSES

As we have previously reported, the underlying internal control environment for Medicare claim processing operations needs substantial improvement. Our FY 2000 audit identified numerous weaknesses in general controls, which involve access controls, entity-wide security programs, application development and program change controls, segregation of duties, operating system software, and service continuity. General controls affect the integrity of all applications operating within a single data processing facility and are critical to ensuring the reliability, confidentiality, and availability of data.

Of 124 general control weaknesses identified, 115 were found at the sampled Medicare contractor sites and 9 were found at the HCFA central office. About 80 percent of these weaknesses involved three types of controls: access controls, entity-wide security programs, and systems software.

Access Controls

Access controls ensure that critical systems assets are physically safeguarded, that logical (e.g., electronic) access to sensitive computer programs and data is granted only when authorized and appropriate, and that only authorized staff and computer processes access sensitive data in an appropriate manner. Weaknesses in such controls can compromise the integrity of program data and increase the risk that data may be inappropriately used and/or disclosed.

Access control weaknesses represented the largest problem area. The most widespread weaknesses concerned administration of the controls themselves. At several contractors, passwords were not properly administered, systems security software was not implemented effectively, or access privileges were not reviewed frequently enough to ensure their continuing validity. We also reported that controls did not effectively prevent access to sensitive data. For instance, computer programmers and other technical support staff had inappropriate access to the data files used in the fee-for-service claim process, such as beneficiary history files. Under these conditions, the Common Working File system was vulnerable to inappropriate use.

At some contractors, programmers had inappropriate access to system logs; this provided an opportunity to conceal improper actions and obviated the logs' effectiveness as "detect" controls. At one contractor, the computer operator could override installation system security precautions when restarting the mainframe computer system. We also noted weaknesses in controls over access to sensitive facilities and media within those facilities. For example, at one contractor, inappropriate individuals had access to the computer center's command post. At another, the computer production control area was not secured during normal business hours.

Penetration Tests. As part of their assessment of access controls, IPA firms performed low-level internal and external penetration testing at eight Medicare contractor sites. The purpose of this testing was to identify real and postulated security risks to, and vulnerabilities of, the information systems. A variety of common penetration testing procedures revealed additional access control risks at certain contractor sites. When dial-up connections were made, computer systems permitted an excessive number of failed remote access log-in attempts before disconnection and disclosed more information about themselves than necessary. In addition, inadequate password protections permitted unauthorized access to certain computer systems, and insufficient controls over print output queues permitted unauthorized "read" access to sensitive data. Such weaknesses increase the risk of unauthorized remote access to sensitive Medicare systems and data.

Entity-Wide Security Programs

Entity-wide security programs ensure that security threats are identified, risks are assessed, control techniques are developed, and management oversight is ap-

plied to ensure the overall effectiveness of security measures. These programs typically include policies on how and which sensitive duties should be separated to avoid conflicts of interest and stipulate what types of background checks are needed during the hiring process. Entity-wide security programs afford management the opportunity to provide appropriate direction and oversight of the design, development, and operation of critical systems controls. Inadequacies in these programs can result in inadequate access controls and software change controls affecting mission-critical operations.

We reported that several contractor sites lacked fully documented, comprehensive entity-wide security plans that addressed all aspects of an adequate security program. Inadequate risk assessments, a lack of comprehensive security awareness programs, and inadequate policies were among the weaknesses noted at the contractors. At the HCFA central office, we found no security assessment of, or security plans for, significant application systems; insufficient security oversight of the Medicare contractors; no formal process to remove system access of terminated HCFA employees and contractors; and deficiencies in the management review and approval process.

Systems Software Controls

Systems software controls help to prevent unauthorized individuals from using software to read, modify, or delete critical information and programs. Systems software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, it supports a variety of applications that may run on the same computer hardware. Some systems software can change data and programs on files without leaving an audit trail.

Weaknesses in systems software controls related to managing routine changes to the software to ensure their appropriate implementation and configuring operating system controls to ensure their effectiveness. Such problems could weaken critical controls over access to sensitive Medicare data files and operating system programs.

Shared System Weaknesses

Since FY 1997, we have reported that the Medicare data centers have inappropriate access to the source code of the Fiscal Intermediary Shared System, which is used by certain Medicare contractors. This unresolved weakness was expanded this year to include the Common Working File system, which all shared systems use to obtain authorization to pay claims. Access to source code renders the Medicare claim processing system vulnerable to abuse, such as the implementation of unauthorized programs and the implementation of local changes to shared system programs. While HCFA requires contractors to restrict local changes to emergency situations, local changes are often not subjected to the same controls that exist in the standard change control process.

CONCLUSIONS

In summary, we remain concerned that inadequate internal controls over Medicare operations leave the program vulnerable to loss of funds, unauthorized access to and disclosure of sensitive medical information, malicious changes that could interrupt data processing or destroy data files, improper payments, or disruption of critical operations. Further, because of weaknesses in the contractors' entity-wide security structures, HCFA has no assurance that information systems controls are adequate and operating effectively. While all of these weaknesses are troubling, we do not know whether the resulting vulnerabilities have been exploited in terms of compromised medical information, fictitious Medicare claims, diversion of taxpayer dollars, or some other type of fraud or abuse by an "insider" or a hacker.

What most concerns us are the continuing problems identified in access and entity-wide security controls. HCFA must ensure that Medicare contractors develop corrective action plans that not only address identified weaknesses but also attempt to determine the fundamental causes of the weaknesses. Among the efforts planned and underway by HCFA is an improved corrective action process. We expect that HCFA's testimony will fully address that process, as well as other short- and long-term actions to shore up information systems controls. We urge HCFA to sustain its focus on these critical internal controls. Furthermore, HCFA and the Medicare contractors should routinely conduct penetration testing to ensure the integrity of their information technology environment.

We in the Office of Inspector General will continue to work with HCFA to overcome the persistent risks to the security of the Medicare program. For example, as required by the Government Information Security Reform Act (GISRA) of 2000, we have begun an independent evaluation of HCFA's security program. Our evaluation will incorporate the results of several efforts: the internal control testing conducted

during our annual financial statement audits, our ongoing work to ensure compliance with Presidential Decision Directive 63, our additional work focused on access and entity-wide security controls at selected Medicare contractors, information systems reviews (known as Statement on Audit Standards 70 examinations) conducted by IPA firms under contract with HCFA, and other security assessments performed by consultants for HCFA.

I will be happy to discuss the extent of our GISRA work, as well as any other matters, in response to your questions.

Mr. GREENWOOD. Thank you. Mr. Neuman, thank you for being with us this morning.

TESTIMONY OF MICHAEL NEUMAN

Mr. NEUMAN. Sure. Essentially, we are ethical hackers, and our job is to ensure that the implementation of a network, of an application of a server matches the policy set forth by the organization and that it matches best industry practices.

Over the course of 1997 to early 2000, we conducted about six penetration tests, both internal and external, meaning as an average employee of HCFA and as an average hacker on the Internet externally. We have also reviewed their architecture. We have reviewed the desktop PCs that they put on everybody's desk. We have dialed all their phone numbers looking for modems. For findings, the bottom line is this: Over the course of that work, we found several serious vulnerabilities that could easily have allowed anybody unrestricted access to the data owned by HCFA.

In our experience with them, these vulnerabilities were quickly fixed, sometimes in a matter of hours. Management also really made security a fairly high priority. Then they wanted to do real security. What we see a lot is people are perfectly happy to deal with security issues by writing more policies dealing with it. That is not the answer. What we do is make sure that the implementation matches that policy. HCFA has made a real effort to ensure that their implementation does match their policy.

What we found is this: Absolutely the biggest cause of vulnerabilities at HCFA is not directly from the fault of HCFA employees but through their facilities management contractors, the people who are responsible for running their networks, for installing new machines, for managing their network connectivity. By far this was the biggest source of vulnerabilities that we found. In our experience, we have seen the contractors actually undermine the security efforts of the HCFA staff. They removed security protections without HCFA's knowledge. They misrepresented the security precautions they were taking. They made serious, serious configuration errors that were inconsistent with even the most basic industry security standards.

Unfortunately, HCFA does not have the technical expertise overseeing these contractors—and, again, these are the facilities management contractors I am speaking of. They could not detect that these contractors were making these mistakes. They did not have the ability to ask the proper questions to determine if they were doing the right thing. On top of that, HCFA also was lacking the contractual power to make the contractors do what they wanted them to. There was nothing in the contracts which said that they had to perform to a certain level of security or that they need to take certain precautions.

Last finding, when we left them, there were a variety of known risks to third parties, in particular we are talking about Medicare contractors. There are a variety of insurance companies, doctors, which are connected both through the MDCN and through direct connectivity into HCFA's network. There are a variety of risks there, which I have detailed in my written testimony.

In the end, we recommend this: HCFA needs to focus on technical security not just policy. Really every organization needs a person who is in charge of implementing the security policy, not just telling people how to do passwords but making sure that the passwords are correct, making sure that systems are configured properly, and so forth. They need better control and technical oversight of their contractors. Again, I am not talking about Medicare contractors, although that probably is an issue; in my experience, the facilities contractors.

They need more testing of everything. When they install remedial fixes, you need to test those fixes after you are done installing them. You need to test everything from applications to servers to networks, and it needs to be done regularly. Threats and vulnerabilities change all the time. And decisions to ignore those vulnerabilities really need to be taken with a full awareness of what the actual risks are when they take that risk.

In the end, if they had the technical expertise and the oversight of their contractors, virtually every vulnerability that we found would have been prevented. And we think that is a significant step they need to take.

[The prepared statement of Michael Neuman follows:]

PREPARED STATEMENT OF MICHAEL NEUMAN, EN GARDE SYSTEMS, INC.

0. SUMMARY

Penetration testing is a critical tool in ensuring the security of everything from an individual software application to an entire network. Unfortunately, security is far too complex to provide any sense of absolutes. Add to that the fact that dozens (if not hundreds) of new vulnerabilities are discovered every week, and the need to continuously test the security of a system is obvious.

We have provided services, similar to those we provided HCFA, to hundreds of companies, and are intricately aware of the "industry standard" state of security. During our tenure providing security services to HCFA, we found both extremely positive and disturbing issues. Major recommendations include:

Technical Oversight: HCFA is lacking the specially trained personnel to oversee their and their contractors' activities and verify the work for security consistent with policy and best practices..

Third-Party Verification: It should be unacceptable for service providers to certify themselves as secure. Any vendor of network services to HCFA should readily accept 3rd party verification of security and have regular testing a part of their contract performance requirements.

Security Specified in Contracts: The security expectations and requirements should explicitly be laid out in contracts with network service providers.

More Testing is Required: It's necessary to independently verify the security features of everything from applications to WWW servers to networks and to do so on a recurring basis.

1. BACKGROUND

En Garde Systems (EGS) provided a variety of security services to the Health Care Financing Administration (HCFA) between December 1997 and June 2000. During that time, EGS performed a number of penetration tests and assisted HCFA in devising network security protections. Specifically, EGS has performed:

- *External Penetration Tests (4).* As an average outsider connected to the Internet, we attempted to gain access to internal HCFA resources.

- *Internal Penetration Tests (2).* Given a connection to HCFA's internal network, we attempted to gain access to internal HCFA resources.
- *Wardialing.* Given a prototype phone number (for example 786-xxxx), we dial every phone number looking for computer modems. When a computer answers, we attempt to gain access.
- *Architecture Review and Design.* Given a complete map of network resources, we spent extensive time understanding the various applications HCFA provides and the security needs of each. We then formulated network architecture changes that would build security into the fabric of the network.
- *Test of Internet services hosted by IBM Global Services.* At the time we tested, HCFA outsourced its internal and external web servers to IBM.
- *NT Desktop Review.* For Y2K, HCFA moved to a Windows NT desktop system. We were provided with a prototypical NT desktop prior to deployment to find security vulnerabilities.
- *HCFA Insider test.* We were given a standard user's desktop computer and asked to gain access to HCFA internal resources. In this case, we were not allowed to bring in our own software, floppies, or PC—only what we could retrieve using HCFA's network.
- *Intrusion Detection System Review.* HCFA ran a "bake-off" of several competing Intrusion Detection Systems and asked us to perform a variety of tests to determine their efficacy.
- *Security Training.* We provided classes over a several day period covering everything from good password choice to Intrusion Investigation and Response.

2. APPROACH

Penetration testing is a critical tool in ensuring the security of everything from an individual software application to an entire network. Unfortunately, security is far too complex to provide any sense of absolutes. Turning on one network service may result in dozens being turned in non-obvious ways. Connecting a trusted partner to your network often means you not only trust him, but everyone he trusts as well. Add to that the fact that dozens (if not hundreds) of new vulnerabilities are discovered every week, and the need to continuously test the security of a system is obvious.

Our approach to testing is almost exclusively "manual". We rarely use automated tools, as our experience has shown they are generally only effective in an extremely small number of cases. Instead, we learn about the network and create new attacks on the fly. In doing so, we are doing exactly what a hacker does.

Proposing solutions to vulnerabilities is perhaps the most complex part of our work. Before we recommend any solution, we need to determine the:

1) Value of the organization's data. If the data is simply pricing and personnel information, it is far less valuable to a hacker than Privacy Act data, for example.
2) Threat to the organization. A government agency will attract far more interest from the malevolent than a small computer company, for example.
3) Path of least resistance. It makes no sense to spend a great deal of effort protecting a network connection to a partner if the "front door" is wide open. These relative threats are determined before any solution is recommended.
4) Cost in man-hours and equipment expenditures. We often make several recommendations based upon the amount of money the customer wishes to spend.

3. FINDINGS

We have provided services, similar to those we provided HCFA, to hundreds of companies, and are intricately aware of the "industry standard" state of security. During our tenure providing security services to HCFA, we found both extremely positive and disturbing issues.

3.1 Positive

3.1.1. There is a healthy approach to security from HCFA management. Whereas many other organizations believe that all security problems can be solved by writing a policy, HCFA has taken significant steps to not only inscribe the virtues of security, but to ensure they practice what they preach.

3.1.2. When we first arrived at HCFA, we found them to be operating with significant and obvious vulnerabilities. These problems were fixed within hours of our reports. Over the course of the years, HCFA has become significantly more secure than the industry standard.

3.1.3. Beyond simply patching vulnerabilities that were found, HCFA has made significant efforts to find the systemic causes of their vulnerabilities and fix them wherever possible.

3.2 Negative

3.2.1. Contractors

By far, HCFA's biggest security problems have been the direct result of the action or inaction of contractors. In general, we have found HCFA's contractors to be outright obstructive to providing sound security. Compounding these errors was HCFA's inability to catch or prevent them.

a. HCFA lacked the technical oversight of their contractors to verify the contractor was actually implementing the security measures they claimed. The managerial oversight had no ability to ask relevant questions.
b. HCFA's contracts had no mention of security expectations of a contractor. As a result, the contractors were free to implement (or not implement) any measures they felt as appropriate, regardless of HCFA's requests.
c. We discovered during our first test that a HCFA contractor ignored change control, bypassed the firewall policy group, and installed his own filter rules directly onto HCFA's primary firewall without anyone's knowledge. These filter rules made the entire HCFA network vulnerable to a variety of serious attacks. After bringing the firewall problem to HCFA's attention, the contractor was directed to remove the rule and instructed about the use of change control. One year later, we tested and found the contractor installed the same rule again without HCFA's knowledge.
d. On several occasions, we witnessed HCFA contractors argue against improving security stating that changes HCFA asked for were "difficult" or "impossible" when, in fact, they were not.
e. During our architecture review, we discovered that the HCFA contractors responsible for network operations could not provide a complete list of all network connections external to HCFA. In fact, we spoke to over a dozen groups, and each would make us aware of another undocumented connection from HCFA to another organization.
f. Contractors have made extremely poor password and configuration decisions, violating the most basic security principals and completely invalidating other security measures put into place.

3.2.2. IBM

HCFA relied on IBM to provide secure network connectivity (via a product called "SecureNet") to MDCN partners as well as for both external and internal WWW servers. We were contracted to evaluate the architecture and determine potential risks.

During a meeting with HCFA management (up to CIO level), IBM's security staff and management responsible for the HCFA contract, and ourselves, we were told by IBM that we didn't need to test because they had taken every imaginable security precaution. They described how:

- Administrators can only connect from a physically secure administrative network
- WWW administration is done through an encrypted management connection
- Patches are installed immediately after a vulnerability is announced
- They would be happy to share their firewall's access control lists with us
- They perform penetration testing every week
- They have a custom designed IDS along with 24/7 response
- The firewalls only allow WWW access through

Upon extensive questioning from ourselves and HCFA's CIO, it we learned from IBM that:

- Administrators can also dial-in from home into a generic "SecureNet" modem bank, that all other customers use, and administer machines.
- WWW administration can be encrypted, but they haven't enabled that feature, and probably won't because it's difficult to do so.
- Patches are only installed when an administrator gets around to it, which is usually in a "week or two".
- They would not share their access control lists because, "If EGS found a vulnerability in HCFA, they would find a vulnerability in all IBM customers."

Because HCFA relies so much on the security of IBM to provide everything from secure connectivity for the MDCN to managed web hosting, we proposed performing three distinct tests:

1) External test against the web servers hosted by IBM
2) Tests from a HCFA partner connected to the MDCN directed at HCFA and other partners on the MDCN.
3) Tests from a non-MDCN customer of IBM directed towards HCFA.

It took IBM and HCFA a year of negotiation to come to terms to allow just the external test against the web servers. We were given several severe restrictions that made the results of the test unrealistic. Specifically:

1) We were not allowed to test the firewalls or any other infrastructure on the IBM network. They did provide us with an extremely limited subset of filter rules that IBM said were installed on their firewalls.
2) We were not allowed to touch any IBM system other than HCFA's web server. This included administrative systems, other customer servers, or any infrastructure.
3) We were not allowed to route traffic through any other IBM network.

These restrictions meant that we could only test the controls in place on the web server. We could not check for configuration errors in access control lists, vulnerabilities in firewalls or routers, or transitive trust issues (i.e. if we can break into the IBM administrative network, or another customer's web server, what can we do then?).

In the end, the restrictions ended up being irrelevant. Using an extremely old, very well known vulnerability in the WWW server software, we were able to gain access to HCFA's web server without any more technical expertise than it takes to point and click. Because of the way HCFA's web server was configured, and an error made in the firewall rules set up by IBM, we were then able to access HCFA's internal network resources. IBM's other claims were then shown either false or useless:

- If they performed a penetration test every week, they would have discovered this blatant vulnerability
- They provided us with the IDS logs collected during the course of our attack, and we had gone completely unnoticed, despite us making no effort to hide our tracks.
- The firewalls allowed not only WWW access through but also another protocol that allowed us unfettered access to HCFA's internal network.

3.2.3. Third Party trust

HCFA has a need to connect with a variety of insurance companies, doctors, and so forth. Network connections were provided both through the MDCN and by direct connectivity to other companies. These connections were configured such that there was no protection of either HCFA from the company or the companies from each other. Essentially, HCFA was trusting these companies completely. As a result, HCFA is subject to whatever security policies and protections are in place by the trusted company. So, if HCFA trusts company A and company A trusts company B, then HCFA trusts company B. Without any control over or auditing of the partner's network, HCFA should not trust that it's secure.

In addition to threatening HCFA, there is a potential for these competing insurance companies to use HCFA as a means to attack one another. HCFA provides the unsecured communications mechanism, and a company simply uses that to get into another's network.

4. RECOMMENDATIONS

4.1. Technical Oversight

HCFA is lacking the specially trained personnel to oversee their and their contractors' activities and verify the work for security consistent with policy and best practices. This position should be solely technical—it should not have any policy development duties associated with it. The position should be independent of any contractors and should be associated with the security policy group. Essentially, the role is to be the "security implementer" of the organization.

The goal is to have an independent and informed person who can ensure that the security of the organization is not simply some high-level goals or a policy on paper. In HCFA's case, such a person would have prevented the vast majority of vulnerabilities introduced by either HCFA or HCFA's contractors. Beyond our experience with HCFA, such a position is direly needed in most organizations.

