S. Hrg. 105–609

WEAK COMPUTER SECURITY IN GOVERNMENT: IS THE PUBLIC AT RISK?

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

MAY 19, 1998

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

49–530 cc WASHINGTON : 1998

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-057456-0

COMMITTEE ON GOVERNMENTAL AFFAIRS

FRED THOMPSON, Tennessee, *Chairman*

WILLIAM V. ROTH, JR., Delaware	JOHN GLENN, Ohio
TED STEVENS, Alaska	CARL LEVIN, Michigan
SUSAN M. COLLINS, Maine	JOSEPH I. LIEBERMAN, Connecticut
SAM BROWNBACK, Kansas	DANIEL K. AKAKA, Hawaii
PETE V. DOMENICI, New Mexico	RICHARD J. DURBIN, Illinois
THAD COCHRAN, Mississippi	ROBERT G. TORRICELLI, New Jersey
DON NICKLES, Oklahoma	
ARLEN SPECTER, Pennsylvania	MAX CLELAND, Georgia

HANNAH S. SISTARE, *Staff Director and Counsel*
ELLEN B. BROWN, *Counsel*
JOHN P. PEDE, Professional Staff Member
WILLIAM C. GREENWALT, Professional Staff Member
JOHN H. COBB, Investigative Counsel
MARGARET A. HICKEY, Investigative Counsel
LEONARD WEISS, *Minority Staff Director*
DEBORAH COHEN LEHRICH, Minority Assistant Counsel
LYNN L. BAKER, *Chief Clerk*

CONTENTS

WITNESSES

TUESDAY, MAY 19, 1998

ALPHABETICAL LIST OF WITNESSES

APPENDIX

WEAK COMPUTER SECURITY IN GOVERNMENT: IS THE PUBLIC AT RISK?

TUESDAY, MAY 19, 1998

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:22 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Fred Thompson, Chairman of the Committee, presiding.

Present: Senators Thompson, Collins, Glenn, and Lieberman.

OPENING STATEMENT OF CHAIRMAN THOMPSON

Chairman THOMPSON. The Committee will be in order, please. The Governmental Affairs Committee today is holding the first of a series of hearings on the security of Federal computer systems. While advances in computing power are creating many opportunities in business and are remaking how the government does business and such things as how future wars are fought, it also creates dangers which must be reduced. It seems that the more technologically advanced we become, the more vulnerable we become. Today's hearings will address the darker side of the information revolution while exploring how we can better protect governmental information.

Computers are changing our lives faster than any other invention in our history. Our society is becoming increasingly dependent on information technologies which are changing at an amazing rate. The singing greeting cards which you buy today for $2 have more computing power than existed in the world before 1950. A video camera which you buy today for less than $1,000 has more computing power than a 1960's computer the size of this room. Combine this rapid explosion in computing power with the fact that information systems are being connected together around the world without regard to geographic boundaries. This interconnection creates both opportunities and dangers.

In today's hearings, we will discuss these challenges and we will hear that the nature of this challenge comes from the fact that our Nation's underlying information infrastructure is riddled with vulnerabilities which represent severe security flaws and severe risk to our Nation's security, public safety, and personal privacy.

While hacker attacks receive much media attention, even more worrisome are the attacks that go unknown. The nature of attacks in the information age seems to allow a malicious individual or group to inflict extensive damage from the comfort and safety of their own home. We must ask whether we are becoming so depend-

ent on communications links and electronic microprocessors that a determined adversary or terrorist could possibly shut down Federal Government operations or damage the economy simply by attacking our computers. At risk are systems that control power distribution and utilities, phones, air traffic, stock exchanges, the Federal Reserve, and taxpayers' credit and medical records.

Unfortunately, government agencies are ill prepared to address this situation. We as a Nation cannot wait for the Pearl Harbor of the information age. We must increase our vigilance to attack this problem before we are hit with a surprise attack.

Our witnesses today have substantial knowledge about what the problems really are and can recommend solutions. First, Dr. Peter Neumann, a recognized private sector expert on computer security, will provide the Committee with an overview of information security issues and testify on the systemic security problems in the government's computer systems.

Then we will hear from L0pht, seven members of a hacker think tank who identify security weaknesses in computer systems in an effort to persuade companies to design more secure systems. L0pht members will testify about specific weaknesses which enable hackers to exploit the Nation's information infrastructure and government information.

Senator Lieberman, do you have any statement to make.

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. I do, Mr. Chairman. First, let me thank you for holding this hearing, which I take it to be the first in a series of hearings on this very important issue. I think this hearing provides a prime example of one of the great responsibilities of this Committee—oversight and looking over the horizon, if you will, or at least using the Committee's investigative powers to educate ourselves and our colleagues and perhaps the public about threats to, or inefficiencies in, government and then, hopefully, to lead or stimulate an effort both in the public and private sector to do something about those problems.

I must say that I am truly troubled by the material that I have read in preparation for this hearing, which brings me personally and in more detail into this realm than I have been before. I find the testimony of the witnesses that we will hear from today, as well as the findings in the GAO reports I gather you will be releasing shortly, really should give us all pause.

Like the rest of our society, our government has become increasingly reliant, remarkably so, on computers in recent years, in a very short number of years, to store information, to communicate and to control important aspects of our lives. But according to GAO and the witnesses that we will hear from today, all of that is, to put it bluntly, at risk, and, therefore, so are we, because we simply have not taken the steps necessary to protect our computer systems from unauthorized infiltration.

As a result, the most private information about all of us and the most vital details of our national security, for instance, are all available to bad actors who, according to today's witnesses, may not need much more than a good knowledge of computer systems and some time and ingenuity to gain access to our government's

computer systems. In fact, the GAO studies on the issue have found government computer security to be so lax that GAO has put that subject on the list of its high risk government programs.

I know Mr. Neumann, from looking at his testimony, is going to provide us with what I consider to be a disheartening depiction of the state of our government's computer security, and the people from L0pht also will offer a very troubling portrayal of the security of our computer systems. Their written testimony notes, they have "found Internet and computer security to be almost nonexistent" and they claim that in less than 30 minutes, they could make the Internet unusable for the entire Nation.

That is obviously all extraordinarily unsettling, and I say that both as a Senator and as a citizen. I am troubled not only by the substance of what I have read and what we will hear today, but also by the sense that government agencies are not yet responding aggressively enough to address these problems, something I hope these hearings will help us change.

So, Mr. Chairman, I thank you again for focusing the Committee on this very important topic and I look forward to hearing from our witnesses today both about the scope of the problem we have and, of course, most importantly, about what we can do to make it better. Thank you.

Chairman THOMPSON. Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you very much, Mr. Chairman. Mr. Chairman, I want to start by applauding your leadership in holding this hearing on the issue of the security of government computers in light of recent reports of intrusions into the systems of critical entities, such as the Department of Defense and the Department of State.

The investigation into Internet fraud which the Permanent Subcommittee on Investigations has conducted has heightened my awareness of the vulnerability of government systems, and indeed, all computer systems. Your first witness has been a familiar expert in assisting the Permanent Subcommittee on Investigations in its past investigations into this area and I am delighted to see him here today.

The pervasive vulnerability of our computer systems raises the specter of malicious attacks by terrorists rather than simply the relatively benign intrusions by teenage hackers. That is of tremendous concern to all of us here and I commend you for your leadership and look forward to hearing the witnesses. Thank you very much.

Chairman THOMPSON. Thank you very much.

Senator Glenn.

OPENING STATEMENT OF SENATOR GLENN

Senator GLENN. Thank you very much, Mr. Chairman. I am glad we are having this hearing, too. I want to congratulate you on calling this hearing.

I guess some things may be looked at as being too good to be true. We have tremendous promise in the computer age and all it is doing for us. It is opening up worldwide commerce in ways we

never thought possible before, uniting the world in many ways, and yet causing a lot of problems in others, as people can use this new technology in ways that disadvantage the advantages, also.

A couple of weeks ago, we had a hearing on the year 2000 software date problem. It seems like such a simple problem. Programmers use two digits instead of four to indicate the year, so simple, but the potential costs in getting it fixed are staggering. The answers to problems of computer security ought to be simple if people lock their cars and businesses guard their trade secrets and so on. We are vulnerable to eavesdroppers and disgruntled employees and malicious hackers, criminals, or even bored teenagers just seeing what they can hack into.

In 1994, I asked GAO to examine security risks in DoD computers and we held a series of similar hearings 2 years ago through our PSI, Permanent Subcommittee on Investigations. The issue, though, continues to grow in importance, and I thank the Chairman for calling this hearing.

The GAO's 1996 report described a very, very porous system. For example, a teenage hacker from Great Britain used phone lines around the world to disguise his break-in into computers at the Rome Air Force Base lab in New York. Among other things, he copied and downloaded air tasking order information. He even went through the DoD system to get into computers in South Korea. If they had noticed, we could have had an international incident.

Since the Rome hacker, we have seen even more hacking into DoD computers. The point is that this is not new. It is also getting worse. The government, the private sector, and public should not be surprised. The question is, what can we do about it? How do we protect ourselves and the critical information on which we now depend for transportation, communication, financial transactions, national security, and more?

This was to be the first of 2 days of hearings. In the second day, we were to hear from GAO about computer security problems at the FAA and State Department. In my experience with GAO, they bring the sort of expertise and analysis needed to really uncover and understand agency management problems, such as those involved in computer security. The GAO reports show very troubling lapses at both FAA and the State Department, and I recommend that everyone read those reports closely. So I hope this hearing is only the first in a series of hearings through which we can find some solutions to those problems as well as others.

If you look at this, in some ways, it is a whole new way of making warfare. It could be used that way, and I do not think that that overstates it one bit. What you try to do in war is bring an enemy's economy to its knees, and if you look at what could be done right now with some of the hackers we have seen getting into some of the programs, they can transfer Merrill Lynch accounts to somebody else, Chairman Thompson's many millions of dollars into the Federal Reserve and from the Federal Reserve back to——

Senator COLLINS. Can I have them?

Chairman THOMPSON. That could be a problem. [Laughter.]

Senator GLENN. And in addition to that, you take more seriously things like the Northeast grid. Our electrical grid is controlled by computers, about a half dozen nodes control the Northeast grid

alone, as we learned in hearings some years ago. If you dump the Northeast grid all at one time by somebody hacking into it and transfer a lot of financial accounts all over the place and foul up Wall Street markets, you have gone a long ways toward doing what you normally would do with warfare. So these are very, very serious matters and I do not think that we as a country have really focused on these things important issues enough yet.

NSA is looking into these things. We know that, and they do not make any bones of the fact that they think this is a problem for our banks and our financial institutions, and they are willing to even counsel banks on how to take care of some of these problems. So I am glad we are having this hearing this morning and I thank you, Mr. Chairman.

Chairman THOMPSON. Thank you.

I will now recognize our first witness, Dr. Peter Neumann, Principal Scientist from Computer Science Laboratory in Menlo Park, California. Dr. Neumann is a renowned expert on computer security, with 45 years of computer experience. I would invite anyone to review Dr. Neumann's background statement, which will be made a part of the record. It is most impressive, his academic background, his professional background and experience. He has been very helpful to the Congress before. We may be a little discouraged that he does not see more progress from his efforts with us, but we appreciate you being here, Dr. Neumann. Would you give your statement, please.

TESTIMONY OF PETER G. NEUMANN,[1] PRINCIPAL SCIENTIST, COMPUTER SCIENCE LABORATORY, SRI INTERNATIONAL

Mr. NEUMANN. It is an enormous pleasure for me to be back here again with you. It is even more delightful to realize that you have just given the first 15 minutes of my testimony, which saves me, out of a 12-minute testimony, a great deal of time.

There is a tremendous amount of awareness and wisdom that is reflected by your remarks, so I am greatly pleased that the four of you, at least, have realized the severity of the problem we are dealing with.

In the small, what we are confronted with is the ability of the U.S. Government to maintain its own well-being—air traffic control, telecommunications, all of the critical infrastructure entities that have been mentioned by you and by the President's Commission on Critical Infrastructure Protection. In the large, however, it is really the survival, if you will, of the United States as a whole, of all citizens. It is not just survival of the government. It is survival of the Nation as we know it.

So the fundamental issue confronting us, even though the title of your session has to do with security, is much broader than that. It is threats to reliability, security, availability, and, indeed, survivability of the infrastructures in the large, not just the critical infrastructures that the President's Commission has recognized, but all of the computer-communication information infrastructures, as well.

[1] The prepared statement of Mr. Neumann appears in the Appendix on page 52.

One thing that the President's Commission realized was that all of these so-called critical infrastructures are very closely interdependent. They all depend on power. They all depend on telecommunications. The one thing the PCCIP really did not stress enough is that they all depend on computer communication infrastructures.

Everybody wants to connect to the Internet today. The problem is that the Internet is simply not ready for prime time, if we are talking about security, reliability, availability, and survivability. So I am going to cast those out as sort of a mantra of what we need in the way of dependable systems.