4.2. Third-Party Verification

It should be unacceptable for service providers to certify themselves as secure. Recently, it's become popular for service providers to get an outside certification of their networks or services and provide that as evidence of their security. In our experience, these too are insufficient, as the certifiers do not reveal their methodology or extent of their certification.

Any vendor of network services to HCFA should readily accept 3rd party verification of security and have regular testing a part of their contract performance requirements.

4.3. Security Specified in Contracts

The security expectations and requirements should explicitly be laid out in contracts with network service providers. Without such clauses, HCFA was essentially powerless to require the use of broadly accepted industry security standards.

4.4. More Testing is Required

Security is such a complex field, with new vulnerabilities being discovered daily, that it's impossible for the average Information Technology professional to keep up. As a result, it's necessary to independently verify the security features of everything from applications to WWW servers to networks and to do so on a recurring basis. In HCFA's case, thoroughly testing the security of the MDCN is critical to its continued operation and information integrity. As it stands, there's no way to know if it's really secure or not. Whenever a new application or service is provided to the public, a new network connection is established, or a new modem installed, these need to be tested for proper operation.

5. CONCLUSION

We believe HCFA has done more to identify and remedy security problems than is common. Despite this, they have experienced a substantial set of serious vulnerabilities over the course of our provision of security services to them. Their reliance upon contractors to operate makes them particularly susceptible to the types of vulnerabilities we have described within this document.

There is always more work to do, however. Security is not a one-time fix—it's something that must be integrated into the business of an organization. It must be continually reinforced, reanalyzed, and redesigned as circumstances dictate. New services, applications, and networks need to be tested before deployment.

Mr. GREENWOOD. Thank you very much.

Okay. Questions. And, Ms. Adair, I am sure you understand that HCFA is not being isolated and singled out. This committee is working its way, fairly methodically, through all the agencies and departments over which we have jurisdiction, and today just happens to be your day.

I would like to direct your attention, Ms. Adair, to a document that is in your binder. Do you have one of these binders available to you? It is document number 1, which is the current contract HCFA has for the operation of the Medicare Data Communications Network, the MDCN. If you look at the second page of this document, toward the bottom, there is a section on, "security requirements." It says, "MDCN security shall be provided/slash maintained/assured by the contractor in order to prevent unauthorized physical, electronic or virtual access to telecommunications facilities, to MDCN hardware or software components and to telecommunications services." It then goes on for two more sentences about how encryption is not required and that the MDCN contractor must report suspicious activity on the system to HCFA.

Now, this document, in reality, is over 100 pages long, but this is only reference to security requirements in the entire document, my staff informs me—these three sentences. Are we to assume from this that HCFA does not provide its MDCN contractor with specific security requirements with respect to access controls, firewall rules, et cetera, and that instead simply simply says, "Give us a 'secure,' system"?

This contract also talks about how the contractor will assure the security of its system from unauthorized attacks, but it doesn't contain any requirements that the contractor actually test the security of its system. How can security be, "assured" without actual testing? How does HCFA plan to revise its contracts to address this issue in the future? And I am heartened to see you and your staff

taking notes so far this morning, so I assume that you intend to take such steps.

Ms. ADAIR. Yes. And I think, though, that I would ask that John Van Walker, who is the Senior Advisor for Technology, to respond to that specific question.

Mr. GREENWOOD. Mr. Van Walker.

Mr. VAN WALKER. Yes, Mr. Chairman. It is certainly true that this is the sole statement in the contract that touches on security. It is written in 1966—or, actually, the contract was entered into in 1966, at a time when security was not such an——

Mr. GREENWOOD. Nineteen ninety-six.

Mr. VAN WALKER. Nineteen ninety-six, sorry, sir.

Mr. GREENWOOD. If it was 1966, I would be praising you for your foresight.

Mr. VAN WALKER. Indeed, and we would have been appreciative. But in 1996, we viewed the network on a far more closed basis, and we actually had interaction with essentially the Medicare contract community. As the network has expanded, as HCFA's responsibilities have enlarged, and the requirements for more and more data from more and more partners have increased, obviously the network has expanded. This paragraph would be completely inadequate in a contract written today. In any future contracts, we certainly would be far more elaborate, sir.

What we have done to deal with this situation is institute and even intensify, as incidents such as those reported by Mr. Neuman have come to our attention, our direct interaction with the contractor. We now meet with the contractor every week. That meeting involves not only face-to-face contacts but the IBM and AT&T security specialists dial in to that conversation from the locations around the country so that we can stay on top of these issues and work through them on a united basis.

Mr. GREENWOOD. How long have you been doing that, sir?

Mr. VAN WALKER. We instituted those meetings, sir, roughly 18 months ago at that level of intensity. There were always weekly meetings for MDC and management, but we have certainly increased the level of interaction of the number of participants, especially on the security side, in the past 18 months.

Mr. GREENWOOD. When does the current contract expire?

Mr. VAN WALKER. This contract expires for—and I should point out that the web hosting contract is actually, because of the interaction between AT&T and IBM, a subcontract within the MDCN contract itself. So they expire simultaneously in December of this year.

Mr. GREENWOOD. Okay. And are you in the process or where do you stand in terms of drafting the new contract?

Mr. VAN WALKER. We are using a GSA contractor to assist us in identifying requirements for the new vehicle. We are having discussions with GSA, with the Department of Interior, with other agencies about vehicles they already have in place. And in whatever contract we issue, the explicit types of security requirements that you and the other witnesses have outlined would be included in that.

Mr. GREENWOOD. How about testing?

Mr. VAN WALKER. Testing, obviously, is one of those requirements, and the types of ongoing, sustained testing programs clearly is something that we agree is a necessary base requirement.

Mr. GREENWOOD. We have found that consistently, as we have been involved in this process for some time.

Let me address a question, if I could, to Mr. Vengrin. I would like you to refer, if you would, to document number 3 in the binder. Do you have that before you? This is the Department's accountability report for fiscal year 1997. On page 23, it says—I will let you turn to page 23—it says, "data security remains a major concern at the HCFA Central Office. Our prior year review demonstrated weaknesses in EDP, which stands for electronic data processing controls, through a system penetration test in which we obtained access privileges to read or modify sensitive Medicare enrollment, beneficiary, provider, and payment information. Although HCFA immediately corrected the prior year vulnerabilities, our current year tests resulted in penetrating the mainframe data base. We obtained the capability to modify managed care production files."

You tell me about this test that penetrated the mainframe, and is it true that you were able to actually alter Medicare payment amounts without HCFA's knowledge?

Mr. VENGRIN. Yes, Mr. Chairman. I remember that event very well. With the permission of HCFA, we entered the system with a very low-level password, and one of their employees was sitting at the terminal. By entering this system and accessing it with a low level password, an individual from one of our contractors was able to go in and identify basically common passwords that were left on when the system was first put on, like "Hot Site"; that password was not removed, and it was a high-level password. And with that, we were able to upgrade the low level and enter the managed care file. And HCFA wanted a demonstration that we explicitly could alter a payment, so we identified a beneficiary payment. We actually altered it, put "zero, zero" in there, and that concluded the test. So we effectively penetrated the system.

Mr. GREENWOOD. And the purpose of that exercise, I presume, is to demonstrate that an unethical hacker could in fact steal money from HCFA by altering the amounts due on bills to virtually any number he choose.

Mr. VENGRIN. That is correct, sir. Passwords such as those should be removed. I believe immediately after that test they did remove that password.

Mr. GREENWOOD. Sort of like breaking into Fort Knox.

What was HCFA's response to this test?

Mr. VENGRIN. Mr. Chairman, they did immediately remove that specific vulnerability, and also they advised us that they would have to go back and check and cross check to make sure that the alteration of the payment amount didn't actually get out to the beneficiary. It did take several days to reconstruct it and validate their data base, so they did kind of complain that it was a disruption to the operation.

Mr. GREENWOOD. Well, isn't it true that not only did they complain but they refused to permit subsequent testing that would be that in-depth ever again?

Mr. VENGRIN. I believe it would be correct to say that we specifically have not reperformed that level of testing. In talking this level of testing over with Dr. Christoph, I think he would prefer to do a higher level of penetration——

Mr. GREENWOOD. Could you identify him, for the record?

Mr. VENGRIN. Dr. Christoph, I am sorry, is the CIO at Health Care Financing Administration. And he would prefer to do that level of testing with individuals that he would choose, which we don't have a problem with.

Mr. GREENWOOD. Do you have any indication that in fact he has done that?

Mr. VENGRIN. Again, he did contract with En Garde to do some of the higher level penetration testing.

Mr. GREENWOOD. Okay. In 1997—let us see—do you think that the CFO audit tests that you have been conducting since 1997 have been sufficient when it comes to penetration tests? And if not, what would you propose?

Mr. VENGRIN. No, sir. As we have told many of the committee members, since fiscal year 1998, or actually from 1997, our objective was to do more of the higher level intrusion testing procedures. But as we proceeded in fiscal year 1998, it was pretty unanimous that the Medicare contractors refused to allow us to do the high-level procedures. They wanted specific indemnification. Should our contractors do this process, the higher level scans, and disrupt operation, the medical contractors specifically wanted to be indemnified for any loss. For many of these contractors, Medicare is a small part of their business function—in some cases it could be 40 percent—so if it resulted in a disruption of operation, they wanted to be paid for it. And, unfortunately, we have not been able to successfully resolve that issue. There are legal ramifications, which HCFA can address.

Mr. GREENWOOD. Well, how valid is that concern? Should they be concerned that there is some real exposure there at these tests that require that kind of indemnification?

Mr. VENGRIN. Mr. Chairman, I have consulted with experts in the field, and as some of our colleagues here have testified, depending on bad configuration, yes, it could shut the operation down. As you do this intense scan, some of the configuration could identify this as a vulnerability, and basically the walls would come down and shut off operations. So no one can guarantee us, sir, that that is not a potential, and hence we would be very dubious about doing further work.

Mr. GREENWOOD. Let me ask Mr. Neuman a question in that regard. This is what you do for a living. Is the state-of-the-art such that you can't do these kind of in-depth penetrations without in fact risking clobbering the system like that?

Mr. NEUMAN. We have done tests for over 100 customers, and we do very in-depth testing. In one case, we brought down a system that we did not intend to. It was back up in a couple of minutes. But there is the possibility of stopping access for at least a short period of time. The possibility of corrupting things such they are unrecoverable is probably very low, but denying service for a few minutes is a reasonable risk.

Mr. GREENWOOD. Okay. Back to you, Mr. Vengrin. This document that I refer to also states, "Moreover, our system penetration tests revealed additional control problems, which could be exploited by unauthorized individuals to compromise one or more of HCFA's computer systems." Can you explain what these additional control problems were?

Mr. VENGRIN. Mr. Meyers?

Mr. GREENWOOD. Or Mr. Meyers. And, Mr. Meyers, if you—yes, thank you.

Mr. MEYERS. Yes. The work that we do as a part of the CFO audit splits down between the general control and the application control reviews, as well as the intrusion protection review. The bulk of the focus thus far has been on intrusion protection, but when you get into the area of general controls, entity-wide security, which is the big issue, as well as access control, we found numerous repeat conditions present since 1997. Some of those areas involve the security program that is being developed at either HCFA Central Office and/or its contractors.

Those programs could be viewed as an umbrella operation to, one, bring the proper level of management oversight into the whole security environment. It would deal with the accreditation of systems as mandated by various legislation or guidance, like OMB A-130 or the FIP Publications, a very critical function in ensuring that you have an effective security environment to deal with this process. We have also noted findings in the area of system software, findings in service continuity, and findings in the application control area, which were alluded to earlier, in the area of change development and application controls.

Mr. GREENWOOD. Thank you. Question to Mr. Neuman. I would like you to refer in your binder, if you would, to document number 6.

Mr. NEUMAN. All right.

Mr. GREENWOOD. That is your document, I believe, written by En Garde to HCFA, dated November 16, 1998, in which En Garde states, "Given the trust vested in the secured network run by IBM at the time, provisions for independent third party penetration testing should be negotiated with IGS and added to the contract. Recommend at least annual testing of all servers hosted by IGS and the blank firewall maintained by IGS for HCFA."

Now, if you would skip a sentence, and then it reads, "In addition, recommend testing to verify that HCFA cannot be reached from the Internet through the secured network or from another customer site on the secured network." These sound like very sensible recommendations. What was HCFA's reaction to this memo, and did they permit you to conduct all of these recommended tests?

Mr. NEUMAN. Their reaction was that they were good ideas. We were permitted to perform the test of their web server. We were not permitted to test from other secured network partners and other secured network customers which were not partners with HCFA. So we tested one out of the three of our recommendations.

Mr. GREENWOOD. Ms. Adair, a subsequent document dated July 6, 1999, it is document number 7 in your binder. Do you have that there? It is a work order for a statement of work that includes the three En Garde recommended tests. HCFA's Internet vulnerability,

MDCN partner vulnerability, and non-MDCN/IBM customer vulnerability. We know that En Garde was permitted to do the first test under very limited conditions. That is what Mr. Neuman just spoke of. But why hasn't HCFA followed through on these other two tests in the 2½ years since they were made? Do you not think it is important to conduct such tests of the alleged secure network?

Ms. ADAIR. I believe, sir, that the answer to the question is, as you pointed out, that we did the first one, we negotiated that, and we have, to date, not been able to negotiate the capability to do the additional tests that are listed here.

Mr. GREENWOOD. Negotiate with whom?

Ms. ADAIR. The MDCN contractor.

Mr. GREENWOOD. Can you elaborate on that? I mean what has prevented in 2½ years—they work for you, right?

Ms. ADAIR. Yes.

Mr. GREENWOOD. What do you pay for that contract?

Mr. VAN WALKER. The current billings under the MDCN contract, Mr. Chairman, I believe, are in the area of $18 million for all services combined.

Mr. GREENWOOD. Annual figure?

Mr. VAN WALKER. That is this year's figure. It would be in the neighborhood of $15 million to $20 million in every year, sir.

Mr. GREENWOOD. Okay. So we are paying these guys that amount of money, and in 2½ years you have not been able to negotiate with them to have these other tests performed.

Mr. VAN WALKER. Right.

Mr. GREENWOOD. Which were recommended by your own independent contractor.

Mr. VAN WALKER. Essentially, the position taken by the vendor in this case is that indeed they were surprised that we were even able to negotiate such an arrangement on a one-time basis with the web hosting vendor, that it is not standard industry practice to allow this, that the danger we would bring to their ability to manage their entire network and the operations of their other customers is so severe that it is simply inappropriate for them to do so.

We continue to have discussions about how we can get around this and even have gone so far as to talk to them, if we can't do it using our own third part resources, what are the possibilities of using their internal white hat ethical hacking teams to do it in a situation in which HCFA would largely define the terms of that and would have access to additional information. That seems at least to be a possibility, and we are continuing to explore that, sir.

Mr. GREENWOOD. Mr. Neuman, I would be interested in your response to that. From what we have just heard, one would conclude that you recommended two tests that their vendor says are highly unusual and not state-of-the-art and not willing to engage in. So one would tend to think that either you are making unrealistic recommendations or the vendor has unrealistic expectations.

Mr. NEUMAN. Well, the first test that we did, I believe, took over a year to negotiate with them. So I am not terribly surprised that they are making it difficult. What we are proposing is very simple. What we are proposing is simply to go from an MDCN partner, see what you can do to HCFA, from a non-MDCN partner, see what

you can do to HCFA. That is it. Touching the infrastructure in the middle is—you are not really hurting the contractor in any way.

Mr. GREENWOOD. And I would assume that you have not been able to negotiate this pursuant to existing contract. What about the future? What does the future hold in terms of contractual language that would enable you to do this?

Mr. VAN WALKER. Certainly we would attempt to get this clause that there are some limitations here. While web hosting is pretty much a commodity practice and we could, without too much disruption to our operations, replace that vendor with another one who might be more willing to allow this kind of testing at the network level—and the HCFA network is somewhat unique. It is not based on current Internet technologies. It uses a combination of Internet technologies and older SNA technologies to do very specific things that are largely concentrated in the financial and insurance industries.

Replacing the vendor would be a difficult multi-year process for us, so our efforts are focused on attempting to work out an accommodation with the vendor that would allow us to do these tests or have these tests performed by them, using guidance, strictures, requirements for which we would get assistance perhaps from the Inspector General's Office, perhaps from firms like Mr. Neuman's to attempt to work out a situation in which we would have further assurances, as you have pointed out, that what they say they are doing is indeed what they are doing. And we have routine, ongoing security briefings from them about the various types of technologies that are being deployed and about ongoing enhancements to the network. But the ability to compel them is not within our power at this time.

Mr. GREENWOOD. But you can tell them in your discussions that you are under intense pressure from the Oversight Investigations Subcommittee now.

Mr. VAN WALKER. I believe reading the testimony on your web site will more than accomplish that, Mr. Chairman.

Mr. GREENWOOD. Thank you. Turn to Mr. Neuman again. In a memo that you wrote to HCFA on October 14, 1990, which is document number 10 in your binder, you alerted HCFA to the serious configuration problem with the IBM web servers. You identified this problem as a major vulnerability, because, "Anyone on the Internet can access internal HCFA systems." In particular, you focused on an architectural problem that the external HCFA web servers are, "dual-homed." Your testimony talks about the ease with which that attack was accomplished remotely and the lack of sophistication that was required.

In the memorandum you sent, document number 10, you state, "The web server had absolutely no protection from remote modification." In the full report you issued to HCFA about the successful attack, which is document number 11, you stated that, "The compromise of the external server allowed us, from the Internet, to send and receive arbitrary data with internal HCFA systems." What does that mean in lay terms, and can you explain what you could have done with this level of access to the web server if you had been intent on malicious activity?

Mr. NEUMAN. In layman terms, it means exactly that. From the Internet, we were able to access any system inside HCFA's network. No fire walls prevented us, no filters, nothing blocked us from connecting to any service, any server on the HCFA network. We weren't tasked to go any further than simply gaining access, so we weren't told to go and try to modify patient data or anything like that.

Mr. GREENWOOD. Okay. At the time of you work, in a report issued on October 27, 1999, which is document number 11, you recommended that HCFA discontinue dual homing of its web server to prevent someone from being able to do what you did—attack the web server to get access to internal networks and computer systems. Can you explain what it means for a web server to be, "dual-homed," and explain why that poses such a vulnerability for HCFA?

Mr. NEUMAN. Sure. This particular web server was connected both to the Internet and it had a separate distinct connection to the secured net. And through the secured net, it was connected into HCFA's internal network. So dual homing means it not only is connected to one network but two. And in fact in this particular machine, it was actually triple-homed. It was connected to the Internet, to the secured net, and to an IBM administrative network, which sat off somewhere else. We specifically were not allowed to test the IBM administrative network. We were not allowed the test the firewalls, any of the infrastructure, anything else there, just the web server itself, and from the web server find out what we can do to HCFA from there.

So there are more serious implications for this multi-homing. Eliminating the dual-home into the MDCN is good, but remember it is also still connected into the IBM administrative network. So if I can get into the administrative network, where can I go from there? There is lots of transitive trust issues which are interesting. A trusts B, B trusts C, therefore A trusts C. It is the same thing. So there are a lot of potential problems that exist, even with removing that back channel, because HCFA still has a connection to the MDCN. It is lots better than it was before. If you are going to attack HCFA, the most obvious target is to go to their web server. That avenue has been directly eliminated. But there are some indirect attacks which remain.

Mr. GREENWOOD. Yesterday, HCFA notified the committee that after 2 years it has finally decided to eliminate the backend web server connection that you exploited. Does this solve all the problems—I think you referred to this, but let me ask you formally, for the record—does this solve all the problems associated with remote penetration of HCFA's internal systems and its Medicare Data Communications Network?

Mr. NEUMAN. Not at all. It helps a lot, as I said. It does not completely solve the problem, because IBM is doing things that they don't tell us about. And we know for sure that they have multi-home systems that still exist. In addition, this is the way that they have been providing web servers for a long time. So not only is HCFA's web server dual-homed into the secured network and the Internet but all the web servers are. So, again, if you can break

into one of them, what does that mean to HCFA? There are some serious implications there.

Mr. GREENWOOD. Okay. Ms. Adair or Mr. Van Walker, either one of you, 2½ years ago you have got the recommendation about the dual homing. Nothing happens to respond to this in terms of the disconnection until a couple of days ago. One might have reason to think that the fact that you called yesterday to tell us that you made that disconnection might have something to do with this hearing. What happened in the intervening 2½ years? What caused you to decide a few days ago to disconnect? And what is the—is that a permanent change?

Ms. ADAIR. Excuse me. Immediately after the report that we got from En Garde, we did some corrective actions that we believe would assist us. There were some firewalls misconfigured that we had immediately corrected. It is true that——

Mr. GREENWOOD. Did you follow up and test those changes after you—test the system after you did this?

Ms. ADAIR. No, we did not. We did not. But in conversations that we had with some of your staff last week and when we went back and conversed amongst ourselves, we decided that, in taking another look at it—something we should always be doing in taking a look at security is looking and relooking—that it was indeed a risk that we no longer wanted to take. And so we, in fact, what is commonly referred to, I guess, is air-gapped ourselves from that. And we thought it was a prudent thing to be doing.

Mr. GREENWOOD. Does it create any problems for you?

Ms. ADAIR. It causes us, in order to update—I mean it is a web server to which we put public information out. It does cause a little bit more cumbersome process for us to be doing the uploading, but we have decided now that that is a burden that we are willing to take. I would, again, mention that subsequent to getting—immediately subsequent to getting—the report, changes were made in our updating relationship, changing the router, putting the communication in one way. But, again, in conversation last week with your staff, as we relooked at it, we decided to take an additional step in air-gapping.

Mr. GREENWOOD. We will keep these staff on board for a little while.

Mr. Neuman, back to document number 11. You recommended that HCFA, "Consider adding a substantial firewall between its secured network and the HCFA internal network." Why was this recommendation so important, and how would it have helped HCFA with its security problems?

Mr. NEUMAN. Well, the problem is that right now—well, at the time that I last tested, that this test was done, there is absolute trust of the secured network by HCFA. There is no protection there at all. There was no protection there at all. So putting all of your trust into a contractor that won't divulge its methods, that has had known vulnerabilities that we couldn't fully test seemed a prudent thing to do.

Mr. GREENWOOD. My understanding is that some of the contractors, the fiscal intermediaries, have in fact taken this recommendation and employed it. Is that your understanding?

Mr. NEUMAN. I have no knowledge.

Mr. GREENWOOD. Okay. Let me go back to you, Ms. Adair, if I could. I understand that HCFA chose not to implement either of En Garde's recommendations: discontinued dual homing of the web server between the Internet and HCFA's secured network, and also it chose not to add the recommended substantial firewall between the secured network and the internal network. As an attachment to document number 16, HCFA provided the subcommittee with an internal email in which a HCFA employee states—do you have that in front of you, document 16, "I had discussions with our techs, and we decided not to install the firewall to MDCN at this time. We know that this should be done, and we will do so once a plan is developed and after Y2K Day One." Y2K Day One was 18 months ago. Has HCFA added the firewall specifically recommended by Mr. Neuman and apparently agreed to by HCFA? And if not, why not?

Mr. VAN WALKER. Just one moment, please, Mr. Chairman.

Mr. GREENWOOD. Take your time.

Mr. VAN WALKER. I guess there are two points there, Mr. Chairman. In as far as the dual homing goes, just to recapitulate on that one, what HCFA did at the time, Mr. Neuman had actually recommended that we do those exchanges using a virtual private network, an encrypted Internet technology, a fairly standard technique. What HCFA chose to do during that period instead, prior to the air-gapping of this week that you have already discussed, was to establish a situation in which the HCFA connection into the web hosting forum at IBM was essentially a one-way path. Protections were placed on that circuit so that HCFA could move content up to IBM, but no one from the IBM facility could use that same circuit to get back down into HCFA and into its stated infrastructure. The step that we took this week was to actually create a machine that is not connected to anything else at HCFA at all to serve that purpose. That is what air-gapping means in this case.

As far as the extended network, HCFA's step for that protection is not to allow anyone who has access to MDCN to access any facilities at the HCFA Data Center or its other contractors. We use a technology or a process called access control list to determine which of our partners can do which things and use that then to filter, as you would, the traffic coming into HCFA. So it is not accurate to state that anyone who has access to the network can get to HCFA and get to the underlying resources. And we use this technology, I believe, on all of the HCFA routers. So, in a sense, the HCFA routers are providing a functionality similar to what firewalls would provide.

Mr. GREENWOOD. Well, let me ask Mr. Neuman if he would comment about that. You heard Mr. Walker's response. He seems to think that the routers are accomplishing what the firewall would have accomplished. It is my understanding that, again, that the—you said you didn't have information about this, but it is my understanding that some of the blues have—they don't have the trust of the network that you seem to have, and they have erected these firewalls. Let me first ask Mr. Neuman if you would respond to what you heard Mr. Walker say.

Mr. NEUMAN. I think it is possible to do filters correctly; again, it needs to be tested.

Mr. GREENWOOD. And you have not tested yours.

Mr. VAN WALKER. We have not conducted the type of third party penetration test, but we certainly have gone through the rules and reviewed them——

Mr. GREENWOOD. And that is because you have not been able to get that negotiated——

Mr. VAN WALKER. To conduct the type of test we talked about, sir, yes.

Mr. GREENWOOD. Ms. Adair, as part of the materials provided by your office to the subcommittee, HCFA provided document number 19, which describes HCFA's new contractor security initiative. This document, dated June 26, 2000, indicates that as of that time, HCFA's contractor security requirements were not current and had not been updated since 1992. Specifically noting that this was, "Before the days of email, Internet, hackers, viruses." It also states that current HCFA requirements, "Do not reflect requirements from GAO and IRS audit guides," and, "Don't include all requirements for HIPAA, which is the Health Insurance Portability Act, Presidential Decision Directive 63, HCFA internal policies or industry best practices."

I understand that on January 26, 2001 HCFA implemented a new security memorandum to program intermediaries, finally updating the outdated requirements, document 21, which is—document 21 describes what I just read. What is going on here and why did it take HCFA almost 10 years to update its outdated contractor security requirements?

Ms. ADAIR. I believe that during that time, since 1992, sir, what we had been doing is not necessarily updating our manual and putting in one place what all of our requirements were. We had been putting them out in individual memorandums to our contractors. We had been talking to them about them in meetings. And we felt that in starting down the path of our security initiative that it was important to bring them all up to date in one place and be very clear about what our expectations were to our contractors. That, in essence, putting out the clear expectations was the first way that we could start to really fulfill our oversight responsibilities. We needed to be clear about what our expectations were and what we were going to hold them responsible for.

Mr. GREENWOOD. In the reports provided to the subcommittee, the only penetration tests of Medicare contractor security that were provided were limited penetration tests conducted in 1998 of four specific Medicare contractors. This was a penetration test performed for HCFA by an independent accounting firm of only 4 of the over 55 Medicare contractors, and there does not appear to have been any more recent testing done by HCFA of its Medicare contractors. Why hasn't HCFA required more substantial testing of its Medicare contractors?

Ms. ADAIR. The four tests that you are referring to were of the Medicare contractors, we did do those and we used those as an opportunity for us to shape what our security initiatives should look like, that we needed some input as to what was the state of what was out there. And we used that as input.

There is a period of time in there, sir, that HCFA, as many other organizations, put a moratorium on much of our IT work as we were doing the remediation efforts for Y2K. Coming out of the Y2K

effort, however, we have put, as I indicated in my last answer, we have put out there a security initiative with what our expectations are. And the contractors right now are in the process of evaluating their own performance relative to our requirements. We will be talking to them about how it is they are going to get up to our standards, and we will be going back and testing subsequent to them making their remediations.

It is also important to note that during that period of time there were other avenues of oversight of our Medicare contractors in these areas. The IG does in fact do testing for the CFO audits. There are what we refer to as statement of auditing standards, which are internal control processes that happen at our contractor shops. These corrective actions come in to us, we evaluate them for reasonableness, and then ask them to follow up. In addition, the IG, after having done a full-blown CFO audit, the next year goes out and does a follow-up if there are findings. And we use the information of those to oversee our contractors.

Mr. GREENWOOD. Thank you. The Chair notes the arrival of the vice chair of the subcommittee, Mr. Whitfield. And if he is ready, recognizes the gentleman for 5 minutes for questions.

Mr. WHITFIELD. Mr. Chairman, thank you very much, and I apologize for being late to this important hearing. I was actually in another hearing, and delighted I made it over here before you all recessed or concluded your remarks.

Mr. Neuman, I was looking through this book last night, and this document 18 in the binder, the En Garde Systems document test report, which is dated June 7, 2000, was a test conducted by your company of HCFA's internal systems and internal penetration tests from the perspective of a HCFA employee that should not have access to sensitive data bases. Now, your report found quite serious problems in this desktop environment, which I understand HCFA has acknowledged and is moving to remedy. But the document on page 3 of that report says, "While it is clear that HCFA has put in place many of the proper precautions, the practice of creating all accounts with administrative permissions negates almost all the security precautions taken on the internal network." And I was wondering could you just elaborate or explain what that statement actually means or refers to?

Mr. NEUMAN. Sure. The way that the desktop PCs were set up there was no delineation between administrators who had complete access to everything on every system on the entire network and normal users. And, in fact, normal users had access to everything on every machine on every network. Once you have that level of access, it is trivial to gain access to anything else on the network you want to. You capture that machine, you watch and see them type passwords or log into machines or do whatever. You have unlimited access to PCs at that point.

So we feel that that is a significant risk in the sense, first of all, you really don't want average users to have unlimited permission; second, their ability to destroy things, even accidentally, is pretty high too, so there are both management and security reasons why you probably don't want this kind of setup.

Mr. WHITFIELD. But that is the current setup; is that correct?

Mr. NEUMAN. Well, we last tested early 2000 so I don't know.

Mr. WHITFIELD. Okay. This report also went on to say that "Problems reside with the policy and access configuration management and security administration. Several major findings include poor choice of administrator passwords by contractors, loosely configured network infrastructures, like printers and token ring cards, administrative privileges given to every new user."

And then on the next page, it reads, "That it was possible to obtain the encrypted passwords for accounts on the machine. We also downloaded, through the HCFA web proxy, that is a password cracking tool, and using this tool we were able to crack passwords on our machine. And then using those passwords were able to obtain further encrypted passwords from virtually every configured machine." I wondered can you describe just how easy it was to guess or crack these passwords, including those of the systems administrators who have unlimited access to the system?

Mr. NEUMAN. It was a trivial event. We found probably 50 to 60 passwords that were the users' name. So, for example, your user name is Whitfield, your password is Whitfield, that sort of thing. The administrator password, if I told it to you, you would laugh; it was that badly done.

Mr. WHITFIELD. Okay. Well, don't tell me then.

Of course you were not asked to fully penetrate the system, but based on the level of access that you were able to obtain, do you think you could have obtained sensitive—access sensitive medical information of Medicare beneficiaries?

Mr. NEUMAN. Without a doubt. I had the ability to control anybody's PC in the organization.

Mr. WHITFIELD. You did? Okay.

Now, Ms. Adair, to follow up on this, roughly 8 months after receiving that June 2000 report, HCFA hired another ethical hacker called Allied Technology to conduct essentially the same set of tests on your desktops. And Allied found virtually identical results, I have been told, and in fact document 23 in this binder says that "The security assessment of the HCFA work station environment shows that an internal user with normal access may uncover vulnerabilities during an exploit attempt of the HCFA network that would allow further exploit of the HCFA network enterprise and its connected systems."

And then it goes on to say that, "In its attempts to successively subvert several user and administrator passwords, Allied Technology discovered blank easily cracked and poorly managed passwords, both from user as well as administrator accounts." And then further down, it says that "Allied Technology was able to use remote-shared connectors to install a password-cracking tool downloaded from the Internet, which was then used to crack passwords on other shared systems."

So it would appear on these two sets of audit results that HCFA made virtually no progress in addressing the deficiencies identified in the prior year, including the basic actions such as preventing the downloading by HCFA employees of hacker tools on the Internet. Why not and why would HCFA spend the money to do the same battery of tests without taking some corrective actions?

Ms. ADAIR. Let me address, first, your question on the passwords. Passwords are something that we are working very hard on.

It is trying to convince people to not use easy passwords. It is a cultural change for individuals. We have a lot of numbers or passwords that we have to remember, for your ATM, for your whatever, and people have a tendency to want to use something such as their children's name, their last name. We are trying very hard to convince people that that is ripe for problems. We work difficult—we work—in trying to work—I am not saying this sentence well, I apologize. We are trying to work with them to enforce that those kinds of bad habits have unintended consequences for us.

In addition, we are exploring technology that we could use that would allow us to go in and take a look at passwords and notify people, "You have passwords that are way too easy. Let us move away from that." As well as something that would allow us, through technology, to enforce the policy standards that we have put out since that test result. We are making that kind of progress since that time.

Let me think what your other question was, sir. The systems administrator, as I understand it, is that we right now have allowed privileges at the desktop that I think that many of us would say should not be there. And the reason that we have done that is that we think there is, at this point in time, for us, an outweighing benefit, which is it allows us to push out anti-virus updates that we get on a timely basis that we would otherwise have to go out and touch each machine to do. And therefore it would not allow us, as effectively, to counteract such things as the Melissa or the "I Love You" virus that were out there.

We don't believe it is the best place for us to be, but in order for us to be there, we had to initiate from the first report a rather long life cycle to move us to a place, and we believe that we will be there in the November timeframe. As was discussed earlier, that when we get some of these findings, some of them are fixes that we can do within an hour. Other fixes take us a longer period of time in our complex environment to get us, and this was one of those fixes.

Mr. WHITFIELD. But do you feel comfortable in the progress you are making at this point?

Ms. ADAIR. I believe we are making progress. I certainly would like it to be faster progress.

Mr. WHITFIELD. So you don't feel comfortable with it.

Ms. ADAIR. I believe that we are doing what we can, yes.

Mr. WHITFIELD. Okay. Okay. Now, the Allied report also found that the HCFA network was susceptible to certain denial of service attacks, mostly due to HCFA's failure to stay up to date with software patches issued by your vendors. In fact, this report said that you are several service packs behind, leaving a system with dozens, if not hundreds, of known vulnerabilities. Now, why can't HCFA expedite the process of updating its patches?

Ms. ADAIR. Before we apply a patch, sir, to our system, we go through a rather rigorous testing scheme, and perhaps we, in that process, are not as quick as we could be.

Mr. WHITFIELD. You go through a what now?

Ms. ADAIR. Rigorous testing regime to make sure that the patch to the system we are putting in doesn't have an unintended consequence to something else or how we have set up our operation.

Mr. WHITFIELD. And that is pretty time consuming?

Ms. ADAIR. It can be, yes.

Mr. WHITFIELD. Mr. Chairman, I don't have any other questions.

Mr. GREENWOOD. Thank you. I just have a couple more questions. Let me address one to Mr. Vengrin. There is a document that was provided to us by HCFA that is dated October 14 of 1999, and it is number 8 in your binder, if you would turn to that. Got it? It references a penetration test conducted by your office's contractor, Ernst & Young, of HCFA's Central Office for fiscal year 1999.

The document states, "HCFA provided a detailed documented description of the testing to be performed and the list of IP addresses to be targeted. This is a deviation from the approach Ernst & Young has used for the other selected HCFA contractor sites and does not allow Ernst & Young to fully explore possible vulnerabilities and new exploits."

Can you explain why it is that HCFA took this approach to this test, how it differed from your tests of other HCFA contractor sites, and what the implications of these changes were for understanding the full extent of HCFA's central vulnerabilities?

Mr. VENGRIN. Yes, Mr. Chairman. And Ed can elaborate more on this. I believe our contractor was attempting to do more work, but HCFA was going to contract with others, such as En Garde, to do this work. And, therefore, the scope of the CFO work was to be curtailed and cut back. So a lot of the Central Office work that we had planned under the auspices of the CFO Act just has not been performed since fiscal year 1997.

Mr. GREENWOOD. Ms. Adair, do you concur with that? Or Mr. Van Walker, either of you.

Ms. ADAIR. Pardon me, I am sorry?

Mr. GREENWOOD. Either one of you, do you concur with that assessment?

Ms. ADAIR. As you know, we have engaged contractors to take a look at ourselves, and I believe that we do want to work with the IG to ensure that we are not duplicating but in fact complementing our work efforts, that we would not want to—both of us have precious resources, and we would want to ensure that they went as far as they could.

Mr. WHITFIELD. Just one more question. Mr. Vengrin, in your fiscal year 2000 audit report, which was document 22 in our book here, you stated that on several occasions that internal users of the Medicare system had inappropriate access to sensitive beneficiary information. And I was wondering if you might just be able to describe some of the examples from your individual site reports?

Mr. VENGRIN. Yes, sir. We noted cases in which programmers had inappropriate access to system logs. This provided an opportunity to conceal improper actions and obviated the log's effectiveness as "detect" controls. There were a number of cases where the programmer had inappropriate access to beneficiary history files. There should be a segregation of duties so that a programmer would not have access to this level of production. That would give them an opportunity to go in there and possibly effectuate a payment. We found numerous instances of these types of problems.

Mr. WHITFIELD. Where they effectuated a payment?

Mr. VENGRIN. No, sir; where there is an opportunity.

Mr. WHITFIELD. An opportunity.

Mr. VENGRIN. Yes, sir.

Mr. WHITFIELD. Okay.

Mr. VENGRIN. There is just the potential.

Mr. WHITFIELD. All right. Now, this same report also discusses the external threat to the contractor systems. How real do you think that the Internet-based threat is at the contractor sites?

Mr. VENGRIN. Sir, unfortunately, we have been doing a very low level of testing. That said, vulnerabilities have been detected through footprint analysis and some of the war dialing. We have identified cases where manufacturers' identification of passwords was left on. Second, very, very simplistic passwords were identified. For example, "manage" or "manager." We could actually do a penetration test had we been permitted to go further. So we noted numerous instances where passwords were a problem.

Mr. WHITFIELD. Okay.

Mr. MEYERS. If I may add to that.

Mr. WHITFIELD. Yes, sir.

Mr. MEYERS. Additionally, when you are trying to make a determination on the risk, you sort of have to look at it as a math formula. You have a vulnerability, and we know that vulnerabilities exist in these systems. You then have to factor in whatever potential impact there may be to that vulnerability, and then offset it with the controls that are present.

As HCFA goes through its current information security reassessments and enhancements, that business impact, that financial impact potential has to now be rolled into all the identified vulnerabilities that we know are present. Once you do that, then you come up with the appropriate countermeasure or control, and your risk then becomes a management decision as to "Do I want to accept this level of risk; can I live with it, or is it a situation where the controls have to be augmented immediately?" But the benefit and the cost cannot adequately be addressed until you factor in the potential impact of all the identified vulnerabilities.

Mr. WHITFIELD. Okay. Thank you. I appreciate that comment.

Mr. GREENWOOD. Thank you, Mr. Whitfield.

One final question for Ms. Adair, and then we will break for lunch. We will adjourn the hearing. Tell us what HCFA's computer security resources consist of. How many people do you have focused specifically on computer security to monitor daily network and web hosting transactions, to evaluation operational procedures, to ensure staff and contractor compliance of security requirements, and to recommend enhanced security policies? How many people do you have doing this? Are we looking at them?

Ms. ADAIR. No, sir. We fortunately have more than this. We actually have—we have doubled the number of people like in the last 3 years that are dedicated to computer security. I would say that we have gone from somewhere in the 30 area, and we are now essentially at 60 FTEs. And I point that out, because it is not necessarily people per se, but sometimes they are in our—for example, in our regional office, those that are going out and doing the oversight of our Medicare contractors. They may be doing some other

additional activities. So I think that we have made some great strides there.

Mr. GREENWOOD. Have you made a specific request for additional funds from the $30 million that the Secretary has testified before one of our subcommittees that he intends to seek for computer security purposes?