We have wonderful systems in terms of the functional power of the applications, but I think the folks who are bringing you most of the, what is it, 90 percent of the personal computers, do not have as a part of their business model any of that mantra. Security, reliability, availability, survivability, are not a part of that business model.

As a result, we see a great many computer systems, not just subject to the possibility of hacker attacks, but the systems have tended to fall apart on their own without any inducement. Several examples have been given already. In the telecommunications world, we have seen the 1990 AT&T long distance collapse, the AT&T frame-relay collapse very recently, the ARPAnet collapse of 1980. All three of those are the same basic mechanism, something that somebody said a long time ago could never happen. This is a local event in a network propagating and bringing down the entire network. These three events happened without any hacker activity. These are just systems falling apart on their own. The year 2000 problem, which you have mentioned, is another example of systems falling apart on their own.

The fundamental problem here is a real lack of foresight. I might go back in history to 1965, when I was working on Multics with MIT and Honeywell. I was at Bell Labs. We designed a system that was, at that time, more secure than anything that anybody had ever seen before, and that for probably—well, maybe until now, is still the most secure commercially available system because we designed it to be secure. We designed it to be reliable and available.

We also designed it not to have the year 2000 problem. Thirty-five years beforehand, we said, you know, we do not think the system will be around in 35 years, but why build another system that has this problem? That was 35 years ago. So my point there is simply that it takes a little bit of foresight.

Now, you asked, what can we do about all of this. There are so-called experts in the field who will say that security is an administrative problem. All we need to do is manage it properly.

There are others who will say it is an operational problem. There are people who accept a new operating system. They leave the root password the same as it was in the delivery box. They never change it. Are they vulnerable? I think the next set of testimonies will suggest that they are very vulnerable. That is an operational problem.

To someone who is a technologist first, they are going to say, well, it is a technological problem. We cannot solve it without bet-

ter operating systems and without better networking software and without better cryptography that cannot be subverted easily.

To educators, it is an educational problem. So it is the old story: To a man with a hammer, everything looks like a nail. Each person sees it as his own fiefdom.

Putting on my hat as the designated holist, I see it as a global problem. I see it as a weak link problem in which, essentially, every component is a weak link at the moment. The operating systems are not secure. The networking software is not secure. The uses of cryptography are not sound. So we are left with a situation in which any of these weak links can, in fact, bring down the entire system complex. And again, I stress the point that it is not just the security problem, it is also the reliability, availability, and overall survivability problem.

Now, what can we do? My first recommendation is that the government must get its own house in order, and there are quite a few ways in which that can be done. If we look at the raft of website hackings, the Justice Department, the CIA, the Air Force, NASA, all have had their web presences disturbed with bogus websites put up in their place.

We had the two Cloverdale high school kids who managed to break into a bunch of Pentagon systems. In response, Deputy Secretary of Defense John Hamre said, "This is the most organized and systematic attack the Pentagon has seen to date." The fact that two kids with essentially no sophistication whatsoever can break into all those systems is ludicrous. The fact that the Pentagon is saying, we really have to go after all of the kids who are breaking into systems, is a joke. If those systems are so unsecure that they cannot withstand the most trivial of attacks, we are really living in a silly world.

We also hear the story, and this may be beyond the purview of your Committee, but let me say it anyway, that actually, it was not that serious because no classified information was leaked. Now, in fact, there is a lot of unclassified information that is very sensitive. So that statement is, on its face, questionable. The second thing is if there were classified information leaked, that information itself would be classified and you would not hear about it.

So the bottom line is that with the random interception of Newt Gingrich's cell phone call and the recent case of the Secret Service pager messages, all of which were being routinely intercepted, despite the fact that 4 years ago, there was a conference in which it was demonstrated how easy it was to do that, this suggests that we are not addressing the real problem.

The real problem is that the infrastructure stinks, that we are dealing with computers and communication systems that are not secure, they are not capable of withstanding attack. The attacks we have had to date, as has been noted, are not serious, but they could have been. The year 2000 problem offers a glorious opportunity for the massive attack to coincide with January 1, 2000. It would cause massive confusion because nobody would be sure whether it was a security attack or whether it was simply another system collapsing because of the calendar date problem.

So this leaves us with a rather gnawing feeling. When I say that the government must get its own house in order, in my written tes-

timony, I suggest that there are a bunch of things you could do. I suggest that the procurement process itself is defective because the government is not requiring secure, reliable, highly available, highly survivable systems. It was Senator Glenn himself who once said, as I recall, in flying around up there that you were wondering about if this was built by the lowest bidder. This is a serious problem.

Senator GLENN. On a government contract.

Mr. NEUMANN. On a government contract, even. I believe that that mentality is something that is causing us great grief. The government simply is not demanding of Microsoft, for example, that the systems that are procured should be reliable, secure, highly available, highly survivable. Maybe they are in the small, if you never connect it to the network and you never have any dial-up lines. But as soon as you open yourself to the rest of the world with Internet network connections and dial-up lines, you are essentially vulnerable.

Now, what can you do about it? There is lots of research in the community. There are lots of commercial outfits, such as—well, there are commercial applications and non-commercial applications, such as Diffe-Hellman and RSA Public Key Crypto that can be used for massively increasing the authentication. At the moment, we do not even know who is attacking the systems. They are coming in anonymously from remote sites. They are hiding their web presence by weaving through all sorts of different places. The systematic use of reasonable authentication using Public Key Crypto would be a massive step forward.

There is a lot of good research that is coming out of the R&D community. Very little of that research is finding its way into the mass-market commercial products. This is a tragedy, because, as I go back to my Multics system of almost 35 years ago, there was some wonderful research that came out of that project, and there are many projects since, that have, in fact, considerably increased the potential for security, reliability, availability, and survivability.

Let me make one suggestion that I think may not be popular with you, but I think it speaks to the problem of your becoming acquainted with some of these problems in a much deeper way, and this is the question of laptops on the Senate floor, which has come up on various occasions. One of my own Senators does not like the idea very much.

I suggest that if you were to start using laptops on the floor in a very local way, not networked, just for your own use, taking notes, observing some of the history of the legislation that you are considering, possibly having the draft version in front of you, you might discover that there were some benefits there. But as you started to locally network within, say, a dedicated Senate net that was shut off from the Internet and did not have all of these problems of connecting to the Internet, you might discover that you could vote from a hearing room, such as this one, without having to disturb the hearing for half an hour, which has happened to me on two occasions.

It would also allow you to monitor, to track the wording changes in bills that were being promoted or proposed at the time, and it

would also enable you to discover some of the vulnerabilities and flaws in the technology.

But the big benefit would come as you conceived of the possibility of hooking those laptops up to the Internet itself and you would realize that you did not want to do that for a very long time, given the available laptops and the security that they provide.

On the other hand, in the long run, I think this would be a marvelous exercise in trying to come to grips with some of the very real issues that we are confronting.

Now, rather than wandering on, I can go on for a long time here, but I think the bottom line is that there are lots of good techniques out there. They are not finding their way into commercial products. As I said earlier, it is simply not in Microsoft's interest that the systems they develop should be secure, reliable, highly available, and survivable in any sense that deals with the Internet use of those systems.

There is a very serious problem as we get into the uses of the Internet for digital commerce. At the moment, the vulnerabilities in those systems suggest that there will be organized crime activities taking billions of dollars out of the U.S. economy with relative ease if the systems that are available today were to be used.

The thrust of your hearings deals with air traffic control, with finance, with power distribution, with telecommunications systems, and all of those are very vulnerable in one way or another. Essentially, every system I have ever looked at over the many years has been one that could be taken apart. Most of the best market commercial systems are relatively easy to break, as you will hear from the succeeding testimony, as I just glanced through what they are going to say.

So we are confronted with a need for dramatically increasing the security, reliability, availability, and survivability, efficiency, effectiveness, performance of the systems that we are dealing with, but the most important thing, I think, is that we have got to recognize with much greater awareness what the vulnerabilities are, what the threats are, what the risks are.

I do not want to go into great detail as to what those risks are. I have written another piece that you will find on my web site relating to air safety and security. I have worked with Alex Blumenstiel at the Department of Transportation in Cambridge and I mentioned some of the reports that he has written over the past many years. His picture is very gloomy if you look at the potential vulnerabilities.

The real question is, does anyone need to do anything about it, and I think the most important part of that answer is once you understand what the vulnerabilities and risks are, you are then in a position to understand what is worth doing. I think many people are scared of this issue because if they do not do something, then they feel they are liable for not having done something. So it behooves you very greatly to understand what those risks are.

My written testimony, I think, goes on at some length, but I have tried to keep it very succinct, so I think most of you have read it and I am very pleased that you have. I would like to make a few remarks on cryptography before I close.

One of the most difficult issues confronting all of us is the issue of cryptography. I have testified for the Justice Committee on the issue of cryptography specifically and I testified at a time when the Director of the FBI and the Deputy Director of NSA were also testifying. They paint a picture that says, if you do not give them all of the keys to all of the crypto everywhere, you have essentially destroyed the Nation.

If you conceive of putting a key recovery, key escrow infrastructure on the computer systems that I have outlined today, you wind up with something that greatly worsens the security of the overall system because you have put a monster trap door in all of the systems, and if the Cloverdale kids can get into the Pentagon systems today, they will probably be able to get into your key infrastructure systems, into your key management systems, without very much trouble.

So the big failure there, I think, is that the FBI folks and the NSA folks have systematically avoided in looking at the risks. There is a recent NSA report that sort of honestly and openly acknowledges that there are some technical realities that have not been discussed in the opening testimony. I commend that report to you. The former Director of NSA, Mike McConnell, has publicly questioned the sensitivity of the key recovery approaches, and Secretary William Daley recently said that the export controls that are in effect may, in fact, totally compromise the American business picture in terms of feeding the overseas marketplace for secure systems.

This is a gap that we cannot afford, and I suggest that before you do any voting in the Senate, this is an issue that strikes very deeply at the entire fabric of our Nation. The privacy issues are important. The law enforcement issues are important. But the simplistic solution of allowing the keys to be obtained under whatever warrant process or subpoena process, as suggested by McCain-Kerrey, is a very serious mistake. So, actually, I endorse the Ashcroft-Leahy-Burns bill which has come up in the last week as one approach that needs very serious consideration.

The bottom line is that we are in very bad shape. The potential risks are probably much worse than I have conveyed, but we will not know until some massive disaster actually occurs and then it is too late. So the recommended solution is that you become very aware of what our risks, vulnerabilities, and threats are and that through this awareness, you will be in a much better position to steer the government, and by steering the government itself, you will help the Nation. Thank you.

Chairman THOMPSON. Thank you very much, Dr. Neumann. I think awareness is certainly a starting point and you are helping us get there. We may always have a problem with computer voting in the Senate, though. I can see that on a controversial vote, in light of the testimony we are hearing, someone would undoubtedly claim that somebody else really cast that vote for him and it was not him.

Mr. NEUMANN. That is why you need good authentication.

Chairman THOMPSON. Your testimony is really remarkable in the sense, not that it is new, but the fact that it is not new. It points out something we have known for a long time, and that is that our

technology has outstripped our ability to handle our technology. You have testified about that before. You said in your written statement, I think, that perhaps we will have to have a Chernobyl of some kind in order to get people's attention and that something like that could happen. You have listed several of the dire things that have already happened more or less by accident and the potential of things that could happen.

I am impressed with your pointing out that it is not just the safety issue but our seeming inability to develop adequate complex systems. We pride ourselves on our ability. Most of us who are not experts in the area think that we have tremendous capabilities in this area, and we do. But you mention our shortcomings in trying to improve our air traffic control system, when we tried our IRS modernization program, and even the "Deadbeat Dads" program that we tried to link up around the country, all have been failures, basically. Is that correct?

Mr. NEUMANN. Yes.

Chairman THOMPSON. And that has nothing to do with security issues. That is just old fashioned inability to develop complex systems to deal with our problems. Then you lay on top of that the interconnectivity and the rapid acceleration of commerce over the Internet. As you point out, the President's Commission on Critical Infrastructure Protection noted that our infrastructures have problems and vulnerabilities anyway—I mean, generally speaking, power, transportation, finance and banking, and telecommunications. But the key ingredient for all of that, what they all have in common is that they are all dependent on an underlying computer communications information infrastructure which is very much flawed, and that we have known that for a long time.

You say that there is a lot of research out there, a lot of good research, but it is not finding its way into commercial endeavors. Why is it not? Is there not enough competition in this area in order for it not to make it in someone's interest to develop something commercially viable in this area?

Mr. NEUMANN. One of the most important attributes of this whole thing is diversity. If you have the same operating system, the same software running everywhere throughout the U.S. Government, the same vulnerabilities and the same flaws are all subject to massive attacks. The notion, then, is one that needs competition. If there is only one solution that everybody is trying to use and it does not have any security in it, we have a problem.