Ms. ADAIR. As you point out, sir, that is in the budget request this year, so we have not yet made any requests against it. It has not yet been appropriated. I think that we would certainly view that as additional security needs come up that we would apply, I think would be the right words, for those funds should it be appropriated.

Mr. GREENWOOD. Okay. We thank you. One suggestion I might make is that you said that with regard to passwords that you are encouraging your employees to change their passwords. You might want to just tell them to do that.

Ms. ADAIR. And I probably did not say it. We have changed the policy, and it is. If I may take a second of your time?

Mr. GREENWOOD. Please.

Ms. ADAIR. It was, I think, earlier this month at about the time that I was talking to your staff that I was addressing a security session that we had in our auditorium, and I took the opportunity at that time to tell our staff not only that we were having conversations with you and use that to in fact enforce to our staff how important this was, but at the same time to discuss the passwords. So hopefully the two of those being mentioned together was of assistance to us.

Mr. GREENWOOD. Okay. Thank you.

Ms. ADAIR. Thank you.

Mr. GREENWOOD. When I came to Congress 8 years ago, I remember that the Congressional Institute put on a conference that they annually do, and all of the Members of Congress went out to conference for a couple of days. And one of the things that they had available to us was an opportunity to surf the World Wide Web, and nobody knew what it was. And I think that is telling all of this has happened very quickly. This technology has emerged very quickly and changed the way we do business. This whole hearing would have been completely unintelligible to people just a very few years ago. So we know that the technology changes very quickly, that the challenges emerge very quickly.

As I said in the beginning, we are pleased with much of what HCFA has done. I think this whole process leading up to this hearing as well as today's dialog gives us—hopefully gives HCFA some direction as to what our expectations are. Hopefully the recommendations that I specifically made in my opening statement—I will provide you written copies of that if you would like—will be implemented, particularly in connection with the new contracts that you are in the process of negotiating. We look forward to working with you in the future to follow up on these discussions. And thank you again for being here.

I would ask unanimous consent to enter into the official record all of the documents that we have referenced today. Hearing no objections, it is so ordered.

Mr. GREENWOOD. Thank you again, and the hearing is adjourned.

[Whereupon, at 12 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.0 INCORPORATION OF CONTRACTOR'S PROPOSAL

a. The contractor's technical proposal entitled Medicare Data Communications Network, Proposal Number 282A-01 of September 30, 1996 and revised 282A-02, Rev. 1 of October 30, 1996 for items 0001 through 1050 and technical change pages received from Advantis through December 20, 1996, submitted in response to HCFA-RFP-96-0004 for MDCN and amendments 0001 and 0002 are hereby incorporated by reference and made a part of this contract. Remaining known issues are to be resolved in accordance with the codicil to this contract. In the event of any further inconsistency between the provisions of this contract and the contractor's technical proposal as referenced above, the inconsistency shall be resolved by giving precedence in the following order: (a) Schedule, (b) FAR clauses incorporated under Section I, (c) contractor's technical proposal, and (d) other provisioins of the contract, whether incorporated by reference or otherwise.

C.1 INTRODUCTION TO STATEMENT OF WORK

a. Independently and not as an agent of the Government, the Contractor shall be required to furnish all the necessary services, qualified personnel, material, equipment, and facilities, not otherwise provided by the Government, as needed to perform the Statement of Work.

b. This Statement of Work (SOW) describes the tasks, activities, telecommunications services, and work products associated with the Medicare Data Communications Network (MDCN) which is being procured to support ongoing and improved processing of Medicare claims.

C.1.1 Background

C.1.1.1 The Medicare Program

Medicare is a Federal Health Insurance Program whose beneficiaries include persons 65 years of age or over, disabled persons, and persons with chronic renal disorders. The program was established by Congress in 1965, when it enacted Title XVIII of the Social Security Act. The Medicare program consists of two distinct parts:

A. Hospital Insurance, which covers expenses of medical services furnished in an institutional setting, such as a hospital or skilled nursing facility, or provided by a home health agency; and

B. Supplemental Medical Insurance, which covers physician services, certain other medical equipment and services, and other outpatient services.

Baseline phase in anticipation of supporting the requirements to be imposed in later phases. This performance monitoring shall be parsed ao as to characterize users by batch *vs.* interactive traffic and by traffic or classes of transactions which are I/O intensive *vs.* computationally intensive.

Table C. 8 - MDCN Performance Requirements

Attribute	Performance Requirement	
	Baseline CWF Goals	Draft MTS-Related Requirements
Response time for interactive network traffic	> 90% @ < 3 sec	Network portion: > 90% @ < 1.2 sec
Probability of a busy signal for dial-in traffic	< 0.01	< 0.01
Network availability	> 0.995	> 0.9999
CPE availability	> 0.995	> 0.9999
Individual line availability	> 0.995	> 0.9999
Bit Error Rate	< 10E-07	< 10E-05

There shall be no single point of failure in the network..

The MDCN shall provide diverse routing for backup and for disaster recovery and support of business resumption.

Network availability requirements are constrained by the operational hours defined for the MTS system. Most operations are limited to six days a week, twenty hours a day (6x20), alloting adequate time for normal maintenance and tuning activities. Only one function requires 7x24 availability, namely the ability for health care providers to verify the Medicare eligibility of a beneficiary. The requirement to exercise this function will likely be limited to nighttime or weekend visits of beneficiaries to health care facilities where the beneficiaries are not established patients-of-record. The relative infrequency of this function should have minimal (if any) impact on network design or operations, provided that Advantis does not routinely take the entire network down for the same time period. No user's primary and secondary ACS may be unavailable at the same time. Further, beyond pre-approved, scheduled downtime, Advantis will be subject to HCFA sanctions for unavailability and/or unreliability.

C.2.9 *Global MDCN Security Requirements*

MDCN security shall be provided/maintained/assured by the Contractor in order to prevent unauthorized physical, electronic, or virtual access to telecommunications facilities, to MDCN hardware or software components and to telecommunications services. Encryption is not a current requirement for Advantis' support of the MDCN network for external MTS users.

The MDCN Contractor shall report intrusions, suspected intrusions, and any anomalies in the characteristics and connectivities of MDCN traffic flow.

United States Department of Health and Human Services

Accountability Report: Fiscal Year 1997

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REPORT ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES CONSOLIDATED FINANCIAL STATEMENTS FOR FISCAL YEAR 1997

JUNE GIBBS BROWN
Inspector General

APRIL 1, 1998
A-17-98-00001

quarterly, PMS should provide operating divisions with a detailed listing of individual grant advance balances summarized by appropriation.

- Determine whether operating divisions have established effective internal controls, i.e., user controls, to ensure that PMS data is complete, reliable, and accurate. These user controls are identified in OIG's *"Report on Department of Health and Human Services, Program Support Center, Division of Payment Management's Policies and Procedures in Operation and Tests of Operating Effectiveness"* (CIN: A-17-97-00011).

5. Electronic Data Processing (EDP) Systems Controls

Weaknesses in EDP systems controls affected eight operating divisions (ACF, CDC, HCFA, HRSA, IHS, NIH, SAMHSA, and PSC). The chart on page 22 summarizes some of the systemic internal control weaknesses, either reportable conditions or material weaknesses, identified during the audits of operating divisions' financial statements or service organizations' operations. Other weaknesses are reported in the individual reports on these entities.

Of particular concern are the HCFA central office's general controls, which continue to be ineffective. Controls associated with the general data processing environment (general controls) are critical to ensuring the reliability, confidentiality, and availability of data. However, we found deficiencies in a number of general controls at the HCFA central office and/or multiple contractor sites. We consider the weakness in HCFA central office access controls to be material. We also identified specific application controls at two Medicare contractors as a material weakness.

Control deficiencies in the HHS Central Payroll System, which is operated by PSC's Human Resources Service (HRS), were first noted in our FY 1996 audit. These deficiencies affect all HHS operating and staff divisions. We consider the weaknesses in the Central Payroll System's error correction module (an application control) to be material.

Audit Areas	HCFA		NIH	ACF	SAMHSA	HRSA	IHS	CDC	HHS Central Payroll
	Central Office	Medicare Contractors							
General Controls									
Entity-Wide Security Program	R	**							
System Access	M	**		R	R	R	R		R
Application Software Development and Change Control	R	**		R	R	R	R	R	R
Segregation of Duties	R	**						R	R
Access to System Software/ Software Maintenance	R	**	R	R	R	R	R		
Service Continuity/ Contingency Planning	R	**						R	R
Application Controls									
Input, Processing, and Output Controls		M***		R	R	R	R		M

M = Material Weakness; R= Reportable Condition.

*** See Inspector General's Report on the Health Care Financing Administration's Financial Statements for Fiscal Year 1997 (CIN: A-17-97-00097).*

****Application control weaknesses at two Medicare contractors.* [redacted] *are considered material. See OIG report A-17-97-00097 for other internal control weaknesses.*

Background

- **HCFA Central Office and Medicare Contractors**. For FY 1997, HCFA relied on extensive data processing operations at its own offices and at contractors that process and account for $212 billion in Medicare expenditures. The HCFA central office computer center primarily maintains administrative data, such as Medicare enrollment, eligibility, and paid claims data, but it also processes all payments for managed care.

  Medicare contractors use one of several "shared" systems to process and pay Medicare fee-for-service claims. The shared systems interface with the Common Working File (CWF) to obtain authorization to pay claims.

- ***PSC.*** The PSC operates the Payment Management System, which processes grant awards and advances for the Department as well as many other Federal agencies. The PSC's HRS is responsible for the HHS Central Personnel and Payroll System. The PSC's DFO provides financial management and accounting services to ACF, IHS, HRSA, and SAMHSA.

- **Division of Computer Research and Technology (DCRT).** This service organization processes transactions for the accounting systems used by HRSA, IHS, FDA, NIH, and SAMHSA. The DCRT also processes transactions for PMS and the Central Personnel and Payroll System.

- ***CDC.*** The CDC processes accounting transactions at its data center for itself and the ACF accounting system.

5a. Entity-Wide Security Program

- ***HCFA Central Office.*** The HCFA's entity-wide security program should provide a framework for managing risk, developing security policies, assigning responsibility, and monitoring the adequacy of computer-related controls. However, our 1997 work disclosed that HCFA had not performed risk analyses, developed security plans, or ensured that proper corrective action was taken for its general support systems, including the computer center, telecommunications and networks, and significant applications. In addition, the security structure was not adequate to ensure that security program objectives are achieved.

5b. Systems Access

- ***HCFA Central Office.*** Data security remains a major concern at the HCFA central office. Our prior-year review demonstrated weaknesses in EDP general controls through a system penetration test in which we obtained access privileges to read or modify sensitive Medicare enrollment, beneficiary, provider, and payment information. Although HCFA immediately corrected the prior-year vulnerabilities, our current-year tests resulted in penetrating the mainframe database. We obtained the capability to modify managed care production files.

  Furthermore, we found that data center users without specific authorization to the managed care system have the potential to gain update access to those same files. Although HCFA made improvements in this area during FY 1996, additional effort is necessary to fully secure the mainframe database. Moreover, our system penetration test revealed additional control problems which could be exploited by

unauthorized individuals to compromise one or more of HCFA's computer systems. Following our fieldwork, HCFA initiated an in-depth security self-assessment, including a sophisticated network penetration test disclosing several weaknesses. The HCFA is actively developing an appropriate corrective action plan.

- ***ACF, HRSA, IHS, and SAMHSA.*** A reportable condition was noted at the operating divisions that use DFO accounting systems because DFO did not revoke systems access of departing employees until they had completed the clearance process. This delay could provide disgruntled employees with an opportunity to alter or compromise systems.

- ***HHS-Wide (Central Payroll System).*** The HRS protects a limited number of data files by a security software program. No attempt has been made to assess the risk of not protecting other mission-critical files. Further, no written criteria have been established to guide security personnel in monitoring and restricting access to data and production program files. Programmers have been granted write-access to production data sets.

5c. Application Software Development and Change Control

- ***HCFA Central Office.*** Serious weaknesses in application development and change controls are still outstanding from the FY 1996 audit. The centralized production control group controlled only about 15 percent of the production batch programs. The HCFA risks implementing unauthorized programs, which could result in improper processing of Medicare claims or eligibility information or allow malicious programming changes that could interrupt data processing or destroy data files and programs.

- ***CDC.*** Changes to production files cannot be verified using the existing change control documentation. Since CDC does not use change control software, the only date that can be verified is the date the production file was last changed. Therefore, individual program migration changes cannot be verified to the systems to ensure that all requested changes were made.

- ***ACF, IHS, HRSA, and SAMHSA.*** A reportable condition was noted at the operating divisions that use DFO accounting systems because of a lack of control over personnel with access to the DFO production library. As a result, any program can be changed without authorization or oversight.

- ***HHS-Wide (Central Payroll System).*** The controls and security measures surrounding the HRS application maintenance process do not adequately protect the integrity of application systems. This problem increases the risk of errors or irregularities in production processing. Further, access controls do not adequately protect production programs and data sets from modifications. Programmers have access to production programs and can make manual modifications which do not leave an audit trail.

5d. Segregation of Duties

- ***HCFA Central Office.*** The HCFA has not addressed the segregation of duties issue identified in our FY 1996 audit. Electronic data processing functions were not adequately separated to prevent one individual from controlling key aspects of computer-related operations.

- ***CDC.*** The CDC database administrator is also responsible for overall systems development activities in a project leader capacity. The duties should be segregated due to the sensitive nature of having ongoing access to all production files, data tables, and extract files used to develop financial reports for management review. The CDC is taking steps to address this condition.

- ***HHS-Wide (Central Payroll System).*** The systems integrity function at HRS was transferred to its programming division. This reorganization placed two incompatible functions in the same division.

5e. Access to System Software/Software Maintenance

- ***HCFA Central Office.*** Controls over operating system software integrity remain ineffective. As noted in our FY 1996 audit, this software was not adequately restricted, and HCFA still allows an excessive number of contractors and systems personnel to have update access to the software. This excessive access increases the risk of accidental corruption of the operating system. In addition, the operating system software parameters could be overridden during system generation or "reboots," which could result in a different mainframe configuration.

- ***DCRT.*** Deficiencies were found in monitoring access privileges to the computer machine room. As such, there was no assurance that physical access to the computer center was restricted to authorized persons. This reportable condition impacts the operating divisions using DCRT facilities.

- ***ACF, HRSA, IHS, and SAMHSA***. A reportable condition was noted at the operating divisions that use the DFO accounting systems because DFO did not have a written policy describing its accounting system maintenance policy and the feeder system interfaces. The lack of a written policy increases the risk that normal operations could be disrupted.

5f. Service Continuity/Contingency Planning

- ***HCFA Central Office***. Serious weaknesses in service continuity controls have not been resolved. These controls should ensure that critical operations continue without interruption or are promptly resumed and that critical and sensitive data is protected when unexpected events occur. The HCFA has not updated its critical application list in the contingency planning document since 1992. Because several applications have been developed, modified, or combined since then, HCFA's contingency plan cannot ensure that its critical applications would be promptly restored in the event of a disaster.

- ***CDC***. The CDC has informally documented its disaster recovery tests. The latest formal documentation, which should provide essential information to CDC's Financial Management Office, was dated 1994.

- ***HHS-Wide (Central Payroll System)***. The HRS does not have an up-to-date disaster recovery plan. Its continuity of operations plan dates to 1990, although its current computer operations have changed significantly since then. The Commissioned Officer payroll system, which is part of the central payroll system, also does not have a disaster recovery plan.

5g. Application Controls

- ***Medicare Contractors***. We noted material control weaknesses related to the [redacted]). For [redacted], data centers had full access to the source code and could make local changes to [redacted] programs. These changes were not subjected to the same controls that exist in the standard [redacted] change process. Additionally, one data center developed an override library to give priority to locally modified [redacted] programs. Consequently, the local programs always override the standard [redacted] programs provided by the maintainer. For the [redacted], each individual carrier could deactivate HCFA-mandated edits. The lack of a controlled modification process over the shared systems does not ensure that only authorized programs are implemented and executed by fiscal intermediaries and carriers.

- ***DFO Accounting Systems.*** A reportable condition was identified at four operating divisions (ACF, HRSA, IHS, and SAMHSA) because DFO staff did not always ensure that data transmitted to the two general ledger systems, CORE or HAS, was accurately received. The DFO did not have procedures to direct its staff on how and when to check that feeder system output matched CORE or HAS input data, how to reconcile the data, and when to make adjustments. Although DFO noted that CORE is being programmed to automatically verify that data sent by the feeder systems matches data received by CORE, procedures will still be needed to require checking and follow-up on the exception reports produced by the system. The DFO also noted that HAS is scheduled to be replaced.

- ***HHS-Wide (Central Payroll System).*** We found that the Payroll Error Correction System (PECS) control that limits corrections to 25 percent of base pay had been turned off. Therefore, employees with passwords could make corrections to their pay (and that of others) that would result in a pay increase of 100 percent or more. The PECS will also accept duplicate corrections. In fact, operating divisions have reported cases of duplicate corrections being submitted and paid. The PECS also does not flag unusual transactions or trends, e.g., corrections can be made to the same person's pay indefinitely without raising concern.

Recommendations. Specific recommendations to the operating divisions and service organizations are covered in the separate reports. In summary, we recommend that (1) systems access be properly controlled, passwords be granted consistent with assigned responsibilities, and password changes be periodically required; (2) application development and program change control procedures be in place to protect against unauthorized changes; (3) computer-related duties be properly segregated; and (4) service continuity plans be kept current and periodically tested.

We also recommend that ASMB oversee the implementation of these corrective actions.

REPORTABLE CONDITIONS

1. Property, Plant, and Equipment

Although CDC, IHS, and SAMHSA improved their accounting and control of property, plant, and equipment (PPE), additional corrective action is still needed at NIH and FDA.

- **NIH.** An annual inventory provides assurance that the recorded amount of PPE is complete and accurate. However, NIH has not taken a complete physical inventory of its PPE, totaling $345 million, net, for 4 years. When inventories

Jim McGeahy
Telephone: (702) 565-7334
Facsimile: (702) 565-6047

En Garde Systems, Inc.

22

Fax Memo

To: Eva Jun

From: Jim McGeahy

CC: File

Date: 11/16/98

Re: Penetration Testing -- IGS/SecureNET

[SECURED NETWORK] [SECURED NETWORK] [Secured network

Dear Eva:

Given the trust vested in [redacted], provisions for independent, third party penetration testing should be negotiated with IGS and added to the [redacted] contract. Recommend at least annual testing of all servers hosted by IGS and the [redacted] Firewall maintained by IGS for HCFA; this testing should supplement any testing/"ethical hacking" accomplished by IBM. In addition, recommend testing to verify that HCFA cannot be reached from the Internet through [redacted], or from another customer site on the [redacted]. All such testing should focus on the effectiveness of security controls/mechanisms to implement HCFA policy, including a review of all applicable router/firewall access lists. Testing should be non-disruptive, but otherwise unrestricted in terms of scope, with results provided directly to HCFA. IGS can be furnished a summary report of findings and recommendations, but not be given full details of the methods and techniques employed for the tests.

ECURED NETWORK]

I hope this helps. Please call me at (702) 565-7334 or send an email to mcgeahy@engarde.com if you have any questions or require additional information.

Best regards,

Jim McGeahy
CEO

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 2 PAGES

IMPORTANT : Mark all packages and papers with contract and/or order numbers.

1 DATE OF ORDER: 07/06/1999
2 CONTRACT NO. (If any): GS35F5927H
3 ORDER NO: HCFA-99-1103
4 REQUISITION/REFERENCE NO: 770-9-030007

5 ISSUING OFFICE (Address correspondence to):
HEALTH CARE FINANCING ADMIN
ACQUISITION & GRANTS GROUP
7500 SECURITY BLVD.
BALTIMORE MD 21244-1850

6 SHIP TO
a. NAME OF CONSIGNEE: HCFA/DHES/SSG
b. STREET ADDRESS: N2-14-17
7500 SECURITY BLVD.
c. CITY: BALTIMORE
d. STATE: MD
e. ZIP CODE: 21244-1850
f. SHIP VIA

7. TO
a. NAME OF CONTRACTOR: [redacted]
b. COMPANY NAME: EG&G
c. STREET ADDRESS: 10687 GASKINS WAY
d. CITY: MANASSAS
e. STATE: VA
f. ZIP CODE: 20109

8. TYPE OF ORDER
☐ a. PURCHASE
REFERENCE YOUR MAY 25, 1999
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheets, if any, including delivery as indicated.
☒ b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATIONS DATA
7590511 95997633 257W

10. REQUISITIONING OFFICE

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☐ a. SMALL ☐ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED

12. F.O.B. POINT: Destination
13. PLACE OF
a. INSPECTION: Destination
b. ACCEPTANCE: Destination
14. GOVERNMENT B/L NO:
15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date): 07/05/2000
16. DISCOUNT TERMS: Net 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Tax ID Number: 042052042 Provide HCFA with support services to perform the Tasks described in Attachment 1. The Period of Performance: July 06, 1999 through July 05, 2000 The delivery schedule is provided in Attachment 1 for each Task. Continued ...					

18. SHIPPING POINT
19. GROSS SHIPPING WEIGHT
20. INVOICE NO.
17(h). TOT. (Cont. pages): $124,851.72

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO
a. NAME: DHHS,HCFA,OFM,FSG
b. STREET ADDRESS (or P.O. Box): Div. of Financial Operations, P.O. Box 7520
c. CITY: Baltimore
d. STATE: MD
e. ZIP CODE: 21207-0520

17(i). GRAND TOTAL: $124,851.72

22. UNITED STATES OF AMERICA
BY (Signature): M.K. Markman

23. NAME (Typed): M.K. MARKMAN
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

OPTIONAL FORM 347 (Rev. 6/95)
Prescribed by GSA, FAR(48 CFR) 53.213(e)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE 2 OF 2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 07/06/1999 | CONTRACT NO GS35F5927H | ORDER NO HCFA-99-1103

ITEM NO (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	The HCFA Project Officer is John McGuire ([redacted]). Each Invoice will be approved by the Project Officer and the Contract Specialist prior to payment.					
0001	Obligated Amount: $124,851.72				124851.72	
	Total amount of award: $124,851.72. The obligation for this award is shown in box 17(j).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

ATTACHMENT 1

TECHNICAL SECURITY SERVICES AND ENGINEERING SUPPORT

I. BACKGROUND

The Health Care Financing Administration (HCFA) is the agency of the Federal Government which administers the Medicare and Medicaid programs. In this capacity, HCFA is responsible for the payment of over $300 billion for medical services rendered to the nearly 90 million beneficiaries and recipients of these programs. HCFA currently has approximately 4,000 employees at its central site in Baltimore, and in ten (10) Regional Offices in major cities throughout the country. HCFA contracts with approximately 80 companies to process claims for reimbursement for medical services rendered under the Medicare program, and also works with all 50 states in the management of the Medicaid program.

In the administration of these programs, much of the data and information collected, especially that relating to individuals, is of a private nature. Access to all such information is controlled by the Privacy Act of 1974, as amended, and the Computer Security Act of 1987, as well as various rules, regulations, policies and guidelines promulgated by the Department of Health and Human Services (DHHS), the Office of Management and Budget (OMB), and the National Institutes of Standards and Technology (NIST).

In order to meet these legal and regulatory requirements, HCFA has embarked upon a comprehensive systems security program. This program encompasses a variety of activities, ranging from the development and implementation of systems security policies and procedures to the testing and review of existing hardware and software applications.

II. PURPOSE AND SCOPE

A. PURPOSE

The purpose of this Statement of Work(SOW) is to obtain support services to:
perform security testing of Medicare Data Communications network services provided by IBM Global Services (IGS);
- conduct network security reviews of the HCFA Enterprise Network; and,

- support HCFA in the planning, design, implementation and evaluation of changes to the HCFA security infrastructure.

B. SCOPE

The contractor shall work with HCFA in a variety of areas and activities related to security testing, network security review, and other technical security services. Specifically, the contractor shall perform a security review of IGS to validate the security of the services provided by IGS, and ensure that protection measures have been put in place to effectively implement HCFA security policy.

The contractor shall also perform a thorough review of the security status of the HCFA Enterprise Network. This effort is to be specifically focused upon problem areas previously identified by previous security audits and penetration testing, and upon changes to the HCFA secure network configuration.

The contractor shall also provide technical security services, including planning, design, development, implementation and evaluation of changes and modifications made to the HCFA enterprise security infrastructure.

III. DESCRIPTION OF TASKS

Independently, and not as an agent of the government, the contractor shall furnish all the necessary services, qualified personnel, material, equipment, and facilities not otherwise provided by the government, as needed to perform the requirements of the Statement of Work.

A. Task 1 - IGS Security Testing

HCFA has contracted with IBM Global Services (IGS) for Internet, Private Network, and Content Hosting Services. Under the terms of this contract, HCFA has levied requirements for twice annual testing to validate the security of services provided by IGS, and ensure that protection measures that have been put in place by IGS effectively implement HCFA security policy. IGS Testing shall be accomplished in accordance with phased task plan described below.

1. Assess Internet Vulnerability

Review the IGS protections between the Internet and the HCFA external web server. (Review of access control lists)

Review the IGS protections between the Internet and the HCFA internal web server. (Review of access lists)

collateral risk (i.e. if the external web server is compromised, there are no protections between the web server and the HCFA internal network)

Test the HCFA external web server system and web service for vulnerabilities in services (CGI scripts, etc.)

Review the IGS protections between the Internet and the HCFA internal network (Review access lists)

2. **Assess MDCN Partner Vulnerability**

Review the IGS protections between MDCN partners and the HCFA internal network (Review access lists)

If necessary, test vulnerability from an MDCN partner

3. **Assess Non-MDCN IGS SecureNet Vulnerability**

Review the IGS protections between non-MDCN IGS customers and the HCFA internal network.

If necessary, test vulnerability of a non-MDCN IGS costumer.

The contractor shall review technical documentation and configuration files, and perform scans and tests as necessary to evaluate the security of IGS managed HCFA connections and resources, and assess risks. Preliminary work, including scans and tests will be limited to those necessary to identify potential weaknesses or vulnerabilities that could be exploited to compromise HCFA resources and/or intrude into the HCFA internal network. Accordingly, upon completion preliminary scans, tests, and documentation reviews, HCFA will be briefed and provided with a test plan that:

- (I) summarizes preliminary findings;

- (ii) describes additional tests that should be conducted to further evaluate identified weaknesses/vulnerabilities; and,

- (iii) discusses the risks associated with such additional tests.

A separate briefing will be presented to IGS. Additional tests to exploit such potential vulnerabilities will not be conducted unless specifically approved by HCFA and agreed to by IGS.

All work will be non-disruptive, and closely coordinated with HCFA and IGS. All testing will be conducted from the HCFA site. Significant findings that represent an imminent risk to HCFA resources will be reported immediately upon their discovery. Under no circumstances will IGS operations be disrupted, or systems placed at risk during testing; any probes and tests will be nondestructive.

Upon completion of all testing, the vulnerabilities or system weaknesses discovered, verified, and/or demonstrated through the testing process will be carefully analyzed to assess risks and

formulate countermeasures or other actions that can be taken to mitigate risk. Wherever possible the contractor will recommend specific security patches, and/or configuration or procedural changes.

Due Dates

All findings and recommendations will be incorporated in a detailed written report and delivered to HCFA within three weeks of completion of all tests. A "sanitized" version of this report will be prepared for distribution to IGS, and delivered at the same time.

The due date for this task shall be on or before 01/31/2000.

B. Task 2 - HCFA Network Security Review

During FY98 and Q1-FY99, the HCFA Enterprise Network was subjected to an extensive security review, including a desk-top review of security policies, procedures, and configuration documentation, and penetration testing and a vulnerability analysis. As a result of this review, action items were identified and coordinated to fix system and network vulnerabilities and configuration liabilities, correct administrative deficiencies, and implement changes to the network (security) architecture. In preparation for the OIG FY 1999 audit, the status of corrective actions must be reviewed, and the current state of Enterprise Network security must be re-assessed. This review and assessment shall be accomplished in accordance with the task plan described below.

1. **Review and Determine Status of Action Items**

   Conduct Interviews and Review Documentation
   Review Aperture Configuration Output

2. **Assess Current State of Network Security**

   Review Technical Documentation and Configuration Files.
   Perform Scans and Conduct Tests as Required.

The contractor shall assist HCFA in preparations for the OIG FY 1999 audit by reviewing and documenting the status of corrective actions and changes to the network security configuration as a result of FY98 security reviews, testing, and architecture studies. The contractor shall supplement this review with scans and security testing as necessary to assess the current state of HCFA network security. Work to be performed shall include, but not be limited to interviews of key persons on the HCFA management and technical staff (including contractors), and a review of all pertinent documentation and configuration files to determine the status of corrective actions. In addition, contractor security scans and testing shall be accomplished to

the extent necessary to determine if controls that are currently in place on critical network components (firewalls, routers, and servers) effectively implement HCFA security policy. The combined results of these reviews and tests shall be used to analyze risks, and assess the current state of HCFA network security.

All testing will be non-disruptive, and closely coordinated with HCFA. All testing will be accomplished on-site. Significant findings that represent an imminent risk to HCFA resources will be reported immediately upon their discovery. Under no circumstances will HCFA operations be disrupted, or systems placed at risk during testing; any probes and tests will be nondestructive.

Upon completion of all testing, vulnerabilities or system weaknesses discovered, verified, and/or demonstrated through the testing process will be carefully analyzed to assess risks and formulate countermeasures or other actions that can be taken to mitigate risk. Wherever possible the contractor shall recommend specific security patches, and/or configuration or procedural changes. The HCFA staff will be briefed on all preliminary findings and recommendations.

Due Dates

All such findings and recommendations will be incorporated in a detailed written report and delivered to HCFA within three weeks of completion of all tests.

The due date for this task shall be on or before 10/31/2000.

C. Task 3 - Technical Security Services

The HCFA Enterprise network is undergoing extensive changes to more efficiently and effectively meet HCFA business requirements, and improve network security. Changes to the secure configuration of the network architecture, and critical network components and interfaces must be carefully evaluated, planned, designed, implemented and tested to ensure that each change is appropriate and correct, and effectively implements HCFA security policy. The work to accomplish this may include security engineering, penetration testing and vulnerability analysis of systems and networks, trade studies, architectural studies, source code audits, security training, and expert consultation on all technical aspects of computer and network security.

The contractor shall provide skilled and experienced personnel with expertise in the technical aspects of computer and network security to consult with HCFA staff, and assist HCFA evaluate, plan, design, implement and test changes to the secure configuration of the HCFA Enterprise Network. To accomplish, the contractor shall perform the following and similar tasks, as required by HCFA:

1. Participation in working groups and deliberations concerning proposed

changes to the HCFA IT architecture to provide expert consultation as might be required to help HCFA evaluate the effect of those changes on the security configuration of the network.

2. Security engineering, testing support, and/trade studies to help the HCFA technical staff evaluate and select appropriate new security technologies.

3. Security engineering, configuration design support, and expert consultation to help HCFA technical staff securely configure critical network components, systems, devices and security products, and implement architecture changes.

4. Source code security audits to ensure that web-based/browser enabled applications and scripts are free of flaws or vulnerabilities that could be exploited by an intruder or malicious user to compromise HCFA systems, or otherwise gain unauthorized access to HCFA resources.

5. Security testing and vulnerability analysis, as required, to ensure that any changes to the IT architecture and critical network components, systems, devices and security products are appropriate, correct, and have no adverse impact on the secure configuration of the network.

6. Security consultation and technical support to help the HCFA technical staff develop and implement appropriate administrative and technical processes and procedures for maintaining the secure configuration of the HCFA network.

7. Periodic and/or random security testing(ethical hacking) and vulnerability analysis to ensure that the secure configuration of critical network segments, components, devices and/or systems continue to effectively implement HCFA security policy.

8. Security training seminars and tutorials on the technical aspects of computer and network security to help HCFA develop in-house skills and expertise that is necessary to effectively implement and maintain the secure network configuration.

GOVERNMENT PROPERTY

The government shall not provide any property and/or equipment to the contractor in the course of this contract.

V. DELIVERABLES

The specific deliverables outlined in tasks 1 and 2 above, shall be delivered by the contractor as an original and five(5) paper copies, as well as an electronic copy on diskette in the Word 97 format. The government shall have ten(10) working days to review these deliverables, and return comments to the contractor. The contractor then has ten(10) working days to return the final deliverable to the government, The contractor shall deliver the final deliverable as an original and five(5) paper copies, and an electronic copy on diskette in Word 97 format.

It is anticipated that the support provided under task 3 of this contract shall require a variety of deliverables, depending upon the specific requirements of the government. The government shall provide the contractor with specific assignments, as the need arises, and require deliverables at times to be determined jointly by the government Project Officer, and the contractor.

The due date for this task shall be on or before 06/30/2000.

VI. MEETINGS

The contractor shall meet with the government Project Officer every week during the course of this contract to discuss progress made, problems encountered, etc. These meetings may be in person, or in the form of teleconferences.

HHS OIG - EDP Controls Assessment
at
HCFA Central Office
As of September 30, 1999

R

DRAFT

Introduction

The external security audit of the HCFA Central Office was performed by Ernst & Young LLP (E&Y) from the Vienna, Virginia Solutions Center Lab. Don Bartley of HCFA provided a detailed documented description of the testing to be performed and a list of Internet Protocol (IP) addresses to be targeted. This is a deviation from the approach E&Y has used for the other selected HCFA contractor sites, and does not allow E&Y to fully explore possible vulnerabilities and new exploits.

FACSIMILE COVER PAGE

To :	Don Bartley	From :	MIKE NEUMAN
Sent :	10/15/99 AT 9:07:48 AM	Pages :	5 (INCLUDING COVER)
Subject :	INTERIM REPORT		

EXCUSE THE INFORMALITY OF THE REPORT, YOU'LL GET A "REAL" REPORT IN A WEEK OR SO.

IF YOU HAVE ANY QUESTIONS, PLEASE FEEL FREE TO CONTACT ME!

MIKE

October 14, 1999
Urgent Interim Report
En Garde Systems

We have discovered a serious problem with the configuration of the IBM-run WWW servers. There are also several other, less severe, security flaws which we will mention briefly in this report. A formal report will follow in a week or so.

1) Major: Anyone on the Internet can access internal HCFA systems

IBM provides two network services to HCFA: IGS OpenNet provides access to the Internet and [redacted] [SECURED NETWORK] [redacted] provides "secure" connectivity to HCFA partners (MDCN), contractors, and employees [SECURED NETWORK] The goal of a two-tiered service is that the [redacted] is completely isolated from Internet malfeasants, and provides a means for secure communication between business partners. If the separation is compromised, the result is the "lowest common denominator" of the two networks, and so the [redacted] [redacted] becomes equivalent to the IGS OpenNet. Because HCFA trusts [redacted] to eliminate security risks, a failure of the [redacted] protection means HCFA is trusting the[1]IGS OpenNet, and therefore the Internet. [SECURED NETWORK] [SECURED NETWORK]

IBM has architected the external HCFA WWW servers to be dual homed. That is, they have a connection to both the IBM OpenNet and IBM SecureNet. We hypothesized, and later proved, that a compromise of an external HCFA WWW server would allow us, from the Internet, to send and receive arbitrary data with internal HCFA systems.

Specifically, we attacked [redacted] The web server had absolutely NO protection from remote modification. [redacted] We were able to traceroute to [redacted], a critical HCFA network management system, entirely through the [redacted] [SECURED NETWORK] [redacted]

Anyone on the Internet could easily gain unlimited access to www.[redacted]. Using this access, he can freely browse any shared filesystem or resource throughout the Internal HCFA network.

Fallout

a) The combination we used to gain access to the HCFA internal network is not the only one available. Many of the problems are systemic
b) IGS's policy of dual homing every web server potentially means that if ANY IGS customer web server is compromised, the HCFA Internal network is exposed

[1] Green Eggs and Ham mysteriously appeared on the HCFA cafeteria menu during a previous visit

Conclusion

We strongly recommend HCFA and IGS review security procedures. Two separate WWW servers [redacted] were so badly configured that an intruder simply needed to "point and click" to break in. It needs to be determined how these systems got so poorly configured in the first place, and why IGS's penetration testing and network security scanning missed these major and extremely blatant problems.

That aside, our penetration testing was conducted under extremely limited conditions. We were only allowed to test end servers, and not routers, switches, or any other customers' equipment. No "real world" intruder would be subject to such limitations. Despite these restrictions, we were able to move easily from the Internet through the [redacted] to the HCFA Internal Network.

[SECURED NETWORK]

Appendix A

[redacted]

EN GARDE SYSTEMS
INCORPORATED

Test Report

Internet Penetration Testing

HCFA – BALTIMORE, MARYLAND

CONFIDENTIAL

This document contain[redacted]tive or technical information regarding HCFA computer systems and programs, the disclosure of which would jeopardize the security of the HCFA network.

PREPARED BY:

EN GARDE SYSTEMS, INC.
4848 TRAMWAY RIDGE DRIVE NE SUITE 122
ALBUQUERQUE, NM 87111
(505) 275-8655

October 27, 1999

EN GARDE SYSTEMS
INCORPORATED

Table of Contents

Table of Contents i
Section I -- Overview 1
Executive Summary 1
Testing Process and Procedures 1
Section II -- Test Results 2
Internet Penetration Test 2
Network Level Tests 5
Section III -- Internet Penetration Test Findings and Recommendations 7
General Comments 7
Appendix A -- System Information for machine [redacted] 10
Appendix B -- Traceroute to [redacted] 17

Section I

Overview

Executive Summary

Our findings, based on information compiled during the internet penetration test indicate that some work must be done to more effectively secure HCFA's internal network and web servers. While it is clear that HCFA is concerned about security, findings indicate that the network is exposed and vulnerable to Internet based attacks. Many of the machines tested are running the latest patches and security fixes but major administration issues have been neglected allowing malicious users to modify pages, upload and run scripts, and initiate attacks into HCFA's internal network. Problems reside with the network architecture, policy and access, configuration management and security administration.

Testing Process and Procedures

En Garde Systems (EGS), Incorporated performs penetration testing as the primary means to evaluate overall system and network security. The tools, methods, and techniques employed by EGS to perform these tests are generally well known throughout both the computer security and "hacker" communities. Hence, vulnerabilities or configuration liabilities discovered as a result of these tests can be viewed as those that any intruder may find while testing the network and connected systems. Testing of the HCFA/IBM network was conducted over the Internet to determine if external network security controls (firewalls, servers, routers, etc.) are effective in preventing unwanted external intrusion, and unauthorized access to HCFA resources on the internal network. All Internet tests were accomplished from the perspective of an outsider[1] trying to gain unauthorized access.

[1] An outsider is someone who has no authorized access to the data or systems to which they wish to login. These are the persons commonly referred to as "hackers" as their goal is to gain inside access by utilizing some form of security override.

CONFIDENTIAL

Internet Penetration Test Results

Public Exposure

Based on the IP addresses that IBM gave us before testing, we proceeded to do [redacted] scans. This yielded the web server services running on the machines included in this report.

[secured network]

During this test we discovered that IBM has designed the external HCFA WWW servers to be dual homed. This means that they have a connection to both the IBM OpenNet and the [redacted]. A compromise of an external HCFA WWW server allowed us, from the Internet, to send and receive arbitrary data with internal HCFA systems. This is an architectural problem. IBM provides two network services to HCFA: IGS OpenNet provides access to the Internet and [redacted] provides [SECURITY NETWORK] "secure" connectivity to HCFA partners, contractors, and employees. This gives HCFA the means to have secure communication with its partners safe from the openness of the Internet and malicious attackers. However, this also allows a malicious intruder to easily gain access to the [redacted] via the Internet by compromising a WWW server. Which was accomplished on [SECURITY NETWORK] several web servers.