As I noted earlier, Microsoft has done a phenomenal job of bringing computers into many, many applications. They have not done a really good job—in fact, they have done no job whatsoever—in trying to make their platforms meaningfully secure, available, reliable, and survivable in the sense of whenever they are networked together, they should be much more robust.

Chairman THOMPSON. Why are they not induced to do that?

Mr. NEUMANN. It does not fit their business model. There is no money in it. They are looking at the bottom line. How does it benefit them? I think they have claimed that the U.S. Government is one percent of their business and who are you guys to tell them what they should do?

Chairman THOMPSON. I think I heard that recently. [Laughter.]

Mr. NEUMANN. If you are only one percent of their business, you do not drive their marketplace. The problem is that, ultimately, in the long run, it has to be in their best interest to build systems——

Chairman THOMPSON. What would make it in their best interest to do that?

Mr. NEUMANN. I have no idea. I have racked my brains on that one for a long time. One of my colleagues has been hired by Microsoft and he is working not on security—he is one of the world's greatest security gurus—he is working on anti-piracy.

Chairman THOMPSON. Is the government, then, going to have to bypass the commercial intermediary and develop something itself? Obviously, we are totally dependent on this. We are not getting what we need. You cannot buy anything off the shelf. I think as these gentlemen behind you will testify later, also, there is not anything out there. Those who claim to be selling safe systems are not really, and it seemingly does not exist. Are we not in a position where the government is going to have to perhaps develop it itself?

Mr. NEUMANN. That may be true. I am right in the middle of a research project, actually, for the U.S. Government in which I am trying to assess the question of can you take systems that are not robust—this is the "can you make a silk purse out of a sow's ear question"—can you take systems that are not very robust and still come up with something that is much more robust? There are some ways in the research community that you can do this, and I am exploring all of the ones that I can find. Perhaps in another 3½ months, 4½ months when I am done, I will share that report with you.

I believe that there is a lot of very good research in terms of security, authentication, anomaly misuse detection, of discovering what happens after you have been taken to the cleaners.

Chairman THOMPSON. And it is not being used, which seems to indicate it is a management problem.

Mr. NEUMANN. Yes. In that sense, it is a management problem.

Chairman THOMPSON. And getting people's attention within the government, making it in their self-interest, managers' self-interest to utilize it and become knowledgeable of what is out there.

Mr. NEUMANN. This is true.

Chairman THOMPSON. Let me ask you just a couple more questions. Y2K, first of all, off our beaten path here a little bit, but what do you think about the nature of that problem in general? Has it been overestimated, overhyped, or under, or what is your total assessment of where we are likely to be on January 1, 2000?

Mr. NEUMANN. Have you seen Representative Horn's scorecard, his report card?

Chairman THOMPSON. I think I saw that in the newspaper.

Mr. NEUMANN. What he shows, basically, is that the Department of Education, Department of Defense, Department of Transportation, Department of Labor, and the Department of State are all failing miserably in their attempts to ratchet up their systems to be able to tolerate——

Chairman THOMPSON. We have hearings on that, too, and came to the same conclusion.

Mr. NEUMANN. Right.

Chairman THOMPSON. But I assumed he was probably getting his information from people like you.

Mr. NEUMANN. No. Actually, he is getting it straight from the horse's mouth, or—well, yes.

Chairman THOMPSON. That is where we get a lot of ours. But, anyway, do you have any independent assessment of all that as a scientist?

Mr. NEUMANN. Let me speak on behalf of the GAO Executive Council on Information Management, of which I am a member. We have been beating very hard on that problem. We have talked with Senator Bennett, we have talked with Representative Horn, we have talked with John Koskinen, who is the President's Y2K czar, and I do not think we get a warm, fuzzy feeling about what the U.S. Government is doing.

I think that the industry is not doing a particularly great job, either. A lot of companies have still to recognize the severity of the problem in some systems. There are some systems that will not be affected because, again, as I said, they recognize the problem and——

Chairman THOMPSON. You say that these security problems are even more severe or more critical than the Y2K problem——

Mr. NEUMANN. I think they are more insidious.

Chairman THOMPSON [continuing]. But that we are getting sidetracked from the security problems because of the Y2K problems.

Mr. NEUMANN. I think this is true. I think the security problems are much more insidious and we have sort of gotten to the point where everybody is concerned with Y2K now and very few people have realized that the Y2K problem is really the tip of the iceberg of the software development problem. You mentioned the IRS. You mentioned the FBI fingerprint system. You mentioned the air traffic control.

Chairman THOMPSON. What happened with regard to the fingerprint system?

Mr. NEUMANN. I think the whole thing was cancelled. It simply did not work. But again, in relation to those kinds of systems, the problem is, unless you know what you are trying to build, unless the requirements are set out in advance that it has to be secure, reliable, available, and survivable, you do not get there. The Y2K problem is one where this problem, although it was recognized years ago, it was not demanded by anybody that the solution had to be forthcoming soon. "We will solve that when we get there."

Chairman THOMPSON. Everybody assumed there would be a solution and there was not.

Mr. NEUMANN. And there is no simple solution to it. But the security problem is even more insidious in the sense that not only is there no simple solution, as I said, it is a weak link problem and any weak link can, in fact——

Chairman THOMPSON. And you do not even know the nature of the problem, do you, because there has not been risk assessment in most cases as to the extent of the vulnerability.

Mr. NEUMANN. We have had several cases, for example, of electromagnetic interference. You can say that is a security problem. You can say that is a reliability problem or a survivability problem. There were Blackhawks (helicopters) that went down as a result of

EMI and the pacemaker case of the guy who was killed when the pacemaker was reset by stray magnetic EMI. There is an Australian Melbourne airport case that the radio frequency communication was destroyed, basically, their ability to operate. This is another kind of a problem that tends to be ignored. So, yes, it is another attribute of the security problem that one has to think about and it is just another weak link.

Chairman THOMPSON. Thank you very much.

Senator Glenn.

Senator GLENN. Thank you, Mr. Chairman.

We can restate the problem over and over. We have been doing that in hearings here for a long time. I am not sure we have any answers yet on this, though. You were talking about the government getting its house in order. I agree with that, and you said the infrastructure system stinks, I think, to use your words, and I would agree with that, but I am not quite sure where we go from there.

If I was made computer czar for the U.S. Government today and I had full authority to do everything that I wanted to do for computers to make them secure, to cure this whole system and to set up an infrastructure that would be good, what should I do? I am not quite sure what the first move would be.

Let us turn it around. If you were sent across the river or you were brought in here and you were given full authority by the administration and Congress, voted to be the computer czar for the American public right now, what would you do? How would you change the infrastructure?

Would you encrypt more? Is encryption the final answer? Do we have encryption now that will work into the indefinite future? Do we have encryption that nobody can violate? Would the hackers who are real pros at this—like those sitting behind you who will testify a little bit later—would agree? Is there encryption now that could be put into general use that they could not break?

If you could give us a 1, 2, 3, 4, 5 step scenario of what you would do if you were the computer czar of government, what would your steps look like? And I guess the next question would be, how much would it cost? Or, I guess we should say, how much would it cost if we do not do it soon? That would be more appropriate.

Mr. NEUMANN. That is a very important question. Let me address the encryption issue first and then I will go back to your——

Senator GLENN. Yes. Give me a 1, 2, 3, 4 here on what you would do if you were the computer boss for all of government.

Mr. NEUMANN. Let me answer the encryption question first, though.

Senator GLENN. Yes.

Mr. NEUMANN. The issue here is that even the strongest encryption today may be breakable if it is put onto a platform that is not secure. So there are some serious issues involved in operating system security to protect the encryption itself.

You need strong crypto to implement good computer communication security, but you also need good computer systems in order to implement strong crypto. So there is a catch–22 here that I allude to in my written testimony.

Now, the most important thing for the government, if I were the computer czar, I would try to bring in some in-house expertise. You need people on government staff—I do not know if you can pay them enough to get them to do what is necessary—but you cannot rely on consultants and companies to be project managers for $4 billion developments. You need the in-house expertise of understanding what it takes to do a large procurement.

Senator GLENN. Let us say they understand that, though; and let us say we have got computers that are the best. They are not cheap computers. They are the best, the type you are talking about. Are we going to have to write new software programs to do this? Are we going to have to put crypto in with software programs? What do we do to get this thing under control?

Mr. NEUMANN. Crypto is only one piece of the whole puzzle. You need good crypto. You need good operating systems. You need good networking protocols. At the moment, the networking protocols have evolved historically. They are not designed to be secure, reliable, available, and survivable. So we need new protocols.

We need new operating systems, or better operating systems. We need better networking software. We need authentication pervasively throughout the system so that you can tell who is coming in. You have insider problems as well as outsider problems. You need authentication of insiders so that you can actually tell who it is who is accessing the system.

Senator GLENN. Do we need changes—and I do not think I am overstating this—but do we need changes in the Constitution to let this happen, because we might be infringing on people's rights for the flow of information and so on?

Mr. NEUMANN. I do not think so, but you have jogged me to mention privacy, which is something that I did not really get into in my testimony. Privacy is a very serious problem in this country, and at the moment, we are on a downward spiral where privacy is going down the tubes.

I believe that a corrective balance is needed. There may be some legislation to deal with non-governmental databases. At the moment, there are privacy regulations dealing with Federal Government databases. They are not widely enforced, but they do exist.

Senator GLENN. Back to square one, though. If we are procuring new computers for the government, are there only certain types we should procure? I am a computer neophyte. I have trouble getting my E-mail off sometimes, so I am talking as one who is not in your league as far as even discussing this. But should we only buy certain types of computers with certain characteristics, and what are those characteristics?

Mr. NEUMANN. I cannot give you specific types of computers. I can give you specific characteristics. You would like a mail system, for example, that seamlessly uses encryption. PGP is one example. It is available essentially in a free form. There are operating systems that you can find that are nonproprietary that are quite good. There is networking software experimentally, especially in terms of authentication, that you can use that is much better than what you can get.

Senator GLENN. Let us say you are still the computer czar and you are going to set up something for the Pentagon or for CIA for

their computers. How would you make them absolutely secure so they cannot be hacked into?

Mr. NEUMANN. You cannot. There is absolutely no way of doing that.

Senator GLENN. There is no crypto we know of that cannot be broken?

Mr. NEUMANN. There is no way of guaranteeing that it cannot be broken into. And you also have to worry about the misuse from inside. So there is no way of——

Senator GLENN. Should we cut down on the use of computers, then? If that information is going to be public to any hacker around the world who wants to tap into it, then we had better keep it off the Net.

Mr. NEUMANN. Well, there are several issues here. One is if NASA puts its web site up on the Internet and it gets broken into, is this a serious problem? Probably not, because——

Senator GLENN. Well, it depends on what you are talking about. If you are talking about the commands back and forth to a spacecraft, I consider that very serious, I can tell you. [Laughter.]

Mr. NEUMANN. That should not be on their web site.

Senator GLENN. If you are talking about putting information out there on past research and things like that, that is something else. We have a policy of making that available to everybody in the world since Eisenhower made that decision a long time ago, in contrast with the Soviet system. But in a lot of these things now, NASA is a good example. The commands that go back and forth to control the spacecraft and reentry and those things that are absolutely critical to the people that are up there, or DoD, there is——

Mr. NEUMANN. Yes, and you do not put that on your web site.

Senator GLENN [continuing]. There is stuff that is on computers over there that they use for command and control. This is not just for information flow. This is command and control stuff.

Mr. NEUMANN. Yes.

Senator GLENN. And you are saying that those cannot be made tamper-proof?

Mr. NEUMANN. Those cannot be made tamper-proof if they are on the Internet and if they have dial-up phone lines and maintenance paths and things like that.

Senator GLENN. Can there be separate computer systems then set up that would not be on the Internet and not be on phone lines. How would you do that?

Mr. NEUMANN. This would be a good idea. Let me give you one illustration.

Senator GLENN. Can you do that?

Mr. NEUMANN. Let me give you one illustration of probably 15 years ago when I was down at Johnson Space Center. One of the engineers there was talking about how the MIT professor, using his UNIX system, would be able to uplink to the space station and control his experiment in real time using the same computer that was being used to control the space station, and I pointed out that this was not a very good idea because every terrorist in the world, every high school kid, anybody who was curious would find that, oh, he can look at the active controls of the space station and discover what is going on. I was stunned by the fact that the engineer then

scratched his head and said, "They can do that?" This is a problem. So you do not put life-critical stuff, Nation-critical stuff, into an environment that is fundamentally not secure.

Senator GLENN. I may have some questions to ask in Houston on my next visit. [Laughter.]

Thank you, Mr. Chairman My time is expired.

Chairman THOMPSON. Senator Collins.