Dual homed machines create a gateway between two networks. This is true if the machine is a firewall which has no services running or a web server running several highly vulnerable services. Once the dual homed machine is compromised entry into back end systems becomes easier. Combined with the fact that new vulnerabilities will constantly be found, making even the most secure system vulnerable, dual homed eliminate the security between networks.

Recommendations:

1. Eliminate dual-homing any of the HCFA external web servers. This will reduce the risk of a malicious intruder gaining complete access to the internal network if a web server is compromised. Should a WWW server be comprised, HCFA will be more protected from an attack on the Internal network if dual-homing is eliminated.
2. Consider adding a substantial firewall between [SECURED NETWORK] [redacted] and the HCFA Internal Network. This will also reduce the risk of an Internal attack if the external network is compromised. And review all firewall logs to ensure they are implemented appropriately.

We were able to exploit a number of configuration problems on www.[redacted].

CONFIDENTIAL

1. [redacted]

2. [redacted]

3. [redacted] We were successful in tracerouting to [redacted] which is a critical HCFA network management system. This was tracerouted entirely through [redacted] [SECURED NET WORK] The traceroute is in Appendix B.

4. [redacted]

The consequences of these problems is that any malicious attacker could easily gain unlimited access to www.[redacted]. Using this access, the malicious attacker can then gain access to any shared filesystem or resource throughout the Internal or "secure" HCFA network. Also, the methods and combinations of methods that we used to gain this unlimited access to the HCFA internal network are not the only ones available. Many of the problems are systemic. IGS's policy of dual homing every web server leaves the entire network completely vulnerable. If any IGS customer web server is compromised, the HCFA internal network is exposed.

Recommendation: Disallow non-HCFA users from modifying the www.[redacted] web site. This will keep a malicious intruder from altering the web site and/or writing to the web server programs which could very easily give information such as configuration files or password files to the malicious attacker.

There are too many third party applications installed on www.[redacted] Looking through the [redacted] server shows such applications [redacted]

December 15, 1999

Don Bartley
HCFA

Don:

We reviewed the document "Responses to Questions for 'CritSit' Complaint #RI7764" as you provided, and had several comments.

1) In the first sentence, IBM states "AGNS has no responsibility for system monitoring in the IBM [redacted] environment". We were under the impression that this was one of the services you explicitly contracted IBM to provide to HCFA. Does this mean that they are absolving themselves of responsibility for attack monitoring, is this simply a comment about whom has responsibility (AGNS or IBM)?

2) In Response 1, they list a set of attacks they detected. Did they detect any attacks from the IBM run WWW server to the HCFA internal network? Once gaining access to the web server, we attacked a variety of internal HCFA services in several "loud" ways. Certainly an attack initiated from the WWW server would be the clearest sign that IBM's server has been "had". If this activity is not currently monitored, it should be as soon as possible. We can't think of any clearer sign of attack or successful penetration.

3) As an aside, we still have not been provided with the attack logs. We are still willing to review those and compare them against the attacks we actually performed, if HCFA would like.

4) In Response 3, they state that customers are separated by VLANs which prevent one customer's web server compromise from affecting any others. There are several issues we would like to bring up:
   a. Can individual customers have IBM misconfigure (by requirements or accidentally) their firewall so that it is possible for a hacker on a compromised web server to attack another customer?
   b. We were specifically disallowed from testing the firewalls proper, so we have no idea if they themselves are vulnerable. If they could be compromised, then certainly an intruder could move freely to all the customers' networks.
   c. What protections exist separating the IBM administrative network from the various customers? According to statements by IBM, individual system administrators have unlimited discretion over which system administration tools to use on each server. Firewalls (if there are any) protecting the administrative network from each web server must therefore not have consistant policies (some allow [redacted] some [redacted] some [redacted] and [redacted]). Since we were disallowed from testing the

administrative network, we have no idea if there is any protection there at all. As a result, if an intruder could break any one web server, and move freely into (or through) the administrative network, he could compromise any of IBM's customers equally.

5) Response 5 was unreadable

6) In response 6, IBM suggests switching the IBM platform for their web server. This suggestion makes little sense given:

   a. IBM states that " can be used and secured properly at the customer's request".
   b. HCFA has a lot invested in using server, and so forth. It would seem to be extremely expensive to convert all of this to an based solution.

   Does IBM have superior technology protecting their systems? That is neither stated nor implied in response 6. Is IBM implying that HCFA did not "request" that be "used and secured properly"? If the answer to both of these questions is "no", then it makes no sense to change server architectures.

7) In response 8, IBM states that there is a Firewall…between the HCFA network and the IBM Environment." What is the configuration of this firewall? Where is it placed on the network? Can it protect against attacks from other IBM run web servers? Other IBM (non MDCN) customers? Without complete answers to all of these questions (including specific configuration details such as access rules), HCFA has no guarantee that this firewall will stop any attacks at all.

8) In response 9, IBM states [non-public] that servers are more secure if they are multi homed. As we have stated before, we don't believe HCFA's server needs the backend connection, as no data is placed on the public web server. In the future, if private data is placed on the server, its protection will not be augmented by a backend connection. Simple encryption (through a VPN or other mechanisms) on the open Internet combined with a push method of server updating will suffice, as the real vulnerability is going to be within the web server itself. In our opinion, having a backend connection on the HCFA open web server only serves as a non-HCFA controlled avenue for outsiders to gain access to internal HCFA resources. We have given more detailed explanations for this in other documents, and would be happy to discuss our reasoning as necessary.

If you have any further questions, please feel free to contact us!

Mike Neuman
En Garde Systems, Inc.

n: Don Bartley
To: BMcmenamin, JSuchocki, SWalter, JSchatoff, MMinion
Date: 12/14/99 8:18
Subject: EnGarde Teleconf Followup

All,

During the EnGarde teleconference of 12/6 held in Eva Jun's office several action items were identified. Please provide an update today to those items to include completion date if necessary.

- Steve Walter to do alternatives to dual and triple homing. Alternatives to content deployment - double posting? Disconnect backend connection to occur?

- Mia Minion/Jack Schatoff to review firewall rules. Has the firewall configuration been mailed to EGS?

- [redacted] ltering to prevent partners accessing infrastructure.

IBM was to provide HCFA with a written proposal for review prior to our meeting. This should have come last week. Has the document arrived and if so, could we receive a copy?

Thanks,
Don

CC: VQuigley

m: Greg Overland
To: RHarmon, DBartley
Date: 12/16/99 11:16
Subject: EnGarde Teleconf Followup - Second Notice -Forwarded

"- Steve Walter to do alternatives to dual and triple homing. Alternatives to content deployment - double posting? Disconnect backend connection to occur?"

This would be an engineering effort assigned to OIS/TIG. It also involves network security, again a OIS/TIG effort.

CC: DJanuchowski, GOverland

: Rebecca Harmon
To: DBartley
Date: 12/16/99 11:29
Subject: EnGarde Teleconf Followup - Second Notice -Reply

Item - [redacted] filtering to prevent partners accessing infrastructure. I had discussions with our techs and Denis and decided not to install the firewall to MDCN at this time. I shared the decision with Victoria (she was not in that day). We know that this should be done and we will do so once a plan is developed and after Y2K Day One.

CC: VQuigley

EN GARDE SYSTEMS
INCORPORATED

R

Test Report

Internal as a User Test

HEALTH CARE FINANCE ADMINISTRATION

CONFIDENTIAL

PREPARED BY:

EN GARDE SYSTEMS, INC.
4948 TRAMWAY RIDGE DR. NE SUITE 122
ALBUQUERQUE, NM 87111
(505) 346-1760

June 7, 2000

EN GARDE SYSTEMS
INCORPORATED

Table of Contents

Table of Contents i
Section I – Overview 2
Executive Summary 2
Testing Process and Procedures 2
Section II – Test Results 3
Obtaining An Account 3
Configured Network Permissions 3
Permissions on Our Account 4
Home Machine Network Configuration 4
Passwords 5
Network Test 7
Section III – Findings and Recommendations 9
General Comments 9
Appendix A – Service Listings 10

Overview

Executive Summary

Findings, based on information compiled during the external test, indicate that some work must be done to more effectively secure the internal HCFA resources from users on the network. While it is clear that the HCFA has put in place many of the proper precautions the practice of creating all accounts with administrative permissions negates almost all the security precautions taken on the Internal network. Problems reside with the policy and access, configuration management and security administration. Several major findings include poor choice of administrator passwords by contractors, loosely configured network infrastructure [redacted] administrative privileges given to every new user.

Testing Process and Procedures

En Garde Systems (EGS), Incorporated performs internal penetration testing as the primary means to evaluate internal system security. During this test we performed a number of system level tests that were used to determine what privileges a typical user on the network is given and what that allows the user to do on the network. The tools, methods, and techniques employed by EGS to perform these tests are generally well known and can easily be discovered by any curious or malicious user on the network. Hence, vulnerabilities or configuration liabilities discovered as a result of these tests can be viewed as those that any internal user may find while using their host machine or the network.

EGS began testing with a single user account on the network. The specific account name given to us to use was [redacted].

[redacted]

CONFIDENTIAL

Passwords

Since we were able to gain any access we wanted to the machine including reading and writing to the [redacted], it was possible to obtain the encrypted passwords for all accounts on the machine. We also downloaded through the HCFA web proxy [redacted] that is a [redacted] password-cracking tool.

Using this tool we were able to crack passwords on our machine, and then using those passwords were able to obtain further encrypted passwords from virtually every [redacted] configured machine. The following tables list passwords that were too easily guessed:

Critical Passwords:

06 26 00

MCOB Talking Points: Medicare Contractor Security Initiative

- Current HCFA Requirements
  - Not updated since 1992
    - Before the days of e-mail, internet, hackers, viruses
  - Do not reflect requirements from GAO and IRS Audit Guides
  - Current HCFA requirements don't include all requirements:
    - HIPAA
    - PDD 63
    - HCFA internal policies – architecture, security handbook
    - Industry best practices
- Manuals only address Carriers, FI's
  - We will have core requirements extended to Standard System Maintainers, CWF hosts, DMERCs and Data Center as well.
  - We will publish core requirements as separate security policy. Manuals and contracts will contain only program management information – what, when, where, and how core security requirements must be implemented and reported upon.
  - We will incorporate core requirements update into contract renewals
- Developing Contractor Assessment Security Tool (CAST)
  - Will enable the documentation of contractor compliance with core requirements.
  - Contractors can use CAST to:
    - Assess compliance with the core requirements and identify gaps to be filled.
      - Will support future security budget requests.
    - Facilitate and expedite GAO, IRS and CFO audits by demonstrating compliance with core requirements.
  - HCFA can use CAST to:
    - Facilitate collection of program management data on the nature and extent of Medicare contractor compliance with core requirements.
    - Review (audit) Medicare contractor compliance with core requirements.
- FY 2001 BPRs
  - Productivity Investment section informs contractors that funds will be provided to implement the core requirements.

  - OIS 414 project plan has requested $10M from FMIB for productivity investment.
- All Contractor Security Meeting
  - Scheduled for late September
  - Contractors, consortium and RO staff will be briefed on the security initiative, core requirements, and CAST.
- IV&V of Security Program Documentation
  - HCFA's IV&V contractor will be required to review contractor security program documentation prepared to comply with the core requirements.
  - IV&V review results will be incorporated in FY 2001 CPE.
- Penetration Testing
  - A penetration testing contractor will test vulnerability to internet hackers and abuse of privileges by contractor employees.
  - Up to 25 contractors will be tested.
    - Will not include those involved in CFO audit.
  - Contractors will be required to repair identified vulnerabilities.
- Security Best Practice Forum
  - Will include all Medicare contractors
  - Will focus on security engineering technologies.
  - To be facilitated by Gartner Group.
- FY 2002 includes funds for Medicare contractor security engineering to close gaps identified in risk assessment and threat analyses.
- FY 2002 Strategy adds all external business partners

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

FEB 26 2001

To: The Secretary
Through: DS ____
COS ___
ES ____

From: Acting Inspector General

Subject: Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000 (CIN: A-17-00-00014)

PURPOSE

Our purpose is to provide you with our audit report on the Department's Consolidated/Combined Financial Statements for Fiscal Year (FY) 2000. This audit is required by the Government Management Reform Act of 1994.

The attached report reiterates problems reported at the Health Care Financing Administration (HCFA) and highlights weaknesses noted during audits of other operating division financial statements and departmental system examinations.

Following is a summary of the major issues discussed in the Departmentwide audit report.

INFORMATION TEXT

In our opinion, the Department of Health and Human Services (HHS) FY 2000 financial statements present fairly, in all material respects, the HHS assets, liabilities, and net position at September 30, 2000; the consolidated net costs and changes in net position; and the combined budgetary resources and financing for the year then ended in accordance with accounting principles generally accepted in the United States.

Our report on internal controls notes two internal control weaknesses that we consider to be material under standards established by the American Institute of Certified Public Accountants and Office of Management and Budget Bulletin 01-02.

- Financial systems and processes remain a significant challenge for the Department. This year, data from a new grant processing system proved unreliable and caused significant delays in preparing the financial statements of operating divisions and the Department. Adjustments to the financial statements were made late in February 2000, more than 5 months after the fiscal year ended. We again note the need for HHS to operate a fully

functioning, integrated financial system. This system should include installation of dual-entry accounting systems at the Medicare contractors and culminate in the production of auditable HHS financial statements. We also point out the need for periodic reconciliations and account analyses throughout the year to improve the timeliness and quality of financial information, as well as stronger HCFA regional office and contractor monitoring of Medicare accounts receivable.

- The Medicare contractors continue to lack adequate electronic data processing controls. Access controls, entity-wide security programs, and systems software controls are most problematic. Such weaknesses do not effectively prevent (1) unauthorized access to and disclosure of sensitive information, (2) malicious changes that could interrupt data processing or destroy data files, (3) improper Medicare payments, or (4) disruption of critical operations.

Material weaknesses are those problems that are systemic across a number of operating divisions, as well as significant dollar issues affecting only one division. These weaknesses are synopsized in this report and are fully described in the individual financial statement audit reports which we released separately.

We are grateful for the cooperation the Department has extended to us in performing this audit. If you have any questions, please contact me or have your staff contact Joseph E. Vengrin, Assistant Inspector General for Audit Operations and Financial Statement Activities, at (202) 619-1157.

Michael Mangano

Michael F. Mangano

Attachment

cc:
Dennis Williams
Acting Assistant Secretary
for Management and Budget

George H. Strader
Deputy Assistant Secretary, Finance

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REPORT ON THE FINANCIAL STATEMENT AUDIT OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES FOR FISCAL YEAR 2000

FEBRUARY 2001
A-17-00-00014

INDEPENDENT AUDITOR'S REPORT

INSPECTOR GENERAL'S REPORT ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES CONSOLIDATED/COMBINED FINANCIAL STATEMENTS FOR FISCAL YEAR 2000

To: The Secretary of Health
and Human Services

We have audited the accompanying consolidated balance sheet of the Department of Health and Human Services (HHS) as of September 30, 2000; the related consolidated statements of net cost and changes in net position; and the combined statements of budgetary resources and financing (principal financial statements) for the fiscal year (FY) then ended. These financial statements are the responsibility of HHS management. Our responsibility is to express an opinion on them based on our audit.

We conducted our audit in accordance with auditing standards generally accepted in the United States; *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin 01-02, *Audit Requirements for Federal Financial Statements*. These standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, the principal financial statements referred to above present fairly, in all material respects, the HHS assets, liabilities, and net position at September 30, 2000; the consolidated net costs and changes in net position; and the combined budgetary resources and financing for the year then ended in conformity with accounting principles generally accepted in the United States.

Our audit was conducted for the purpose of forming an opinion on the principal financial statements referred to in the first paragraph. The information in the Overview and the Supplementary Information are not required parts of the principal financial statements but are considered supplemental information required by OMB Bulletin 97-01, *Form and Content of Agency Financial Statements*, as amended. Such information, including trust fund projections,

has not been subjected to the auditing procedures applied in the audit of the principal financial statements. Accordingly, we express no opinion on it.

In accordance with *Government Auditing Standards*, we have also issued our reports dated February 26, 2001, on our consideration of HHS internal controls over financial reporting and on our tests of HHS compliance with certain provisions of laws and regulations. These reports are an integral part of our audit; they should be read in conjunction with this report in considering the results of our audit.

February 26, 2001

REPORT ON INTERNAL CONTROLS

We have audited the principal financial statements of HHS as of and for the year ended September 30, 2000, and have issued our report thereon dated February 26, 2001. We conducted our audit in accordance with auditing standards generally accepted in the United States; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin 01-02, *Audit Requirements for Federal Financial Statements*.

In planning and performing our audit, we considered the HHS internal controls over financial reporting by obtaining an understanding of the HHS internal controls, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin 01-02. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982, such as those controls relevant to ensuring efficient operations. The objective of our audit was not to provide assurance on internal controls. Consequently, we do not provide an opinion on internal controls.

Our consideration of internal controls over financial reporting would not necessarily disclose all matters in these controls that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of internal controls that, in our judgment, could adversely affect the HHS ability to record, process, summarize, and report financial data consistent with management assertions in the financial statements. Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts material to the financial statements may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal controls, misstatements, losses, or noncompliance may nevertheless occur and not be detected. However, we noted certain matters discussed below involving internal controls and their operation that we consider to be reportable conditions and material weaknesses.

In addition, we considered the HHS internal controls over Required Supplementary Stewardship Information by obtaining an understanding of the HHS internal controls, determining whether these controls had been placed in operation, assessing control risk, and performing tests of controls as required by OMB Bulletin 01-02. Our procedures were not intended to provide assurance on these controls; accordingly, we do not provide an opinion on them.

Finally, with respect to internal controls related to performance measures reported in the *FY 2000 HHS Accountability Report*, we obtained an understanding of the design of significant internal controls related to existence and completeness assertions, as required by OMB Bulletin 01-02. Our procedures were not designed to provide assurance on internal controls over performance measures; accordingly, we do not provide an opinion on such controls.

Using the criteria and standards established by the American Institute of Certified Public Accountants and OMB Bulletin 01-02, we identified two internal control weaknesses that we consider to be material and two reportable conditions, as follows:

INTERNAL CONTROL WEAKNESSES*

		Page
	Material Weaknesses	
1.	Financial Systems and Processes	4
2.	Medicare Electronic Data Processing	13
	Reportable Conditions	
1.	Medicaid Estimated Improper Payments	17
2.	Departmental Electronic Data Processing	18

* "Financial Systems and Processes," called "Financial Systems and Reporting" in our FY 1999 report, has been retitled to incorporate continued problems with Medicare accounts receivable and Health Care Financing Administration oversight of Medicare contractors. The reportable condition for "Property, Plant, and Equipment" has been removed.

MATERIAL WEAKNESSES

1. Financial Systems and Processes (Repeat Condition)

Since passage of the Chief Financial Officers (CFO) Act, as amended by the Government Management Reform Act of 1994, agencies have prepared financial statements for audit by the Inspectors General. The act emphasized production of reliable financial statements; consequently, HHS worked diligently to prepare statements capable of receiving an unqualified audit opinion. With this year's audit, HHS sustained the important achievement of an unqualified, or "clean," opinion, which we issued for the first time on the FY 1999 financial statements.

A clean audit opinion, however, assures only that the financial statements are reliable and fairly presented. The opinion provides no assurance on the effectiveness and efficiency of agency financial controls and systems, criteria for which may be found in OMB Circular A-123, *Management Accountability and Control*, and OMB Circular A-127, *Financial Management Systems*. Taken together, the criteria require agencies to record, classify, and report on the results of transactions accurately and promptly. Although manual processes may be used, the system(s) must be efficient and effective to accomplish the agency mission and to satisfy financial management needs.

In our view, the Department continues to have serious internal control weaknesses in its financial systems and processes for producing financial statements. Because many systems were not fully integrated and, in some cases, were in the process of being updated or replaced, the preparation of financial statements required numerous manual account adjustments involving billions of dollars. In addition, significant analysis by Department staff, as well as outside consultants, was necessary to determine proper balances months after the close of the fiscal year. Had the operating divisions followed departmental policies and conducted financial analyses and reconciliations throughout the year, many account anomalies would have been detected earlier. While we observed steady improvement in the financial statement process, system and process weaknesses still did not ensure the production of timely and reliable financial statements. These weaknesses related to grant and other accounting issues, Medicare accounts receivable, and Health Care Financing Administration (HCFA) oversight of Medicare contractors.

Background

In addition to the individual operating divisions, two divisions of the Program Support Center play important roles in the departmental financial process: the Division of Financial Operations (DFO) and the Division of Payment Management (DPM).

The DFO provides financial management and accounting services to the Administration for Children and Families (ACF), the Substance Abuse and Mental Health Services Administration (SAMHSA), the Health Resources and Services Administration (HRSA), the Indian Health Service, the Administration on Aging, the Program Support Center, the Agency for Healthcare Research and Quality, and the Office of the Secretary. The remaining operating divisions — HCFA, the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), and the Food and Drug Administration (FDA) — are responsible for their own accounting.

The DPM provides centralized electronic funding and cash management services for approximately 65 percent of Federal civilian grants and certain contracts. In FY 2000, the DPM Payment Management System made almost 274,000 payments totaling approximately

$195 billion to more than 24,000 grantees on behalf of HHS as well as 10 other Federal agencies and 42 subagencies.

After awarding grants, agencies transmit award amounts and grant payment limits to DPM. Based on these parameters, grantees withdraw funds to pay the expenses of their operations, and they report their expenses to DPM quarterly. The DPM records the withdrawals and expenses and issues reports on these transactions to granting agencies and the Department of the Treasury.

Grant Accounting Issues

From 1970 until July 2000, grant transactions were processed by the DPM Payment Management System on a mainframe computer at the NIH Center for Information Technology. In FY 1994, it was determined that expanding this legacy system was not practical and that the system should be replaced with a new client server, web-enabled system. Programming of the new system began in early FY 1998. In February 1999, a decision was made to defer implementation of the new system until after January 2000, and efforts were then focused on remediating the legacy system for Y2K compliance. Independent public accountants (IPAs) determined that for the period September 1, 1999, through July 28, 2000, the legacy system's internal controls were operating effectively. In July 2000, after successfully running parallel for about a month to test the more critical functions, such as fund transfers, the new Payment Management System was brought online without major incident. Grant authorizations, payment requests, and fund transfers were processed through the system at expected volumes.

However, the expenditure subsystem used to produce and process forms 272, Federal Cash Transactions Report, was not fully tested. The DPM determined that this subsystem could be tested after the new system was implemented and before recipients began returning their completed June 30 (third quarter) expenditure reports in September. While processing the June 30 expenditure reports, two programming problems surfaced. As a result, incomplete or erroneous data were reported to the operating divisions and other customer agencies. First, the algorithm used to allocate expenditures to a common accounting number (CAN) did not function properly. While total expenditures were captured, the amounts were incorrectly distributed to the CANs. Although we noted certain concerns with the allocation of disbursements among the operating divisions, we determined that total cash disbursements charged to the operating divisions, in the aggregate, equaled net cash disbursements reported to the Department of the Treasury and distributed to grant recipients. Second, the new system could not process paper 272 reports; this produced a backlog of about $2.1 billion in unprocessed reports. Compounding these problems, the lead programmer working on the expenditure process unexpectedly left the employment of the system development contractor in August.

After correcting the programming problems, DPM began processing the backlog of expenditure reports. In late September, an expenditure file was distributed to the operating divisions reflecting what DPM thought was the majority of grantee expenditure reports. **Because DPM was of the opinion that any remaining expenditure amounts would be immaterial, it did not notify any of its customers of this problem.** These assumptions were incorrect. In actuality, many of the paper 272 reports involved large grantees and totaled about $2.1 billion in unprocessed third quarter expenditures. The DPM should have analyzed the unprocessed reports and determined the extent and seriousness of the problem rather than speculate that it was immaterial. These problems were not fully communicated to senior operating division management or the auditors until February 2001. As a result, grant expenditures, grant advances, and the grant accrued expense calculation contained billions of dollars in errors until final correction. The errors caused account anomalies noted by auditors and substantially delayed final conclusion of the audits of NIH, ACF, HRSA, SAMHSA, and CDC and the Department's compilation of the financial statements:

- The DFO, the operating divisions, and/or auditors analyzed grant expenditures reported on the Statement of Net Cost and found that the yearend balances contained aggregate errors of $2.7 billion. This amount included understatements of $2.1 billion ($1 billion for ACF, $1 billion for NIH, and $100 million for CDC) and overstatements of $628 million ($420 million for HRSA, $97 million for CDC, $91 million for SAMHSA, and $20 million for ACF). As a result of these errors, the financial statements initially were materially misstated. Certain operating divisions did not detect these errors through their internal controls.

- The DFO extensively analyzed July and August grant advance transactions reported by DPM and determined that advances recorded in the general ledger were understated by $858 million: $449 million for ACF, $335 million for HRSA, and $74 million for SAMHSA.

- From October 1, 1999, to June 30, 2000, many accounts in the subsidiary detail were not properly classified as intragovernmental or nongovernmental transactions. The absolute value of classification errors in the subsidiary detail was approximately $6.4 billion: $5.4 billion for ACF, $552 million for HRSA, and $445 million for SAMHSA. The DFO ultimately corrected these errors ("outside the general ledger") in its manual yearend process of preparing financial statements.

- The ACF grant transactions of approximately $1.1 billion were recorded to the wrong CAN. As a result, these amounts were reported in the wrong appropriation. We were informed that this occurred because of discrepancies in

the CAN table that were not identified until several months after the end of the fiscal year.

Although these four problems were eventually corrected, we remain concerned that the operating divisions did not routinely analyze accounts to detect such accounting anomalies. When such analyses are not performed in the normal business cycle, material errors and irregularities will not be promptly detected and the resulting financial statements will be at risk of inaccuracies. Also, procedures should be established to ensure that detected anomalies are effectively communicated to top management.

Medicare Accounts Receivable

The HCFA is the Department's largest operating division with about $316 billion in net outlays. Along with its Medicare contractors, HCFA is responsible for managing and collecting many billions of dollars of accounts receivable each year. Medicare accounts receivable are primarily overpayments owed by health care providers to HCFA and funds due from other entities when Medicare is the secondary payer. For FY 2000, the contractors reported about $30 billion in Medicare accounts receivable activity which resulted in an ending gross balance of approximately $7.1 billion — over 87 percent of HCFA's total receivable balance. After allowing for doubtful accounts, the net balance was about $3.2 billion.

For several years, we have reported serious errors in contractor reporting of accounts receivable that resulted from weak financial management controls. Control weaknesses were noted again this year. Because the claim processing systems used by the contractors lacked general ledger capabilities, obtaining and analyzing financial data was a labor-intensive exercise requiring significant manual input and reconciliations between various systems and ad hoc spreadsheet applications. The lack of double-entry systems and the use of ad hoc supporting schedules increased the risk that contractors could report inconsistent information or that information reported could be incomplete or erroneous.

To address previously identified problems in documenting and accurately reporting accounts receivable, HCFA began a substantial validation of its receivables by contracting with IPAs in FY 1999. The HCFA continued the validation effort this year. As a result, the receivables balance was adequately supported as of the end of FY 2000.

The IPAs reviewed accounts receivable activity at 14 Medicare contractors which represented over 68 percent of the total Medicare accounts receivable balance at September 30, 1999. While they noted significant improvement in the HCFA central office's analysis of information included in its financial statements, along with improvement in contractors' processing and reporting of receivables, their review identified overstatements and understatements totaling

$374 million as of March 31, 2000. This amount included errors of $201 million in Medicare Secondary Payer (MSP) receivables and $173 million in non-MSP receivables. Most of the MSP misstatements were due to a lack of supporting documentation for the amounts reported in the contractors' quarterly financial reports to HCFA. Misstatements of non-MSP receivables were attributed to the following:

- $74 million resulted from clerical and other errors.
- $50 million should have been eliminated when providers eventually filed their cost reports. Until a provider files a cost report, all outstanding interim payments are considered technical overpayments and are recorded as receivables.
- $47 million was not supported by records.
- $2 million concerned receivables transferred to a HCFA regional office but still included on the contractor's books and thus recorded twice.

While it is quite clear that the root cause of the accounts receivable problem is the lack of an integrated, dual-entry accounting system, HCFA and the Medicare contractors have not provided adequate oversight or implemented compensating internal controls to ensure that receivables will be properly accounted for and reflected in their financial reports. To address its systems problem, HCFA plans to develop a state-of-the-art Integrated General Ledger Accounting System. This system will replace the cumbersome, ad hoc spreadsheets currently used to accumulate and report contractor financial information and will enable HCFA to collect standardized accounting data. In addition, the system will replace HCFA's current accounting system, the Financial Accounting Control System, and will include an accounts receivable module to provide better control and support for receivables. A HCFA-wide project team has been formed under the guidance of the CFO and the Chief Information Officer. Depending on funding, HCFA does not expect to implement the new system until FY 2007.

HCFA Oversight of Medicare Contractors

Pending implementation of a fully integrated accounting system, HCFA's oversight of the Medicare contractors becomes critical to reducing the risk of material misstatement in the financial statements. However, as discussed below, HCFA oversight of contractor operations and financial management controls has not provided reasonable assurance that material errors will be detected in a timely manner.

The responsibility for collecting delinquent provider overpayments is dispersed among the 54 Medicare contractors, the 10 HCFA regional offices, the HCFA central office, and external

agencies. The majority of overpayments are recovered by the contractors through offset procedures. However, when the contractors' collection efforts are unsuccessful, delinquent receivables are transferred to the regional offices and then possibly to various other locations, including the central office, the HCFA Office of General Counsel, the Department of Justice, and the Department of the Treasury's Debt Collection Center.

In an October 28, 1999, report to HCFA (*Safeguarding Medicare Accounts Receivable*, A-17-99-11999), we noted significant weaknesses in regional office accounting for debt. Our review showed that regional and central office accounts receivable were misstated by $184.5 million. Examples of the misstatements included:

- an overstatement of $96.9 million in receivables with no supporting documentation,
- overstatements and understatements totaling $33.9 million due to various reporting and clerical errors, and
- an understatement of $21 million in improperly recorded transfers of receivables from the Medicare contractors to the regional offices.

Not only did the regional offices not safeguard debt in their custody, their monitoring of contractor financial information was inadequate to prevent errors in financial reports and data. As mentioned above, it was necessary for HCFA to hire IPAs to properly determine the accounts receivable balance for the past 2 years. For non-MSP receivables during this period, the IPAs identified about $590 million in recorded debt that the Medicare contractors could not support. While these receivables were written off because of the lack of support, it is possible that some of these receivables were actually debt due to Medicare and should have been collected. Had the regional offices been required to conduct reviews similar to those conducted by the IPAs, many of these problems could have been detected or prevented more timely.

Similarly, stronger regional office oversight of the contractors' reconciliations would help to ensure that contractors have adequate controls in place to prepare accurate and complete financial reports. The HCFA requires all Medicare contractors to reconcile "total funds expended" reported on the prior month's HCFA 1522, Monthly Contractor Financial Report, to adjudicated claims processed using the paid claims tape. This reconciliation is an important control to ensure that all amounts reported to HCFA by Medicare contractors are accurate, supported, complete, and properly classified. However, of the 10 contractors in our sample, 9 did not conduct this reconciliation using the actual paid claims tape. Numerous errors and omissions in contractor reporting resulted. For example, at one contractor, over $65 million in paid claims from the current month's HCFA 1522 was inadvertently included in the previous month's HCFA 1522.

The contractor's HCFA 1522 had to be resubmitted because an unreported manual payment of $6.3 million had not been posted to the contractor's financial records.

Other Accounting Issues

While the timeliness of the HHS financial statements has improved, delays were noted again this year. Numerous adjusting entries at yearend were needed to correct errors and to develop accurate financial statements. Many of these adjustments would not have been necessary had management routinely reconciled and analyzed accounts throughout the year, recorded transactions using prescribed accounts, and refrained from making "financial statement only" adjustments. These controls help to promptly identify and correct accounting aberrations, provide more reliable financial information during the year, and prevent a material misstatement of the financial statements at yearend. Some examples follow:

National Institutes of Health. The NIH financial system, which dates back to the early 1970s, was not designed for financial reporting purposes and lacks certain system interfaces. Because the accounting function is decentralized among the 25 NIH Institutes and Centers, the NIH Office of Financial Management spent considerable time in consolidating and adjusting 23 trial balances in order to prepare financial statements. The NIH, which had net budget outlays of $15.4 billion, was unable to prepare reliable financial statements for September 30, 2000, until February 2001.

During FY 2000, NIH recorded approximately 9.4 million entries in its financial system. About 18,000 of these entries, with an absolute value of about $200 billion, were recorded using nonstandard accounting entries which could circumvent accounting controls. The bulk of these transactions pertained to FY 1999 manual closing entries. Many of these entries were incorrect and were not corrected until months after the original transactions were recorded. For example, entries totaling $140 million were recorded three times in April 2000. Four months later, the duplicate entries were reversed, leaving the correct entries in the system. In addition, we noted that NIH, as in past years, delayed entering some of the prior year's financial statement adjustments, valued at $5.1 billion, to its general ledger for nearly a full year. Such delays cause the general ledger to be misleading and inaccurate during the year.

For FY 2000, to compensate for system inadequacies, NIH developed an ad hoc, yearend process to create and post correct standard general ledger accounts. The output of this process formed the trial balance. However, an additional 95 entries, totaling an absolute value of approximately $28 billion, were necessary in order to adjust the trial balance to prepare the financial statements.

In 1998, NIH launched a project known as the NIH Business System to replace existing administrative and management systems. Once the new system is fully implemented, we believe

that improved financial information will provide for better decision-making, potential cost savings, and a means to meet current Federal accounting and budgetary reporting requirements. However, the system is not expected to be fully operational until 2005.

Administration for Children and Families. The ACF, the second largest operating division with net budget outlays of $37.5 billion, prepared its financial statements more accurately and more timely than last year, largely as a result of having performed many of the required reconciliations and analyses during the year. But many "Fund Balance with Treasury" reconciliations were performed late, and most of the required budgetary account reconciliations were not performed until yearend to prepare the financial statements.

Fund Balance with Treasury reconciliations deserve particular mention because the differences between the general ledger and the Department of the Treasury's records were so great. At various times, the difference ranged from $200 million to $6.3 billion. This suggests that ACF did not post transactions timely or accurately; in our testing, we found instances of this problem. For example, we noted that a $143 million transaction had been posted to the wrong appropriation and remained uncorrected for over a year.

Recommendations. We recommend that the Assistant Secretary for Management and Budget (ASMB):

- direct each operating division to establish controls to identify and report significant accounting anomalies to top management;
- direct the CFO of the Program Support Center to communicate accounting and control problems more effectively to the CFOs of serviced entities;
- direct that operating division CFOs work with their program office counterparts to develop procedures for analyzing and explaining unusual changes in account balances;
- oversee and maintain close liaison with entities serviced by the Program Support Center and CFO offices during the installation of new systems or the revision of operating procedures;
- continue to support the development of the HCFA Integrated General Ledger Accounting System and oversee its implementation;

- monitor HCFA's corrective actions to strengthen regional office and contractor monitoring of accounts receivable and to ensure that key financial reconciliations are performed timely;

- consider directing operating division CFOs to prepare and analyze interim financial statements, particularly the statements of net cost, budgetary resources, and financing, as an aid in the reconciliation and analysis process; and

- require each operating division to prepare quarterly reports on the status of corrective actions on recommendations in the specific CFO reports on internal controls. The ASMB, in turn, should summarize and report quarterly on these actions to the Deputy Secretary and OIG.

2. Medicare Electronic Data Processing (Repeat Condition)

The HCFA relies on extensive electronic data processing (EDP) operations at both its central office and Medicare contractor sites to administer the Medicare program and to process and account for Medicare expenditures. Internal controls over these operations are essential to ensure the integrity, confidentiality, and reliability of critical data while reducing the risk of errors, fraud, and other illegal acts.

The HCFA central office systems maintain administrative data, such as Medicare enrollment, eligibility, and paid claims data, and process all payments for managed care. In FY 2000, managed care payments totaled about $39.8 billion. The Medicare contractors and data centers use several "shared" systems to process and pay fee-for-service claims. All of the shared systems interface with HCFA's Common Working File (CWF) to obtain authorization to pay claims and to coordinate Medicare Part A and Part B benefits. This network accounted for and processed $173.6 billion in Medicare expenditures during FY 2000.

Our review of EDP internal controls covered general and application controls. General controls involve the entity-wide security program, access controls, application development and program change controls, segregation of duties, operating system software, and service continuity. General controls affect the integrity of all applications operating within a single data processing facility and are critical to ensuring the reliability, confidentiality, and availability of HCFA data. Application controls involve input, processing, and output controls related to specific EDP applications.

We completed general control reviews at nine Contractors' Medicare data processing facilities that support the Medicare contractors sampled. In addition, we assessed application controls of the Fiscal Intermediary Shared System (FISS), the Multi-Carrier System, and the CWF at three separate

contractors. At the HCFA central office, we updated the status of prior-year findings concerning general controls.

We found numerous EDP general control weaknesses, primarily at the Medicare contractors. Such weaknesses do not effectively prevent (1) unauthorized access to and disclosure of sensitive information, (2) malicious changes that could interrupt data processing or destroy data files, (3) improper Medicare payments, or (4) disruption of critical operations. Further, weaknesses in the contractors' entity-wide security structure do not ensure that EDP controls are adequate and operating effectively.

As noted in the following table, a total of 124 weaknesses were identified. The majority were found at the Medicare contractors, and most (about 80 percent) involved three types of controls: access controls, entity-wide security programs, and systems software. While individually the conditions found are not material, the cumulative effect is material.

General Control Audit Areas	Number of Weaknesses		
	Central Office	Medicare Contractors	Total
Access controls	2	55	57
Entity-wide security programs	4	17	21
Systems software	1	20	21
Service continuity/contingency planning	-	11	11
Segregation of duties	1	7	8
Application software development and change controls	1	5	6
Total	**9**	**115**	**124**

Access controls. Access controls ensure that critical systems assets are physically safeguarded and that logical access to sensitive computer programs and data is granted only when authorized and appropriate. Closely related to these controls are those over computer operating systems and data communications software. These controls further ensure that only authorized staff and computer processes access sensitive data in an appropriate manner. Weaknesses in such controls can compromise the integrity of sensitive program data and increase the risk that such data may be inappropriately used and/or disclosed. However, access control weaknesses represented the largest problem area. Of the 124 EDP control weaknesses reported, 57, or 46 percent, related to access controls.

- ***Administration of access controls*** (29 conditions: 27 at 11 Medicare contractor sites and 2 at the HCFA central office). In numerous instances, passwords were not properly administered, systems security software was not implemented effectively, or access privileges were not reviewed frequently enough to ensure their continuing validity.

- ***Access to computer programs and system files*** (5 conditions at 5 Medicare contractor sites). At some sites, installation-level controls over critical system software libraries were inadequate, and programmers were inappropriately allowed access to production software program libraries. We also noted cases in which programmers had inappropriate access to system logs; this provided an opportunity to conceal improper actions and obviated the logs' effectiveness as a detect control. At another site, the computer operator could override installation system security precautions when restarting the mainframe computer system.

- ***Access to sensitive data*** (15 conditions at 9 Medicare contractor sites). These are instances in which computer programmers and/or other technical support staff had inappropriate access to the data files used in the claim process. At several sites, programmers had inappropriate access to beneficiary history files. Under these conditions, the CWF system was vulnerable to inappropriate use. At several other sites, programmers had inappropriate access rights to production files, including beneficiary history and other sensitive data. Also, users of one contractor's local area network could access Medicare program data without adequate controls. During vulnerability testing at three Medicare contractor sites, excessive remote access attempts were permitted and more information about the computers being tested was disclosed than necessary. Such weaknesses increase the risk of unauthorized remote access to sensitive Medicare systems.