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

Dr. Neumann, you described yourself in your written testimony as feeling a bit like Cassandra, that you give these dire warnings over and over and nothing seems to happen. If what you have said about the Department of Defense's reaction to the recent break-in in its computers by relatively unsophisticated kids is accurate, it sounds like Cassandra's warnings still have not reached the Department of Defense.

Mr. NEUMANN. I would think that is true. On the other hand, I would guess—I have no knowledge inside—that Director Hamre was a little bit off base in that he might have by now realized that what he said was simply not true. But the implication of that is, again, in relation to Senator Glenn's question, if this is critical, sensitive information, you do not put it on the Internet using computer systems that are doubly vulnerable. You separate it in some way.

The recommendation that I made, for you to start using laptops and start intranetting them within the Senate, and then thinking about whether you should connect to the Internet or not, would give you a really good opportunity to understand some of these issues, and I think that that issue is something where you certainly do not want your day-to-day messages accessible over the Internet, even through clever penetration attacks. You certainly do not want them out there openly.

On the other hand, C–SPAN covers everything and it is an open book. It might be a good thing at some point to have certain information on-line. I think it is very wonderful for voters to be able to have direct access to what is going on and I certainly applaud that, but that does not have to be the laptops that are on the Senate floor. That is a separate system. You have some controlled paths that you can invoke.

But as soon as you build a connection between the sensitive systems and the web-presence systems, you have again opened up vulnerabilities. You have to remember that a lot of these systems have maintenance paths, dial-up lines. Some of our most critical infrastructures have dial-up lines for the maintenance, and these are huge vulnerabilities.

Senator COLLINS. That brings me to a point that you made in your testimony, where you said that the system is only as secure as its weakest link. As long as we are going to have these kinds of connections and as long as the government is going to rely primarily on off-the-shelf, commercially-available software, are we not going to be vulnerable? Are there not going to be weak links everywhere in the system?

Mr. NEUMANN. Yes. That is a true statement.

Senator COLLINS. Should the government, thus, be developing its own software and no longer relying as heavily on commercial products?

Mr. NEUMANN. That has been tried over the past 30 years or so, until recently, and did not work. That was a massive failure because the government was incapable of procuring the kinds of systems that are needed.

Senator COLLINS. I guess I, like the Chairman and Senator Glenn, are troubled by trying to figure out where we go from here. We have clearly identified a serious problem. Let me ask you one other question. Is the private sector doing a better job with computer security than government agencies?

Mr. NEUMANN. No. They are totally reliant on what is off-the-shelf.

Senator COLLINS. So we cannot look to the private sector for help?

Mr. NEUMANN. There are two organizations, I would say, that are deeply concerned. The banking community is one, first of all, that has permission to use stronger cryptography, for example. They long ago realized that they are very vulnerable, much more so than a lot of other people, and in some sense, money talks. So if you are dealing with a finance-critical application, you tend to do things a little bit better.

Certainly, the finance community can help a little bit by telling you what they have done, and, in fact, I have heard testimony before where they said that they were doing wonderful things and they are perfectly secure. It is clear that they are not at the moment. So even though they are using extraordinary measures to be more secure, they are not secure enough. And as we get into digital commerce where everybody is on the Internet, the ball game has changed rather dramatically.

So I, too, am very concerned that I do not have easy answers, and my closing remark is always—there are no easy answers. This is not a problem that has simple solutions. The solutions are very complex. Anybody who tries to sell you an easy answer is a huckster.

Senator COLLINS. I was struck by the reference in your written testimony, as was the Chairman, to your saying that perhaps it is going to take a Chernobyl-like disaster or a massive coordinated attack on our government's computers before we really take this seriously.

I was struck by the fact that we almost went to war with a Nation because of our concern over biological and chemical weapons and it sounds like we have here essentially the ability of terrorists to engage in a whole different kind of weapon of mass destruction.

Mr. NEUMANN. I think the President's Commission on Critical Infrastructure Protection addressed that issue of terrorism somewhat obliquely. I think this is not an issue one wants to talk about too openly, but it is very clearly a problem.

Senator COLLINS. My final question, and this is a long shot, but would imposing liability on Microsoft or other software manufacturers for security lapses be one way to provide a financial incentive for those companies to start paying attention to this problem?

Mr. NEUMANN. Liability is a real double-edged sword. What happens in a lot of cases is that people refuse to acknowledge that there is a problem, because if they acknowledged there was a problem, they would have to do something about it. As long as the mass norm throughout the community, the best practices, is dumbing down everything, the liability does not work.

I remember asking an under secretary, a colonel, actually, in the Pentagon years ago what he was doing about the security problem. He said, "There is no computer security problem in the Air Force. If I were to admit that there is one, I would be in real trouble. Therefore, there is no problem." I think it is this head-in-the-sand problem that bites us more than anything else.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman THOMPSON. One class action lawsuit could change that kind of thinking.

Mr. NEUMANN. This is true.

Chairman THOMPSON. Senator Lieberman.

Senator LIEBERMAN. Thanks, Mr. Chairman.

If I may, just briefly, share some things that we have learned. I serve also on the Armed Services Committee, and there is a lot of concern in the Pentagon now about what the former Chairman of the Joint Chiefs of Staff, General Shalikashvili, called asymmetrical warfare, which is to say we are clearly the mightiest, the strongest Nation in the world and yet, as this discussion today points out, even the strongest have points of vulnerability. A hostile nation or even a non-national group, terrorist group or even an economic syndicate, perhaps even a very wealthy individual, nonetheless, being much less wealthy and less mighty than we, would look for points of vulnerability and strike those.

Conventionally, we have thought about that in terms of, for instance, denying American aircraft access to forward deployment sites. If you have airplanes that cannot fly from here to there, you have to base them closer to the "there" if you are denied access to the "there" by, for instance, chemical warfare in our time. That is an active asymmetrical warfare.

But there are others. One is related to our growing dependence on space-based assets for communications, navigation, surveillance, etc., targeting, and another is this one that we are talking about today, where you can imagine that because of our enormous dependence on computer systems, both in the direct sense of national security systems being dependent on them, but also all the other aspects of our lives, particularly financial, for instance, that someone with a hostile intent much weaker than we might find this a cheaper way to incapacitate us either totally or temporarily and partially at a moment when they wish to strike something else. This is ominous stuff and it does go not only to questions of privacy but also to the heart of genuine national security concerns.

In that regard, as I have been following your testimony and the questions that my colleagues have asked, I was asking myself at the outset, is this a question of the answers being in reach but the computer industry has not felt a financial incentive, as I thought you were suggesting at the outset, to give us the answers, the solutions, or is it that we really do not have the solutions at hand?

I think, as I have heard your testimony, and I will ask you to respond to this, at one point, you said there is no way of making these computer systems today absolutely secure, and at another point, more recently in response, I believe, to Senator Collins, you said, "There are no easy answers here," which suggests that there may be answers but they are not easy.

Because we are in an age, a remarkable age of technological advance, scientific advance, we do not accept the fact that there may be a problem without a solution. We are just now, in the last few days, hearing unbelievable advances in the pursuit of cures for cancer. So my question is, am I right that we really do not have the answers yet, and then I want to follow up with some questions about what, for instance, the government can do to stimulate and facilitate some of those answers.

Mr. NEUMANN. I have several comments. One is, there are quite a few partial answers today.

Senator LIEBERMAN. Yes.

Mr. NEUMANN. There are quite a few system vendors who are, in fact, very much concerned about security. There are several that are very concerned about networking, for example, and have been for many, many years.

Senator LIEBERMAN. And have products that can deal with the problem?

Mr. NEUMANN. And they have products that can deal with some of the problem. When I say there is no absolute security, I have to realize that, in the first place, there are always trusted insiders who are not trustworthy. This is a serious problem.

Senator LIEBERMAN. Understood.

Mr. NEUMANN. There are also things like the maintenance paths, where you want to be able to remotely maintain your system, and so you have created a trap door, basically, that allows the maintenance folks to get in. In the presence of things like that, there are always vulnerabilities. You have a disgruntled former employee who happens to know the access code, which has not been changed yet, and lo and behold, he is able to get in and bring down the entire network. So in the realistic sense of the fact that all of the systems today do have some vulnerabilities, and some have vastly more than others, it is today impossible to have total security.

Senator LIEBERMAN. I understand that context.

Mr. NEUMANN. In the future, it will also be impossible to have total security. The question is, what is the best you can do?

Senator LIEBERMAN. Yes. So let me ask you, just to pick up on what you have said, what about those vendors who are offering partial security? Why is the government not buying those systems?

Mr. NEUMANN. Well, in some cases, it is. It is deciding that maybe the networking critical stuff or the servers need to be more secure than the simple PC platforms. So you are actually procuring some of those things.

Senator LIEBERMAN. Let me ask a final question, because the time is running out, about what we can do. Understanding for all of the reasons of the concern about internal compromising, which always could be a problem, but in terms of the systems, to try to find systems that can protect us, give us more security, do we need the government, for instance, as we have done in a host of other

areas, to be investing more money in research programs aimed at finding an answer, a better answer to the security problem?

For instance, in environmental protection, the automobile industry will say, "We cannot build a car that will emit less pollution, that will get more miles per gallon," but then we pass a law and, by God, we drive the technology, if you will. In the transportation area, we have NHTSA which sets standards for safety. Do we need to find ways through legislation to drive this system?

Those are my two questions. One is, should we invest more in research, and two, should we be driving technology through law making?

Mr. NEUMANN. The President's Commission recommended a massive increase in the funding of research in information systems security, and that may be too much, but I think, in general, there are selected areas of research that are very much needed.

In terms of what you can do—what was the other part of your question?

Senator LIEBERMAN. The question was really about should we be passing a law that tries to set some industry standards that drive the technology.

Mr. NEUMANN. Right. I would be very cautious in doing that until you have studied it quite carefully. There are a lot of knee-jerk reactions that look good when they are first done and then they turn out to have serious problems. The Communications Decency Act was one that, I think, was not done properly the first time.

In general, I think, yes, that you should look at that very carefully. I think there are possible areas where much more could be done. The National Institute of Standards and Technology, for example, is trying to come up with a new cryptography standard. They have been having difficulties with the National Security Agency for a long time, as you know. I do not need to tell you that. But certainly, standards in secure systems would be very important.

Unfortunately, the standards that we have, the so-called DoD trusted system security evaluation criteria, are not adequate, and those have not been changed in the past 10 or 12 years. They simply have not reflected the networking.

So one of the things that is absolutely essential would be to go back and get the so-called Common Criteria to the point where they actually deal with this problem in a meaningful way. All of the existing criteria do not. They leave out availability. They leave out survivability. They leave out many of the attributes of security and they leave out reliability in a massive way. So the requirements are simply not there.

What the government has done is it said, there is a Defense standard, DoD–5200.28–STD. It is the so-called Orange Book and what government procurements have done is simply said, use the Orange Book. We want a C2 system and we are happy. Unfortunately, a C2 system is not anywhere near adequate. So in answer to your question, yes, very specifically, I think there are some important things that can be done there.

Senator LIEBERMAN. Thanks very much, Dr. Neumann, for very helpful testimony.

Thanks, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

Thank you, Dr. Neumann, as usual, for your help. We look forward to continuing to work with you on some possible answers to these problems.

Mr. NEUMANN. Thank you.

Chairman THOMPSON. We will introduce our second panel, if you gentlemen would come forward. We are joined today by the seven members of the L0pht hacker think tank in Cambridge, Massachusetts.[1] Due to the sensitivity of the work done at the L0pht, they will be using their hacker names of Mudge, Weld Pond, Brian Oblivion, Kingpin, Space Rogue, John Tan, and Stefan Von Neumann.

Senator LIEBERMAN. I thought you were the kingpin, Mr. Chairman. [Laughter.]

Chairman THOMPSON. I hope my grandkids do not ask me who my witnesses were today and I reply, Space Rogue. [Laughter.]

But we do understand your need to do that and we appreciate your being with us. May I ask your name?

Mr. MUDGE. I am Mudge.

Chairman THOMPSON. You are Mudge. Mudge, would you like to make a statement?

TESTIMONY OF MUDGE, L0PHT HEAVY INDUSTRIES

Mr. MUDGE. Yes, I would. Thank you very much for having us here. We think this is, hopefully, a very great step forward and are thrilled that the government in general is starting to approach the hacker community. We think it is a tremendous asset that the hackers actually bring to the table here in an understanding.

My handle is Mudge. I and the six individuals seated before you, which we will run down the line, Brian Oblivion, this is John Tan, Kingpin, Weld Pond, Space Rogue, and Stefan Von Neumann, make up the hacker group known as the L0pht. For the past 4 years, the seven of us have been touted as just about everything from the hacker conglomerate to the hacker think tank, the hangout place for the top U.S. hackers, network security experts, and a consumer watch group. In reality, all we really are is just curious.