- ***Physical access*** (8 conditions at 5 Medicare contractor sites). These include weaknesses in controls over access to sensitive facilities and media within those facilities. For example, at one contractor, inappropriate individuals had access to the computer center's command post. At another, the computer production control area was not secured during normal business hours.

Entity-wide security programs. These programs are intended to ensure that security threats are identified, risks are assessed, control objectives are formulated, control techniques are developed, and management oversight is applied to ensure the overall effectiveness of security measures. Programs typically include policies on how and which sensitive duties should be separated to avoid conflicts of interest. Likewise, policies on background checks during the hiring process are usually stipulated. Entity-wide security programs afford management the opportunity to

provide appropriate direction and oversight of the design, development, and operation of critical systems controls. Inadequacies in these programs can result in inadequate access controls and software change controls affecting mission-critical, computer-based operations. Of the 124 EDP control weaknesses reported, 21, or 17 percent, related to security program weaknesses.

- ***Entity-wide plans*** (8 conditions at 8 Medicare contractor sites). Eight contractor sites lacked fully documented, comprehensive entity-wide security plans that addressed all aspects of an adequate security program. One site also had no mechanism for ensuring that system audit findings were effectively addressed and resolved.

- ***Implementation of entity-wide plans*** (13 conditions: 9 at 6 Medicare contractor sites and 4 at the HCFA central office). Inadequate risk assessments, a lack of comprehensive security awareness programs, and inadequate policies were among the weaknesses reported at the contractors. At the HCFA central office, four conditions remained reportable: no security assessment of, or security plans for, significant application systems; deficiencies in the security plan accreditation process; insufficient security oversight of the Medicare contractors; and no formal process to remove system access of terminated HCFA employees and contractors.

Systems software controls. Systems software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, it is used to support and control a variety of applications that may run on the same computer hardware. Systems software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some systems software can change data and programs on files without leaving an audit trail. Of the 124 EDP control weaknesses, 21, or 17 percent, related to weaknesses in systems software controls (20 at 7 Medicare contractor locations and 1 at the HCFA central office). Problems related to managing routine changes to systems software to ensure their appropriate implementation and configuring controls associated with the operating system to ensure their effectiveness. Such problems could weaken critical controls over access to sensitive Medicare data files and operating system programs.

Shared system weaknesses. We found that the prior control weakness related to the Medicare data centers' having full access to the FISS source code remained unresolved. This weakness has been expanded to include the CWF system, since the design of the CWF software provides for programmer update access to CWF data files to meet operational needs. As we previously reported, Medicare data centers had access to the FISS source code and were able to implement local changes to FISS programs. Such access may be abused, resulting in the implementation and processing of unauthorized programs at contractor data centers. While HCFA requires

contractors to restrict local changes to emergency situations, local changes are often not subjected to the same controls that exist in the standard change control process.

HCFA central office. Our followup work found that the HCFA central office had resolved the prior-year deficiency in mainframe database access controls. The central office has also continued to implement enhanced control procedures, specifically in access controls and application development and program change controls. However, actions were still underway as of the end of FY 2000. Improvements not yet completed included:

- issuance of task orders to various contractors to address issues related to risk assessment, security policies and procedures, independent verification and validation of entity-wide security plans, and related procedures for significant systems and
- migration to enterprise-wide program change management software, with full implementation planned during FY 2001.

Recommendation. We recommend that ASMB oversee HCFA's identification and implementation of corrective actions to address the fundamental causes of Medicare EDP control weaknesses. Detailed recommendations are contained in the HCFA audit report.

REPORTABLE CONDITIONS

1. Medicaid Estimated Improper Payments (Repeat Condition)

The Medicaid program, enacted in 1965 under Title XIX of the Social Security Act, is a grant-in-aid medical assistance program largely for the poor, the disabled, and persons with developmental disabilities requiring long-term care. Funded by Federal and State dollars, the program is administered by HCFA in partnership with the States via approved State plans. Under these plans, States reimburse providers for medical assistance to eligible individuals, who numbered more than 33 million in 2000. In FY 2000, Federal and State Medicaid outlays totaled $207.1 billion; Federal expenses were $118.7 billion.

We found that HCFA still lacked a methodology to estimate the extent of improper Medicaid payments on a national level. For the last 5 years, OIG reviewed a statistical sample of Medicare claims and estimated the extent of payments that did not comply with laws and regulations. The majority of errors fell into four broad categories: unsupported services, medically unnecessary services, incorrect coding, and noncovered services. This information helped HCFA to monitor and reduce improper Medicare payments. Because HCFA has not established a similar methodology for the Medicaid program, it cannot reach conclusions on the extent of Medicaid

payment errors. We recognize that Medicaid is a State-administered program, so estimates of improper payments will require the cooperation of States.

Our prior report recommended that HCFA work with the States to develop procedures and implement a methodology for determining the extent of improper Medicaid payments. We noted some recent progress in this area. A project coordinator has begun requesting State participation in a pilot error rate project.

Recommendation. We recommend that ASMB and HCFA continue to work with the States to develop procedures and implement a methodology for determining the extent of improper Medicaid payments.

2. Departmental Electronic Data Processing (Repeat Condition)

The following summarizes some of the systemic EDP control weaknesses identified in audits of operating division financial statements and service organization operations. Other weaknesses are reported in the individual reports on these entities. We note that NIH has resolved the previous year's reportable findings related to systems access controls.

Division of Financial Operations. The Program Support Center's DFO uses several automated systems to provide financial services to certain operating divisions. While DFO continues to strengthen controls over these systems, further improvements are needed.

- The DFO entity-wide security program lacked a formal risk assessment, a formal security plan, and adequate personnel security policies. In addition, the security features of the DFO accounting system (CORE) were not accredited as required by OMB Circular A-130. Such weaknesses in the entity-wide security structure limited assurance that EDP controls were adequate and operating effectively.

- The DFO policy for application change control included no formal test procedures and lacked adequate emergency change procedures, as well as adequate library management software. Additionally, DFO did not consistently follow its documented application change control procedures. For example, change request forms, used to ensure that software changes are approved and documented, were not always complete; supervisory approval of program modifications was not consistently documented; and "before and after" images of program code were not compared to ensure that only approved changes were made to the CORE application.

- A penetration test of the DFO internal network and computing resources to assess the security of systems and to identify vulnerabilities determined that user account policies and administrative passwords on servers were weak. This type of weakness increases to a high level the risk that the system will be compromised by unauthorized users.

Food and Drug Administration. In FY 1999, FDA had several findings under each of the six major categories of general controls. Although FDA resolved many of these findings, some were still outstanding this year. When viewed in the aggregate, these exceptions constituted a reportable condition. Areas still in need of improvement included the entity-wide security program, access controls, software application change controls, and service continuity.

Recommendation. We recommend that ASMB oversee the efforts of the operating divisions and service organizations to improve security issues, system access controls, application change controls, and service continuity plans. Specific recommendations are covered in the individual audit reports.

OTHER MATTERS

FMFIA Reporting

As part of our audit, we also obtained an understanding of management's process for evaluating and reporting on internal control and accounting systems, as required by the Federal Managers' Financial Integrity Act (FMFIA), and compared the material weaknesses reported in the HHS FY 2000 FMFIA report relating to the financial statements under audit with the material weaknesses noted in our report on internal controls. Under OMB guidelines for FMFIA reporting, HHS reports as a material weakness any deficiency the Secretary determines to be significant enough to be disclosed outside the agency. This designation requires HHS management to judge the relative risk and significance of deficiencies. In making this judgment, HHS management pays particular attention to the views of the HHS Inspector General. The HHS management agrees with the HHS Inspector General in reporting to the President and the Congress the two material weaknesses described in this report.

Medicare National Error Rate

At HCFA's request, we developed a national error rate of the extent of improper Medicare fee-for-service payments for FY 2000. As discussed in detail in our separate report (CIN: A-17-00-02000), and based on our statistical sample, we estimate that improper Medicare benefit payments made during FY 2000 totaled $11.9 billion, or about 6.8 percent of the $173.6 billion

in processed fee-for-service payments reported by HCFA. This year's estimate of improper payments is the lowest estimate to date and about half the $23.2 billion that we estimated for FY 1996. There is convincing evidence that this reduction is statistically significant. However, we cannot conclude that this year's estimate is statistically different from the estimates for FY 1999 ($13.5 billion) or 1998 ($12.6 billion). The decrease this year may be due to sampling variability; that is, selecting different claims with different dollar values and errors will inevitably produce a different estimate of improper payments.

As in past years, these improper payments could range from inadvertent mistakes to outright fraud and abuse. We cannot quantify what portion of the error rate is attributable to fraud. The overwhelming majority (92 percent) of these improper payments were detected through medical record reviews coordinated by OIG. When these claims were submitted for payment to Medicare contractors, they contained no visible errors. Although HCFA has made substantial progress since FY 1996 in reducing improper payments in the Medicare program, continued efforts are needed.

****

This report is intended solely for the information and use of HHS management, OMB, and the Congress and is not intended to be and should not be used by anyone other than these specified parties.

February 26, 2001

REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

We have audited the principal financial statements of HHS as of and for the year ended September 30, 2000, and have issued our report thereon dated February 26, 2001. We conducted our audit in accordance with auditing standards generally accepted in the United States; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin 01-02, *Audit Requirements for Federal Financial Statements*.

The HHS management is responsible for complying with applicable laws and regulations. As part of obtaining reasonable assurance about whether the HHS financial statements are free of material misstatement, we performed tests of management compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and with certain other laws and regulations specified in OMB Bulletin 01-02, including the requirements referred to in the Federal Financial Management Improvement Act (FFMIA) of 1996.

The results of our tests of compliance with laws and regulations described in the preceding paragraph, exclusive of FFMIA, disclosed no instances of noncompliance required to be reported under *Government Auditing Standards* or OMB Bulletin 01-02.

Under FFMIA, we are required to report whether HHS financial management systems substantially comply with Federal financial management systems requirements, applicable Federal accounting standards, and the United States Government Standard General Ledger at the transaction level. To meet this requirement, we performed tests of compliance with FFMIA section 803(a) requirements. The results of our tests disclosed instances, described below, in which HHS financial management systems did not substantially comply with Federal financial management system requirements.

- The financial management systems and processes used by HHS and the operating divisions were not adequate to prepare reliable, timely financial statements. Because the Department is decentralized, operating divisions must have efficient and effective systems and processes to report financial results.
    - At HCFA, extensive consultant support was needed to establish reliable accounts receivable balances and to oversee Medicare contractors.
    - The Payment Management System, an application for processing grant payments, did not record and report grant transactions properly.

- At most operating divisions, suitable systems were not in place to adequately explain significant fluctuations in grant transactions.

- At NIH, an integrated accounting system was not in place to consolidate the accounting results of transactions by the Institutes. Extensive, time-consuming manual adjustments were needed before reliable financial statements could be prepared.

❑ The EDP internal control weaknesses identified at the sampled Medicare contractors were significant departures from requirements in OMB Circulars A-127, *Financial Management Systems*, and A-130, *Management of Federal Information Resources*.

The results of our tests disclosed no instances in which the HHS financial management systems did not substantially comply with applicable Federal accounting standards or the U.S. Government Standard General Ledger.

The HHS CFO prepared a 5-year plan to address FFMIA and other financial management issues. Although certain milestone dates have passed, we recognize that the plan will require periodic updating to reflect changed priorities and available resources.

Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit; accordingly, we do not express such an opinion.

****

This report is intended solely for the information and use of HHS management, OMB, and the Congress. It is not intended to be and should not be used by anyone other than these specified parties.

Michael Mangano

Michael F. Mangano
Acting Inspector General
Department of Health and Human Services

February 26, 2001
CIN: A-17-00-00014

FISCAL YEAR 2000 CFO REPORTS ON HHS OPERATING DIVISIONS AND SERVICE ORGANIZATIONS

Nine separate financial statement audits of HHS operating divisions were conducted in FY 2000:

- Administration for Children and Families *(CIN: A-17-00-00001)*
- Centers for Disease Control and Prevention *(CIN: A-17-00-00008)*
- Food and Drug Administration *(CIN: A-17-00-00006)*
- Health Care Financing Administration *(CIN: A-17-00-02001)*
- Health Resources and Services Administration *(CIN: A-17-00-00003)*
- Indian Health Service *(CIN: A-17-00-00004)*
- National Institutes of Health *(CIN: A-17-00-00007)*
- Program Support Center *(CIN: A-17-00-00005)*
- Substance Abuse and Mental Health Services Administration *(CIN: A-17-00-00002)*

Four Statement on Auditing Standards 70 examinations were conducted:

- Center for Information Technology, NIH *(CIN: A-17-00-00010)*
- Central Payroll and Personnel System, Program Support Center *(CIN: A-17-00-00012)*
- Division of Financial Operations, Program Support Center *(CIN: A-17-00-00009)*
- Payment Management System, Program Support Center *(CIN: A-17-00-00011)*

Appendix II

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D.C. 20201

FEB 26 2001

Michael F. Mangano
Acting Inspector General
Department of Health and Human Services
Washington, D.C. 20201

Dear Mr. Mangano:

This letter responds to the Office of Inspector General opinion of the FY 2000 audited financial statements of the Department of Health and Human Services. We concur with your findings and recommendations.

We are tremendously pleased that, once again, your report reflects an unqualified, or "clean", audit opinion for the Department. Through our joint efforts, we were able to reach the goal of both a clean and timely Departmental financial statement audit.

We also acknowledge that significant internal control weaknesses remain. In addition to the incremental progress we have made on these weaknesses over the last year, we have greatly accelerated our efforts to improve our financial systems to ultimately resolve these material weaknesses.

I would like to thank your office for its continuing professionalism during the course of the audit.

Sincerely,

Dennis P. Williams
Acting Assistant Secretary for Management and
Budget/Chief Financial Officer

HCFA INFRASTRUCTURE PENETRATION TESTING
QUARTERLY TEST PLAN NUMBER 1

WINDOWS NT DESKTOP ENVIRONMENT
INTERNAL SYSTEM SECURITY

TEST R[redacted]

Prepared for:

Health Care Financing Administration
7500 Security Blvd.
Baltimore, MD 21244-1850

COMPLETE

:
·oup, Inc.
evard
1706

March 9, 2001

Executive Summary

The Health Care and Financing Administration (HCFA) is the agency of the Federal Government that administers the Medicare and Medicaid programs. Much of the data and information collected in administering these programs relates to individuals, and is private, sensitive, and confidential information. Access to all such information is controlled by the Privacy Act of 1974, as amended, and the Computer Security Act of 1987, as well as various rules, policies, and guidelines of the Department of Health and Human Services (DHSS), Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST).

In order to meet these legal and regulatory requirements, HCFA has embarked upon a comprehensive systems security program. This program encompasses a variety of activities, ranging from the development and implementation of systems security policies and procedures to the testing and analysis of existing hardware and software applications.

Task 5 of HCFA Contract, dated August 30, 2000 requires Allied Technology Group to perform Internal System Security Testing at the HCFA Baltimore facility. Therefore, in accordance with the Quarterly Infrastructure Penetration and Web Presence Testing Test Plan #1, dated January 30, 2001 and approved by HCFA, Allied Technology conducted Internal System Security Testing during the period February 6-8, 2001.

The focus of the internal system security testing was to determine if the internal network controls are effective in preventing and/or identifying an approved network user from gaining unauthorized access to specific information resources, or to compromise HFCA operations and associated IT assests. The testing was performed in two parts:

1. A complete security assessment was performed using two workstations that were allocated by HCFA officials.

2. The same workstations were then used to scan across the internal HCFA network for selected subnets containing workstations. The purpose was to find open ports, services and shares.

The workstation assessment revealed a number of security vulnerabilities including:

- Corrupt Antivirus Detection
- Service Pack Version Installed
- No Current Patches or Fixes
-
-
- Account Enabled
-
- Inadequate Permissions

- Software Installation Allowed Under [redacted] User Access
- Vulnerability to [redacted] Program Installation
- Weak Logon and Shutdown Configuration
- No Floppy or CD-ROM Drive Policies
- Security Event Log Not Set

In addition, [redacted] services were discovered on printers with the following IP addresses.

- [redacted]

The second segment of the HCFA internal penetration test revealed that there are a number of vulnerabilities present that expose HCFA to exploitation or compromise.

- Poor Password Management
- Default File Sharing
- [redacted] Services on Printers
- Potential Denial of Service Vulnerabilities
- Open Ports and Services Including [redacted]
- [redacted] Account Enabled
- [redacted]
- Software Installation Allowed Under Normal User Access
- Unauthorized Access to [redacted] Information

A significant increase in additional open ports and services between the initial sniff and the subnet scans conducted for this test was revealed. Ports and services found open in the October 17 initial sniff are still open. Ports and services found NOT open in the October 17 results are now open. Additional services that have been added also show open ports and services.

Allied Technoloy Group met immediately with HCFA officials to inform them of these security weaknesses and vulnerabilities and anonymous ftp services.

The remainder of this report describes in detail the testing methology and results obtained, and makes recommendations to improve security on the HCFA internal systems.

3.0 Findings and Recommendations

The security assessment of the HCFA [redacted] workstation environment shows that an internal user with 'normal access' may uncover vulnerabilities during an exploit attempt of the HCFA network that would allow further exploit of the HCFA network enterprise and its connected systems. Although a few minor configuration changes were noted, the overall desktop environment on the two [redacted] workstations tested is configured to the [redacted] default installation. In its default configuration, [redacted] contains a number of known security vulnerabilities.

A number of major security vulnerabilities also were discovered on the subnets tested, exposing HCFA to a number of serious potential vulnerabilities. The following [redacted] addresses registered to HCFA are running unnecessary services including potential denial of service vulnerabilities, [redacted]

- [redacted]

In addition, [redacted] rvices were unc[redacted]ughout this internal testing on printers with the following IP addresses [redacted]

- [redacted]

The assessment also shows additional security weaknesses in the HCFA [redacted] environment. Corrupt ant-virus detection definitions were found, no apparent floppy or CD-ROM drive policies were in place, software installation was allowed under normal user access, and passwords were cracked easily [redacted]

- Poor Password Management
- Default File Sharing
- [redacted] Services on Printers
- Potential Denial of Service Vulnerabilities
- Open Ports and Services Including [redacted]
- [redacted] Account Enabled
- [redacted]
- Software Installation Allowed Under Normal User Access
- Unauthorized Access to [redacted] Information

3.2.1 Password Management

Findings

Weak passwords present a significant security risk, even if proactive measures are implemented, such as using [redacted] and forcing a strong password policy. In its attempts to successfully subvert several user and administrator passwords, Allied Technology discovered blank, easily cracked, and poorly managed passwords, both from user and administrator accounts.

Allied Technology utilized User Manager to obtain user account information on the [redacted] workstations tested. Using [redacted], Allied was able to very quickly crack passwords for a user account on the [redacted] workstation. On the Baseline [redacted] workstation, the [redacted] account did not have a password at all.

If not configured properly, the file sharing capability can be used to [redacted] password-cracking software to find [redacted] rmation of all workstations under the same network administration, includi[redacted] The file sharing capability on the HCFA workstations was enabled by default. In addition, this capability, which is normally referred to in [redacted], was not named. Allied Technology was able to use remote shared connections to install [redacted], which was then used to crack passwords on other shared systems.

Recommendations

[redacted] allows passwords of up to 14 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and non-printing ASCII characters, (generated by using the Alt key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character within the first seven characters.

Blank passwords are unacceptable and should be disabled. HCFA administrators can prohibit blank passwords using User Manager or User Manager for Domains. To do this,

open the Account Policy dialog using the Policies | Account command, and make sure that the minimum password length is set to a reasonable value.

HCFA should set stronger password policies. Use the Account Policy dialog in the [redacted] application (choose the Policies | Account command) to strengthen the system policies for password acceptance. [redacted] suggests that the following password practices be implemented.

- Set the minimum password length to at least 8 characters
- Set a minimum password age appropriate to your network (typically between 1 and 7 days)
- Set a maximum password age appropriate to your network (typically no more than 42 days)
- Set a password history maintenance (using the "Remember passwords" radio button) of at least 6