For well over the past decade, the seven of us have independently learned and worked in the fields of satellite communications, cryptography, operating systems design and implementation, computer and network security, electronics, and telecommunications. Throughout our learning process, we have made a few waves with some large companies, such as Microsoft, IBM, Novell, and Sun Microsystems. At the same time, the top hackers and the top legitimate cryptographers and computer security professionals pay us visits when they are in town just to see what we are currently working on. So we kind of figure we must be doing something right.

I would like to take this opportunity to let the various members talk about a few of their previous projects, their current projects, and what they are going to be working on in the future.

[1] The prepared statement of L0pht Heavy Industries appears in the Appendix on page 71.

Chairman THOMPSON. You have heard the testimony this morning.

Mr. MUDGE. Yes.

Chairman THOMPSON. If there are any points in the process that you want to make, fairly briefly, with regard to some of the previous questions or testimony, you can feel free to do that also.

Mr. MUDGE. We definitely will.

TESTIMONY OF WELD POND, L0PHT HEAVY INDUSTRIES

Mr. POND. Good morning. My name is Weld Pond. I am a hacker and programmer with over 10 years' experience working as a software developer in the commercial software industry. My college training is as a computer engineer. At the L0pht, I specialize in writing software programs for exploring computer network security and operating systems security.

My current projects include finding vulnerabilities in Microsoft Windows NT security. I am actively working on L0pht Crack, a program that we created to exploit the weaknesses in Windows NT's password security, which uses cryptography to secure the passwords, but we have found vulnerabilities in their implementation.

This program has been extremely well received by military, government, and corporate security groups who use it to test their own passwords for weaknesses. Prior to the release of this program, security experts claimed it would take thousands of years to uncover a Windows NT password, and our program can do it in days and, in some cases, hours.

As a licensed amateur radio operator, I also enjoy radio communications. A future project plan is collaborating with the L0pht hardware people to create secure public wireless networks, something that we are very interested in.

TESTIMONY OF KINGPIN, L0PHT HEAVY SECURITIES

Mr. KINGPIN. Good morning. My name is Kingpin. I am the youngest member of the L0pht and one of the electrical engineers and hardware hackers. While some of the L0pht members concentrate on software programming, I work with hardware design and implementation of electronic circuits. My interests include embedded system design, surveillance and countersurveillance tools, and wireless data transmissions.

My current research project involves experimentation with the monitoring and eavesdropping of stray electromagnetic fields from computer terminals, otherwise known as "Tempest Monitoring." Using low-cost electronic equipment, one can capture the contents of computer screens from more than 200 meters away, possibly gaining passwords and other sensitive information.

The phenomenon of Tempest Monitoring has been known to the industry for decades, but there is not much unclassified information available on how to both capture the emissions and also protect oneself from becoming an eavesdropping victim. My research will not only help me learn about the monitoring technology, it will enable me to educate others to help them protect their computer systems from prying eyes.

TESTIMONY OF JOHN TAN, L0PHT HEAVY INDUSTRIES

Mr. TAN. My name is John Tan. At 28, I have been involved with computers, telecommunications, and security for 14 years now, the last 8 years of which have been spent in the financial services industry. My involvement with the L0pht has primarily been nondescript, but I have achieved some notoriety in terms of documentation of some existing problems with Novell Netware and a compilation of a newly created home pilot document library. Recently, I have consulted for various manufacturing, financial services, and management consulting firms regarding information security policy and how to establish a corporate security effort.

I will continue in the future to pursue an understanding of the risks of the information age and communicate those findings to the government, industry, and the media to provide a clear, consistent message of where we are and where we need to go.

TESTIMONY OF SPACE ROGUE, L0PHT HEAVY INDUSTRIES

Mr. SPACE ROGUE. Good morning. I am Space Rogue. Although my background contains no formal computer training, I have amassed a great deal of knowledge in computer security and the use of technology applications in the area of physical security. Currently, I am working on assessing the vulnerabilities in various proximity detection devices, such as those used by Easy Pass, Mobil Speed Pass, and controlled access cards. In conjunction with Stefan Von Neumann, seated here today, and others in the hacking community, I am actively seeking vulnerabilities in Apple Share IP by Apple Computer.

I wish to take this opportunity to thank the Members of this Committee for inviting us here today.

TESTIMONY OF BRIAN OBLIVION, L0PHT HEAVY INDUSTRIES

Mr. OBLIVION. Good morning. My pen name is Brian Oblivion. My focus currently is microprocessor system design, telecommunications equipment, wireless communications architecture, and systems administration. Over the past few years, I have conducted research on the cellular networks, exploring the unencrypted data channels and their protocols and explore the easily bypassed hardware-based non-cryptographic authentication used to track call expenses.

Recently, I am researching virus digital coding methodologies involving both dedicated hardware and software analysis via digital signal processing. This will result in the exposing of claimed secure wireless messaging in communications systems and, thus, increasing the requirement of a more secure communications infrastructure.

As an amateur radio operator, I am exploring authentication methods for amateur radio data networks. Technology developed in this arena will be applied to commercial wireless networking products, protocols, and equipment that will utilize not only authentication but encryption of the radio channel, as well.

The L0pht for me provides a much needed avenue for the dissemination of the present state of insecurity among various consumer networks and products. If it was not for groups such as ours and other motivated individuals in the security community, the

state of awareness we have today would be years behind. Thank you.

TESTIMONY OF STEFAN VON NEUMANN, L0PHT HEAVY INDUSTRIES

Mr. VON NEUMANN. My name is Stefan Von Neumann. I have been working with L0pht since 1993, focusing primarily on high-power electronics, flaws in data networks, and the increasing convergence of power distribution and data distribution. My professional background includes supporting users on common computing products and networks, which gives me first-hand experience with how relatively unaware of computing risks most users are. Even worse, software publishers, Internet providers, and utility companies are tight-lipped about flaws or risks inherent in products and services that touch the daily lives of most Americans.

For example, in many areas of the country, including the Boston area, electric utility companies are using radio transmissions and/or power lines to transmit data, meter data, from customer locations. These same utility companies are also using such data transmissions for controlling their power systems. Even public water companies are using radio transmissions for controlling their water systems.

In the same way that the so-called phantom controller was able to impersonate an airport control tower and issue instructions to a pilot, one could impersonate a legitimate utility company and disrupt water or electric service.

Another example is Internet data sent over cable television systems. Most customers of these services are not aware of the potential for another user to watch their "private" communications across the cable TV network, and worse, the users are not aware of the possibility that an improperly configured computer could make available their data without their knowledge.

I would personally like to see that the same type of independent review process that should exist for software companies extended to utility companies and Internet service providers. Finally, customers and end users should be made aware of the risks.

Thank you for having us here.

Mr. MUDGE. I am one of the network system and cryptography wizards at the L0pht. Basically, I am the person who breaks into the systems and undermines the network security, and that is what I do in my day job. Companies like that.

Some of my previous projects were L0pht Crack, along with Weld Pond, in which we developed the tool for showing administrators and users the insecurities in Microsoft's passwords. I have released several security advisories on various pieces of commercial software which have prompted vendor patches, which means they improved the software after we pointed it out to them. Unfortunately, many times, they would not improve the software until we actually went public with the findings. Companies do, indeed, want to ignore problems as long as possible. It is cheaper for them.

Recently, I conducted training courses at NASA's Net Propulsion Lab to try and raise their level of awareness as to the vulnerabilities, especially with the name brand recognition. In the very near future, I will be conducting training courses over at the NSA.

Shortly after that, the L0pht will be releasing a white paper on new cryptographic weaknesses that I, along with one of the top U.S. cryptographers, have found in a very prominent commercial operating system, to remain nameless.

If you are looking for computer security, then the Internet is not the place to be. If you think that you are an exception to the norm and that you have a secure setup that communicates over the Internet, you are probably mistaken. Furthermore, if you feel that the government is giving you access to the enabling technology you need to combat this problem, you are wrong yet again.

The foundation of the Internet is over 20 years old at this point. While the technology still works, it is being asked to perform tasks that it was never intended to via secure fashions, nonetheless. How can one be expected to protect a system on a network where any of the seven individuals seated before you can tear down the foundation that the network was built upon, let alone the systems that are sitting on top of it? So even if computer systems and other peripherals on the network were secure, the problem is still moot.

Can the systems be secured? In many cases, they actually can be. For instance, the problem with the phantom air traffic controllers could be remedied by incorporating relatively trivial and inexpensive cryptographically secure authentication. The same would hold true for MDC4800, which is the protocol most commonly used by mobile police data terminals to remotely pull and update records. Personal paging protocols, everybody has a little personal pager nowadays such as POCSAG, FLEX, and GOLAY, which the White House Communications Agency uses to coordinate movements of the President, would also benefit from this relatively trivial modification.

Why do not strong authentication properties exist in these protocols? Most likely the same reason that simple security mechanisms are missing from all of the software, or almost all of the software sold to corporations and agencies today. It is cheaper and it is easier for companies to sell insecure software. There is no liability attached to the manufacturers and there is no policing done to stop companies from selling insecure software under the guise of secure.

In an industry where time to market matters, who wants or cares to add security or even thoroughly test their product? You should. You, the government and consumer, should care and want software products to include security and authentication mechanisms, and I think you do. You should encourage the companies to include this in their products and hold them liable when their products fail.

There are parts of the situation that the government can directly help. Lifting the constraints on cryptographic export would encourage companies to more readily include authentication encryption in their products. The Cellular Telecommunications Protection Act is an example of legislation that is in place right now that hinders consumer watch groups, such as ourselves, thus perpetuating the insecurity status quo that is out there.

In conclusion, hopefully, your having us here is not a fluke and, hopefully, we have not offended in any way, but this might be the beginning of an ongoing dialogue between the government and hacker groups such as ourselves. Perhaps the information from

such meetings will end up becoming an enabling mechanism for future change that will help organizations of all sizes, not just large government organizations.

We encourage you to read the written testimony and we are more than happy to answer any questions in as much detail or technical detail or non-technical detail as you see fit and expound or clarify upon any concerns. Thank you very much.

Chairman THOMPSON. Thank you very much. You have not offended any of us, just the contrary. I think it is probably appropriate that gentlemen such as yourselves are the ones who come forward and demonstrate that the emperor has no clothes. So we appreciate your coming here, especially in light of the fact that the *Washington Post* described you as rock stars of the computer hacking elite. So we appreciate your being with us here today.

I am informed that you think that within 30 minutes, the seven of you could make the Internet unusable for the entire Nation, is that correct?

Mr. MUDGE. That is correct. Actually, one of us with just a few packets. We have told a few agencies about this. It is kind of funny, because we think this is something that the various government agencies should be actively going after. We know the Department of Defense just did a very large investigation into what is known as denial of service attacks against the infrastructure. In our various day jobs, we contributed a large portion of the information to that actual investigation. Much to our chagrin, the learnings from it were instantly classified, which we were giving them largely public information.

It is very trivial with the old protocols to segregate and separate the different major long haul providers, which would then be the national access points, the metropolitan area ether sections. AT&T cannot talk to MCI, cannot talk to PSINet, cannot talk to AlterNet, etc., and keep it down that way as long as we really wanted to. It would definitely take a few days for people to figure out what was going on.

Chairman THOMPSON. You state that with regard to commerce over the Internet, which is rapidly growing, as we all know, that the Internet was not designed for it. What do you mean by that?

Mr. MUDGE. The Internet was designed out of the Defense Department's Advanced Research Project Agency to simply have computers talk to each other. This was a very laudable act and a laudable goal and I think they succeeded fantastically. This was largely an academic environment with some government research organizations. It grew up, it flourished, it struck everybody by surprise, and now big business is saying, well, let us jump on board and make some money off of this.

This is kind of like, if you have driven in Boston, the streets are not tremendously designed in a wonderful fashion because they followed the cows around and laid the pavement down. You can get it to work, but it can be really painful, and that is the stage we are in right now.

Chairman THOMPSON. You say that you have been working with some governmental agencies with regard to some of these problems and, of course, with commercial entities. What occurs to me in listening to you and listening to our prior witness is that there does

not seem to be an inducement for industry to do much about this at this stage of the game. That is what you are saying, essentially, is it not?

Mr. MUDGE. Yes.

Chairman THOMPSON. I hope that there are some more forward-looking people in some of these industries than we have had in times past. You can look at the automobile industry or the tobacco industry or any number of industries whose chief executives have kept their heads in the sand about problems on the horizon. As much as we dislike lawsuits and there are too many of them in this country, this is clearly going to be something that is going to hit somebody big time before very long. Hopefully, it will not take an economic disaster to cause that.

But you can see it on the horizon, can you not? They are going to have to come to terms with the fact that their ability to do something about this is out there, and they are turning their back on a way to make their systems more secure. They are not doing it and they are going to clearly have to answer to that.

You say that the Internet and computer security is almost nonexistent. Could you elaborate on that a bit? Do you mean literally?

Mr. MUDGE. There are many aspects that make that up. The operating systems, as we just heard testimony from Dr. Neumann, very correctly, are not incorporating any sort of real security mechanisms. There is a lack of education. There is a lack of understanding as to what the problems are out there. There are no mechanisms for places to keep abreast of current findings. I mean, the security realm, and network security in particular, is very rapidly changing, so it is kind of difficult.

What was the analogy with the cars that somebody gave, about the recall? They send you a letter if your Ford Explorer is going to have a very serious problem. The number of operating systems out there, they are not sending people letters. They are saying, you have to do your own due diligence and come to us and find out what we have made publicly available or what we have decided to alert you to. At the same time, keep in mind that if we do not alert you to it, we save a lot of money and we save our top engineers' time by not having to throw them at the products where they can add new bells and whistles into whatever.

Mr. SPACE ROGUE. Mudge, the analogy was that the Volkswagen Beetle that just got recalled, evidently, they found three cars that had a problem, three, and they did not cause any serious deaths or injuries but they just found three potential problems in the vehicle. They sent out 8,500 letters to every purchaser of the vehicle in the United States.

If there is a software company that has three hack attempts against it, or three successful hack attempts against it, a particular piece of software or an operating system, they are not going to go call every single one of their people that just spent a lot of money buying their software and tell them, hey, there is a problem. We need to call back our software so we can fix it. Right now, that does not happen.

Mr. POND. Some of the problems that are found are reported to the manufacturers and they do not even make a fix publicly available. They work on a fix internally, and if you have the same prob-

lem and you come to them and you say, "I am getting broken into. Someone is attacking my system in this way." They will say, "OK. Well, we have this behind-the-scenes fix that you can apply to your system, but we have not even made it publicly available yet."

Until the problem mushrooms up and enough people complain about it, then they will come out with a public fix. But if it is behind the scenes, people just contacting the manufacturer, we have seen that they do not really come public and even tell the other users of their system that this problem exists and here is the fix for it.

Mr. OBLIVION. I would like to add one more thing.

Mr. MUDGE. One thing real quickly. This is one of the main problems with the Computer Emergency Response Team.

Mr. OBLIVION. Right. There is also a lot of finger-pointing in the industry, where systems administrators claim that the software provided to them is not shipped in a secure manner. The industry says that they should not be responsible for that, and I am not quite sure, because I am not a lawyer or even nearly skilled in political matters, but I do not know if there is any legislation that could fix the liability problem, but I know that is one of the issues.

Mr. KINGPIN. I just want to add one thing to that. In the point of liability, the car manufacturers will be and are held liable if something goes wrong in their product. If something is wrong in 1 of the 10,000 cars and it explodes, they will be held liable. If something breaks in the software, the companies are not held liable and they think: "Why do we have to tell people about this?" They are not responsible.

Mr. POND. Just another sort of liability analogy which we have found which sort of makes sense is Kryptonite makes bicycle locks. They say, our lock is so good, if your bike is stolen—it is a $30 to $40 lock—if your bike is stolen, we will pay up to $1,000 to replace your bicycle. So, basically, they are saying, our security works and we will stand behind it.

Software vendors do not stand behind their security. They say, well, if it is broken and there are enough problems, maybe we will fix it. But if you lose thousands of dollars, say you have an e-commerce site up on the Internet and your whole business is built around their software which they have told you is secure, they have told you, "Oh, we have added all these great features and you can run your business on our software," and then your business fails because they caused your business to fail, essentially--if it is e-commerce, if your site is down, you are not making money—they say, sorry.

Mr. MUDGE. One of the things about the Kryptonite locks is they are not unbreakable and they are not unpickable and the company knows that, but they have raised the bar. They have raised it enough that the ankle-biters, the novices will go to the next bike that is unlocked. The same thing with car alarms. You get a discount on your insurance for performing due diligence. You just raise the bar and you get away from the noise level.

Chairman THOMPSON. Thank you very much.

I have one more question. I know the other Members have questions. Part of what you are trying to do is demonstrate something that you feel like the American people need to know, and that is

part of our job, also. I am curious, if a foreign government was able to assemble a group of gentlemen such as yourselves and paid them large amounts of money and got them in here or hired them to wreak as much havoc on this government, how much damage could they do?

Mr. SPACE ROGUE. We would be in trouble.

Chairman THOMPSON. Just give me some idea of what we are talking about.

Mr. MUDGE. We had some of your aides up to talk to us and check us out at the beginning and I think they were relatively impressed with what we have managed to put together without any funding whatsoever. Brian, do you want to talk about some of the satellite communications, or let alone just taking us down from the financial aspect. There are so many different ways that——

Chairman THOMPSON. Well, each of you that have a comment on that, just relate it, please.

Mr. MUDGE. We can run down the line.

Mr. OBLIVION. OK. Regarding satellite communications, you could—if you were highly paid enough, you could assemble jamming gear to temporarily knock out uplinks. You could take an area, I am sure you are aware of, like, the HERF guns and the EMP blasts and typical informational warfare. It is more on the physical level rather than just the information security, where you would be able to disable equipment by generating a high-energy pulse, disabling the clock which controls everything in the computer system.

Chairman THOMPSON. What would that do? What would be the effect of that?

Mr. OBLIVION. Well, it depends on the equipment. You could do it to a telephone switch. Generally, national access points for the Internet are in unshielded buildings. Sometimes they are in just regular commercial buildings without any type of——

Chairman THOMPSON. But what would be the effect of that? How would we feel that?

Mr. OBLIVION. You would feel that by an instant disruption of Internet service on that point.

Chairman THOMPSON. All right. What is another area?

Mr. MUDGE. We will let Kingpin talk about Tempest. Some of the areas you should worry about are your phone systems are down, your electricity is gone in——

Mr. TAN. Financial markets.

Mr. MUDGE [continuing]. Financial markets. We recently had a very close call in the financial markets. Disruption of service is a wonderful way of messing people up. In addition, by disrupting service in certain patterns, you can force people to take other routes.

Let us say that I have taken over MCI's networks, which would not be a tremendously difficult thing to do. Most people can get access to the metropolitan area ethers and the national access points, physical access, even. So I can watch everything that goes through this major backbone provider's transitory networks, but I cannot watch Sprint. Well, what am I going to do? I will disrupt Sprint's service so that everybody routes through me. Now I can learn everything you are doing. I can watch your movements. I can stop

your movements. I can issue requests on your behalf. You would be surprised how much stuff is tied into the general networks now.

Mr. SPACE ROGUE. I think if a nation state funded a group of people to attack the United States electronically, the number of systems that can be disrupted or compromised is so great that it would probably wreak a lot of havoc in the country. Whether or not the country can recover from that in an adequate period of time or defend against it is a good question. But there is definitely some potential there for abuse.

Mr. KINGPIN. Also, as I mentioned in my initial statement about Tempest Monitoring, which will allow outsiders or insiders to receive emissions from computer terminals, one can see the screens of other people's computers. They can read the E-mail from the screen or if a user is accessing some confidential systems or looking up some kind of criminal records, the outsider or intruder could then become familiar with the system and access it in a different way.

Mr. MUDGE. What would you do with the mobile data terminal?

Mr. KINGPIN. With the mobile data terminal, the same type of thing can happen. You can either intercept the data via wireless transmissions or you can monitor the terminals with Tempest technology, and by just monitoring the transmissions, you can view what the police are transmitting and receiving about criminals or internal government agencies or something.

Chairman THOMPSON. All right. Thank you very much.

Senator Glenn.

Senator GLENN. Thank you, Mr. Chairman.

I know you have fictitious names here, but I think I had the pleasure of talking to a couple of you gentlemen some 3 or 4 years ago in a different venue. That was a fascinating conversation and this is fascinating this morning.

I am not quite clear. Does the L0pht do this on a business basis now, too, or are you just amateurs that get together and do this because, as it says in your testimony here, you are having fun, pushing the envelope, examining security systems, providing full disclosure to all those in the security industry of your findings. Is it strictly an amateur group, or are you available for hire from people that wanted to avail themselves of your expertise?

Mr. MUDGE. We have been a strictly voluntary group for some time. This is a very monetarily taxing for us, so——

Senator GLENN. So you all have day jobs, I guess in addition to this?

Mr. MUDGE. We all have day jobs and this all comes out of our own pockets for all the equipment that we try and salvage together and the different projects we want to learn about. We do, when the purse strings become very tight, go out and take consulting jobs or do different consulting work. We would be more than happy to come help people out. Unfortunately, a lot of people are scared to come talk to us. We end up beating people over the head publicly in order to get them to even fix their problems, which does not endear us with them tremendously. [Laughter.]

Senator GLENN. Let me expand the area of vulnerability just a little bit here and get your comments on this. Can you get into the command structure or the command signals that go up to position

communications satellites? Could you relocate them and then foul up the whole system, not by destroying them or not by fouling up the computers necessarily but take them out of their positions?

Mr. OBLIVION. Well, actually, companies like COMSAT and other telemetry command and control systems are using authentication for their command structure, which is what we would recommend to other areas of wireless telemetry and control. That would increase the bar of the state of security of radio-controlled telemetry systems.

Senator GLENN. How about our GPS system? Is it vulnerable, also? That is the Global Positioning System. We are going to be relying a lot more on that. We are relying on that for some of our weapons systems. It used to be highly classified. Now, there has been a lot of writing about it. We are using that to a tremendously increased degree these days for our military and for commercial aviation and everything else. I have a little Magellan handheld I use in my little airplane flying back and forth and it is great.

Mr. SPACE ROGUE. One of the problems with GPS is it is a very weak signal. It is very easy to jam that signal. As a matter of fact, there was an incident a few months ago in upstate New York where a test was being conducted by the Air Force. The test, unbeknownst to the Air Force personnel, was interfering with the GPS signals to aircraft landing in New Jersey. Luckily, it was during the day time and the aircraft was trying to rely on the GPS signals to land, but they lost their GPS, so they went on manual and landed that way.

Senator GLENN. If somebody wanted to, though, could they get into the GPS system and actually relocate some of those satellites slightly, which would throw it off and screw up all the information that you are getting? Is that possible?

Mr. OBLIVION. Traditionally, the military has been very good about authentication methods on telemetry and command and control systems. I think you would be more worried about setting up a 1.X gigahertz jammer rather than somebody actually moving satellites around or colliding them.

Mr. MUDGE. The end result would be the same, though.

Senator GLENN. It would be easier to jam it than relocate it because of a weak signal.

Mr. OBLIVION. Or it could be hidden in——

Mr. NEUMANN. I have one comment here. On August 21, I believe, of 1999, a lot of the receivers will fail. They have a year 2000 type problem, where they run out of bits and it resets to January 1980. I just thought I would toss that one in.

Senator GLENN. You mean do not be flying that day if I want to get where I am supposed to be going, is what you are telling me. I will check that one out.

Could you get in and transfer Federal Reserve funds to someplace?

Mr. MUDGE. Just about everything is possible. It depends on how much money you want to throw at it, time, and effort. From the amount of time and effort and the money, which is nonexistent for us, and the fact that we like not being in jail, we would say, no, we would not do that. If we really wanted to and really had to, yes,

because if you make it easy enough for yourself or somebody else to use it, you make it vulnerable.

Senator GLENN. I look at you guys as the white hats in this whole thing.

Mr. MUDGE. Thank you.

Senator GLENN. I think your motivation, as far as I know, is excellent, and I think you want to be considered that way, but let us say we have a bunch of bad guys now. Can you, with your expertise, track back and find out who the bad guys are if they are trying to foul up GPS or the Federal Reserve or something else? Can you track that back and locate the people that are not of good will?

Mr. MUDGE. Backtracking and reverse hacking is a relatively tricky area. Based upon the relatively antiquated protocols that you are dealing with, there is not a tremendous amount of information as to where things came from, just that they came. It is kind of like giving a confessional to a priest. You have this big blind in between you and you are just hoping and trusting that the person is actually there listening to you and that they can do anything about it. [Laughter.]

Mr. SPACE ROGUE. It is like getting a letter with no return address and nothing inside. You received something, but there is no way to know where it came from.

Senator GLENN. OK. That is what I was afraid of.

Mr. Neumann is still here, and I think his answer when I asked him whether a secure system that could not be hacked into is possible, and I believe his answer was he did not think so. Do you gentlemen agree with that? Do you think there is a system that can be designed that would be foolproof that we could use for defense and for key elements, such as the Northeast grid, or financial systems, the Federal Reserve or whatever? Is it possible to design a foolproof system?

Mr. SPACE ROGUE. I do not think it is possible to design a foolproof system, but I do not think that should be the goal. The goal should be to make it very difficult to get in. The more difficult you make it, the less risk that you assume from a foreign nation state or a teenage kid from breaking into that system. So the goal is to raise the bar and then have a plan to reconstitute after the fact if it does happen.

Senator GLENN. Mr. Von Neumann, I think you are in power distribution, can you, in effect, blow a computer? Can you overpower it? Can you put enough material in that you just blow it? You do not need to worry about getting the material off or fouling it up. You can just put it in and blow the computer. Can you do that?

Mr. VON NEUMANN. It is not so much an issue of blowing a computer, destroying it over a power line. There is HERF, high-energy radio frequency. There is EMT (Electro-Magnetic Pulse). They can do that from means other than over a power line. Maybe more of a concern would be interruption of power. We were, in the course of one of our investigations, able to use a power interruption that was nothing to do with us, it happened to be a coincidental power interruption, but to our benefit, that power interruption that was deliberate.

Senator GLENN. I was not thinking so much of overpowering with so many high power electric currents coming in. I was thinking of

getting in and fouling up circuits in such a way that it will dump its programming. Can you do that?

Mr. VON NEUMANN. Yes. Mudge, do you care to talk about buffer overflow?

Mr. MUDGE. I think what maybe they are talking a bit more about is bit shifting, and there has been a tremendous amount of improvement in actual analysis of cryptographic protocols by bombarding with x-rays to actually flip bits inside. The trick is to be able to control this little black box and watch the information you are sending in and the information that you are getting out from it as you change its innards, even if you do not necessarily know what you are changing precisely.

Buffer overflows are a extremely common coding problem. Many of the problems that are out there that contribute to this lack of security are extremely simple. Buffer overflows are spottable in source code by a first-year college computer programmer, by people without any college computer programming skills. The notion of race conditions, where there is a certain amount of time between what I tell you something and between what you tell another Senator, that I could go in and change that information so that Senator Lieberman believes that you said something else, these are all very straightforward problems. They were not addressed because computers really came out of a tremendous amount of fun and joy and research and exploration. They did not think about the commercial ramifications and aspects. I probably did not answer the question at all there. [Laughter.]

Senator LIEBERMAN. But it was a fascinating answer. [Laughter.]

Senator GLENN. You may want to run for public office 1 day. [Laughter.]

We alluded to this a while ago when Mr. Neumann was here, about whether it would be possible to set up a whole different system for defense, for intelligence matters, for CIA, for NSA, for people doing very highly classified work that we do not want out. Would there be an advantage to us funding and setting up a whole separate system, and how long would it be invulnerable if we did such a thing? Is it worth the effort? It would be very expensive to do it. Would it be worth doing?

Mr. MUDGE. One of the things that was said earlier was there are no easy answers, maybe not any answers at all, but what I believe is that there are answers. They are just quite painful.

Yes, I think that is one of the ways to do it. Several of the agencies within the government currently do that. It is very expensive. If you have extremely sensitive information, you do not trust it with other networks that are less sensitive, that are less trusted. The actual computer systems can be made to be relatively secure, the physical hardware in it. It becomes very costly. It is a cost-benefit analysis that you end up doing here.

The software can be improved upon. The software does not have to be fantastic. One of the things that strikes me is there is a tremendous amount of interest in the year 2000 problem. Every time I hear it, I have to sit back and I chuckle to myself because we are worried about the year 2000 when these systems crash, but they are crashing left and right right now and nobody cares.

The systems, you can work with them right now. They do crash. I mean, how many times has anybody in here run Windows and had to reboot it, or Macintosh? I mean, left and right. They still work. If you put them in a secluded room, put a guy with a gun next to it, and do not let it talk to other systems, it is relatively secure.

Senator GLENN. I am not quite sure what we do if we require the computer industry, though, to do something. You say there are no incentives for industry to do much. I think of it as some people may want to buy the equivalent of a Model–T Ford or a tiny car. Other people want to buy more security and so they buy a great big car, or a lot of people are going to vans now because they are bigger and heavier and show less fatalities in an accident. You are going to have different levels of what people want.

How would you go about this in the computer industry? What would you require them to do that would make this program better. Or would it just be making government agencies and people know that if they are going to go to certain types of information that they have to buy a computer that is upgraded to a certain level, and we should be much more cognizant of these security levels when you purchase a computer than ever before. That is sort of a convoluted statement, but you know what I am driving at. How do we regulate this? I am not sure we could.

Mr. POND. Well, actually, in the industry now, Microsoft sort of does the Model–T and another car example. They have Windows, which is sort of the Model–T. That is for your individual user at home. Then they have Windows NT, which is a more secure system. The problem is it is just more secure. It does not mean it is really good enough for doing what you would say is a secure system that is good enough.

The problem is, we get back to they have no liability and they just say, "It does not work. Sorry. We will fix it in the next release." They do not have any way of telling you, the customer, or no one really does that I know of, what they did to make the system secure. You cannot say, show me your security architecture. Show me your development process that went through and looked for the problems and show me that the system is secure. No one is doing that. No one is really selling a commercial product that does that, can assure you, the buyer, that you are buying the Cadillac with the bulletproof glass. So no one is really selling that and no one is really assuring anyone that that is true.

Mr. SPACE ROGUE. It comes down to Microsoft just saying, "Trust us," and there is really no way to test the product to find out if, in fact, it is secure, at least by the end user or the consumer. So unlike the Cadillac with the bulletproof glass, you can go up and you can look at the glass and see how thick it is. You cannot do that with software.

Senator GLENN. I am sure my time is more than up. We do not have lights here, but I have just one more question. Maybe this overstates it, but it seems to me that maybe all of our concern about whether people get in and have access or can manipulate a system where it transfers something to another spot or something, is not our biggest danger. Maybe it is Stefan's idea that if you really want to do harm to our country, you just get in and, in effect,

blow the computer or do the transfers, as you said, by x-ray or whatever it is and you have fouled up the whole thing irretrievably, rather than going in and trying to manipulate a system.

Should our biggest worry be in this area? It would seem to me that that might be something that would be easier to protect against than all this getting in and fouling up somebody's specific software program. Am I overly optimistic?

Mr. VON NEUMANN. It is much simpler for someone to perform a denial of service than it is to change the data and insert their own or to manipulate.

Senator GLENN. It would not be surreptitious. You would know it when it happened, that is for sure.

Mr. VON NEUMANN. Yes, exactly. It is much less expensive to do that kind of damage and much simpler. Easier to prevent against, perhaps, and perhaps more straightforward in the short term to harden the major network access points to the extent of a military facility, making more tempest-proof facilities.

Senator GLENN. Or x-ray-proof shielding, something like that.

Mr. VON NEUMANN. Yes. That may be simpler in the short term.

Mr. KINGPIN. There is documentation on that and it is possible to shut down machines with the high-energy RF. Protecting against it has been done. It is done and it is fairly simple. You can basically enclose something in a giant metal box, which will prevent the outside RF. I do not know if that is done a lot inside the government agencies. Some of the military computers need to be Tempest-proof,.

Senator GLENN. Yes. Brian, you were going to say something.

Mr. OBLIVION. I think I was just going to say that the box needs to be grounded.

Senator GLENN. All right.

Mr. TAN. If I may, one of the things I think is coming out here has got to do with it is not just the encryption, the strong encryption. It is not just the network or the operating system. It is all these things that have to be applied across the board in order for one person to actually have enough responsibility to be able to tackle the problem themselves. They have to be in an environment where there are others, not only in their own industry but in other industries that are trying to raise that bar, so as a whole, the security goes up.

Senator GLENN. My time is up. Thank you, Mr. Chairman.

Chairman THOMPSON. Senator Lieberman.

Senator LIEBERMAN. Thanks, Mr. Chairman.

Thanks to all of you. Senator Thompson indicated that somebody had referred to you as rock stars of the new computer age. It is probably not what you came to hear, but actually, I think you are performing an act of very good citizenship and I appreciate it. I hope you do not mind that I am not going to call you rock stars. I would compare you more to Rachel Carson, who sounded some early warnings about what environmental pollution was doing to the environment, and in the defense context, you may be modern day Paul Reveres, except in this case, it is not the British coming. We do not know who is coming. That is the problem.

Mr. MUDGE. Right. You have got it. [Laughter.]

Chairman THOMPSON. We have met the enemy and the enemy is ourselves.

Senator LIEBERMAN. Yes. The Chairman's question before was chilling. You are obviously very bright and very creative and work at this, but if there is anything we have learned in the modern age is that you cannot, particularly in this age, particularly because of computers, where knowledge and information travel so quickly, just as you have been able to do this at L0pht, there are people all around the world who are able to do this and they may not be good citizens. They may be up for hire to people who do not wish us well.

I appreciate what you are doing, and I must say in this regard that it may be that the appropriate metaphor here is not Chernobyl but, unfortunately, Oklahoma City, where if we looked at it, we would have understood, and some did, that there was real vulnerability, but we did not do anything about it. I think that is what you are telling us, and I hope we can continue to work with you to try to raise our guard.

I think the other thing you have helped me to understand is that there is no such thing as absolute security. No system is foolproof. I think what you said is that the aim here should be to make it more difficult to break a system, to infiltrate it. Of course, there never has been absolute security. I suppose it is just that the consequences of insecurity in an age in which we are all so reliant on computers are more consequential. They are more massive. They are more widespread.

Let me ask you a couple of questions following up on that theme of accepting that there is no system that is foolproof. You have said here in your testimony that given 30 minutes, you might be able to render the Internet unusable, not forever, obviously, but for some period of time. What can we do? What can the system do? What can the government do? What can private folks do to try to protect against that?

Mr. MUDGE. The one method of doing that that we were referencing there, there are several, there are dozens of them, actually, but this is a good example. You can prevent and you can stop that particular attack from happening. However, the nature of the Internet and the companies that are providing the long haul backbone connections of it is to move the information as quickly as possible across it, because that is money. Every packet, and millions of packets go by a second, is worth a little bit of money. If you even stop to look at the packets, you have to send slightly less than your maximum capacity might be, in which case your competitor now has an edge on you because they can offer faster, more efficient service.

So in order to protect yourself, you very slightly, 1 millisecond per packet, degrade service, but that definitely cascades into a noticeable financial hit, which the companies are not willing to take, so they remain vulnerable.

Senator LIEBERMAN. Let me just compare things and go to you, Stefan Von Neumann, because you talked about your work in utility systems. Let me ask you just to compare. For instance, today, leaving aside what we have talked about, or let us say 10 or 15 years ago, somebody who wanted to do damage to a utility system

could cut wires. They could, if they were more aggressive, blow up a power station, a substation. So compare the effects of something more primitive like that from somebody with hostile intent to the possibilities that you envision in the new world.

Mr. VON NEUMANN. It could be more well timed or more specific of an impact. Where the detonation of an explosive near a substation could take down an entire grid, with specific computer control of an area, you might be able to interrupt only one customer's service. Say if there was a commercial entity that was a target, that one commercial entity or that one government building could become denied of electric service or water service or whatever the utility service was that was going to benefit the attacker.

Senator LIEBERMAN. Computer service.

Mr. VON NEUMANN. Yes, exactly. So in the past, where it simply was a destruction, it might not have had the specific focus on the attack point, where now it allows that.

Mr. SPACE ROGUE. I think another issue is if somebody goes out and cuts a line, there is a plan in place. You send out a repairman, he fixes the line, and you are all set.

Senator LIEBERMAN. Right.

Mr. SPACE ROGUE. You blow up the building, they rebuild it.

Senator LIEBERMAN. Right.

Mr. SPACE ROGUE. Attack the computer systems, how do we reconstitute them?

Mr. VON NEUMANN. There are no plans in place right now, and there may be no way to anticipate the follow-up. I mean, if there is an attack, a physical attack, an explosion against or a line cutting, then there can be increased security in that area on those same facilities so the same thing would not happen again.

Senator LIEBERMAN. Right.

Mr. VON NEUMANN. If it is a computer issue, the attacker could be sufficiently skilled that they could simply change their method slightly and go around any defense that is put up in the place of the first attack.

Senator LIEBERMAN. And the ability to find the attacker would be compromised. It would be harder to find the attacker.

Mr. VON NEUMANN. Simply because of the nature of the Internet as it is, the no authentication, no proof of where you are, who you are.

Mr. SPACE ROGUE. In your line-cutting analogy, the guy goes out and snips the wire, maybe somebody saw him and we can track him through a witness. If he comes in over the Internet and attacks the computer systems, you do not know where he came from and nobody saw him.

Senator LIEBERMAN. Exactly. I have a final question. Somebody used the VW example, and it is an interesting one. As you said, three cars show some sign of the impact of the wiring defect; they recall all 8,500 of the new Beetles that they have sold in the United States. As you said correctly, as far as I know, three indications of hacking into a system, nobody is under an obligation to do it.

I have not looked at this in a while, but the automobile companies and the recalls are not motivated simply by, if I may overuse

the term here, good citizenship. There is law and there is the fear of liability.

This is a complicated area, and as Dr. Neumann said, we have got to be real careful not to jump too quickly without thinking about it, but is there a way in which we should be setting some standards here? I mean, for instance, a very simplistic standard would be to require systems operators or service providers or manufacturers to give public notice of instances of hacking, successful hacking into a system.

Mr. MUDGE. Or at least public notice of vulnerabilities that they have found in their system. This is definitely a double-edged sword, because when you give the information out, other people can figure out how to exploit it.

Senator LIEBERMAN. Yes.

Mr. MUDGE. However, if you do not give the information out, the people out there cannot protect themselves. I think we have tried it, the route where we have kept the information secret. The Computer Emergency Response Team out of Carnegie Mellon does that. I think, and I know a whole bunch of people in the computer industry agree with me on this, that they have become more detrimental than beneficial by a long shot. A couple of words of encouragement from right behind me.

Full disclosure is very important. I mean, you have to educate people. Education is one of the largest things that is really missing out of this. If I am an administrator and there is a problem in what I have to control but the companies do not let me know about it, I cannot be expected to fix it. Even if the companies do not have a fix themselves, if I know of the problem, I might be able to put other things in place in front of it so I can catch it.

Senator LIEBERMAN. Right.

Mr. MUDGE. I might have a different setup. Not everybody has the exact same setup.

Mr. POND. You might disconnect your system from the network.

Mr. MUDGE. Yes. I might say, hey, that is really bad. I need to get off of there right now. But I would be able to do that.

Mr. VON NEUMANN. I will go one further, not only to point out the flaws but also to point out the inner workings. This may be rehashing something that is well known, but the UNIX environment, being around for so many years, being public, being able to be examined, has most of the fixes quite well known. Microsoft Windows NT, all of their code is completely hidden from public eyes. They do not release it. It is, as has been said, a black box. So the public, even if an end user wanted to go and look inside the internals of, say, Windows, Windows NT, they are not allowed to. It is illegal according to the software licensing put forth by Microsoft to disassemble, to try and reverse engineer it. That kind of a limitation is just putting the brakes on investigation of the flaws.

Mr. MUDGE. It is like buying a car and not being able to open the hood.

Mr. VON NEUMANN. Exactly.

Senator LIEBERMAN. Amen. That is a good comparison to close on. I want to thank you again. This is another classic example of what we find very often on this side, as lawmakers, which is that we see a problem, we want to make it better, we contemplate law,

but this is in an area of very developed expertise which most of us do not have. So we often rely on science and data and on the people who have more expertise and then try to make the best judgment we can.

In thanking you, I really want to, although I know you have already got a day job and a vocation, but to the extent that you find time, I really ask you, request that you think about what we, as lawmakers, if anything—I mean, it may be that you are going to come back and say, you are only going to mess it up here—what we might do through law to protect ourselves from some of the vulnerabilities that you have identified. Thanks very much.

Chairman THOMPSON. Thank you very much.

Gentlemen, thank you very much for being here with us today. I, like Senator Lieberman, think that you are performing a valuable service to your country and we appreciate that and want you to continue and want you to continue to help us.

I think the liability question is a very good one. I wonder, for example, whether or not it is a matter of law, as whether or not there are already laws under the common law, under State laws, the general tort law of negligence and fraud and the Uniform Commercial Code and all those things, the first time some big company has been compromised because of this, it may fix itself because there will be a massive lawsuit and everybody will wonder why we did not address this in the beginning.

But they are fascinating issues. You have pointed out that our computer security is virtually nonexistent and how easy it is to obtain sensitive information and shut down valuable governmental operations. We are going to have to do something about it. It is that simple.

I am going to release now, and you gentlemen might just stay where you are, I am going to move on to another matter very briefly. This will be the final piece of business and I do not think there will be anything here that you find shocking. At this time, the Committee will now release three GAO reports on computer and information security all prepared at our direction.[1]

The first two reports involve careful study by GAO of the level of computer and information security at two Federal agencies, the State Department and the Federal Aviation Administration, whose operations affect the safety and well-being of all of us. In their entirety, the State and FAA reports are classified, but the agencies have agreed to make public edited versions of the reports, which we are now releasing today.

As the reports demonstrate, both State and FAA have pervasive and crippling security problems. First, regarding State, GAO hacked into State's computers with ease, using hacking tools available for free on the Internet. The results of GAO's work are startling. GAO was able to access all kinds of sensitive information, including travel itineraries for senior U.S. diplomatic officials, personnel and employment records, and E-mail traffic among State Department employees. Even worse, GAO was literally able to take control of the State Department's computers and could have shut

[1] The GAO reports appear in the Appendix on pages 95, 117, and 136 respectively.

them down or falsified the information on them. Unfortunately, this went undetected by the State Department.

Unlike the State Department, the GAO did not even have to break into FAA's computers to satisfy themselves of the weaknesses there. GAO found well-documented evidence in the FAA's own files that details security problems in the air traffic control system. The GAO report contains tough criticism of the FAA practices, concluding that FAA is not doing the job properly in critical areas. The title of the report sums this up, "Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety."

I might read a couple sentences from that report. I think it points out another critical problem with regard to the question of risk analysis. It says the FAA had performed the necessary analysis to determine system threats, vulnerabilities, and safeguards for only 3 of 90 operational air traffic control computer systems, or less than 4 percent. Further, according to the team that maintains FAA's telecommunications networks, only one of the nine operational air traffic control telecommunications networks has been analyzed. Without knowing the specific vulnerabilities of this air traffic control system, FAA could not adequately protect them. So we do not even know the extent of our problem, the extent of our vulnerabilities.

Finally, a third GAO report that we are releasing today may hold the key to improving Federal Government computer security. The report, which details the best practices used by leading private companies for computer security, ought to provide an indication for improvements as the State Department, FAA, and other Federal agencies struggle to manage computer security concerns. We intend to follow up with the FAA and State Department to monitor their progress in implementing the GAO recommendations.

With these reports, the Committee is also releasing a statement by GAO that summarizes their findings.[1] We will have subsequent hearings with the GAO, with the people at the State Department and the FAA and other governmental agencies that the GAO is doing additional investigations with regard to.

So with that, this hearing concludes and the Committee stands adjourned. Thank you very much.

[Whereupon, at 12:23 p.m., the Committee was adjourned.]

[1] The prepared statement of GAO appears in the Appendix on page 43.

APPENDIX

GAO PREPARED STATEMENT FOR THE RECORD BY GENE L. DODARO, ASSISTANT COMPTROLLER GENERAL, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION

INFORMATION SECURITY: SERIOUS WEAKNESSES PUT STATE DEPARTMENT AND FAA OPERATIONS AT RISK

(GAO/T-AIMO-98-170)

Mr. Chairman and Members of the Committee: We are pleased to be asked to discuss our work in computer security. As requested, our testimony will focus on the results of our recent reviews of the Department of State and the Federal Aviation Administration (FAA). Significant computer security weaknesses at both these organizations threaten the integrity of their operations, and we have made numerous specific recommendations for improving State and FAA's information security posture. Unfortunately, such weaknesses are typical at most Federal agencies we evaluate. However, good management practices and organizational discipline can do much to mitigate the risks all government agencies face from security threats. Accordingly, we will also highlight best practices we have identified in studying leading organizations that can be used by all agencies to protect sensitive information and computer systems.

Computer Security is an Increasing Threat To Critical Government Operations

The dramatic increase in computer interconnectivity and the popularity of the Internet are offering government agencies unprecedented opportunities to improve operations by reducing paper processing, cutting costs, and sharing information. At the same time, however, malicious attacks on computer systems are increasing at alarming rates and are posing serious risks to key government operations. Thus, the ultimate success of agencies' ability to use interconnected systems to carry out critical governmental functions depends in large part on their ability to protect the integrity, privacy, and availability of the data and systems they rely upon.

This Committee has long been concerned about the need to protect sensitive information in Federal computer systems. These concerns are well-founded. At the request of you, Mr. Chairman, and Senator Glenn, we have undertaken a large body of work to address the issue, including reviews of most of the Federal Government's largest departments' and agencies' computer security programs. In conjunction with our financial statement audit focus and high-risk reviews, this work has revealed a disturbing picture of our government's lack of success in protecting Federal assets from fraud and misuse, sensitive information from inappropriate disclosure, and critical operations from disruption. For example:

- In May 1996, we reported that computer hackers had penetrated Defense computer systems; obtained and corrupted sensitive information; shut down and crashed entire systems and networks; and denied service to users who depend on automated systems to help meet critical missions, including weapons and supercomputer research, logistics, procurement, and military health. Our recommendations focused on the need for Defense to assign clear responsibility and accountability for the successful implementation of its security program; improve its security policies and procedures; increase security awareness; and implement more proactive technical protection and monitoring systems. [1]

[1] Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

- In September 1996, we reported that, over the previous 2 years, serious weaknesses had been reported for 10 of the largest Federal agencies, concluding that poor information security was a widespread Federal problem with potentially devastating consequences.[2] In that report, we recommended that OMB play a more proactive role in overseeing agency practices and managing improvements, in part through its role as chair of the Chief Information Officers (CIO) Council.
- In February 1997, we identified information security across all government agencies as a high-risk area. We found management and system controls to be largely inadequate leaving critical operations at many agencies highly vulnerable to unauthorized access.[3]
- In three 1997 reports, we identified a wide range of continuing serious weaknesses in IRS systems, including inadequate controls over employee browsing of taxpayer records.[4]
- In March 1998, in our report on the Federal Government's consolidated financial statements, we emphasized that pervasive computer control weaknesses were placing enormous amounts of Federal assets at risk of fraud and misuse, financial information at risk of inappropriate disclosure, and critical operations at risk of disruption.[5]

Also at your request, we are currently (1) examining computer security programs at other selected agencies including the National Aeronautics and Space Administration, (2) developing a comprehensive and detailed analysis of information security problems at the largest Federal agencies, and (3) producing an updated summary of actions taken by OMB and the CIO Council to address these problems from a governmentwide perspective.

Today, the Committee is releasing the redacted versions of our reports on computer security at State and FAA.[6] These reviews resulted in many findings that are too sensitive to discuss in today's open setting and, accordingly, detailed reports have been provided to this Committee and to appropriate agency officials under separate cover. However, we will describe the types of weaknesses found and the risks they posed to critical systems and information.

Pervasive Computer Security Weaknesses Threaten State Department Operations

Last year, this Committee asked us to assess whether the State Department's unclassified automated information systems were susceptible to unauthorized access. State relies on a variety of decentralized information systems and networks to help it carry out its responsibilities and support business functions, such as personnel, financial management, medical, visas, passports, and diplomatic agreements and communications. The data stored in these systems, although unclassified, are sensitive enough to be attractive targets for individuals and organizations seeking monetary gain or desiring to learn about or damage State operations. For example, much of this information deals with employees working for the department and includes American and Foreign Service National personnel records, employee and retiree data, and private health records. Background investigation information about employees being considered for security clearances is also processed on State's unclassified network.

The potential consequences of misuse of this information are of major concern. For example, unauthorized deletion or alteration of data could enable known criminals, terrorists, and other dangerous individuals to enter the United States. Personnel information concerning approximately 35,000 State employees could be useful to foreign governments wishing to build personality profiles on selected employees. Manipulation of financial data could result in over- or underpayments to vendors, banks, and individuals, and inaccurate information being provided to agency man-

---

[2] Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996).

[3] High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[4] IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997); Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements (GAO/AIMD-97-89, August 29, 1997); Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997).

[5] Financial Audit: 1997 Consolidated Financial Statements of the United States Government (GAO/AIMD-98-127, March 31, 1998).

[6] Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998) and Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

agers and the Congress. Furthermore, the overseas activities of other Federal agencies may be jeopardized to the extent they are supported by State systems.

To determine State's vulnerability to computer attacks, we tested the department's technical and physical controls for ensuring that data, systems, and facilities are protected from unauthorized access. We designed our tests to simulate two security penetration scenarios: (1) an unauthorized individual who has no knowledge of State's automated information infrastructure (for example, a hacker or terrorist organization) and (2) a mid-level internal user with limited access privileges and some specific computer related information (for example, a State employee) exceeding his or her limited privileges.

In simulating these scenarios, we wanted to know whether an unauthorized user could compromise—that is, improperly access, modify, disclose, or destroy—sensitive data if he or she successfully penetrated State's computer resources. During our testing, we performed controlled penetration attacks at dial-in access points, internal network security controls, the department's Internet gateways, and public information servers. We also attempted to gain unauthorized physical access to certain State facilities and assessed users' awareness by attempting to get them to reveal sensitive information such as their passwords. Such techniques, sometimes referred to as social engineering, can be used by attackers to easily bypass an organization's existing physical and logical security controls.

Unfortunately, our penetration tests were largely successful. They demonstrated that State's computer systems and the information contained within them are very susceptible to hackers, terrorists, or other unauthorized individuals seeking to damage State operations or reap financial gain by exploiting the department's information security weaknesses. For example, without any passwords or specific knowledge of State's systems, we successfully gained access to State's networks through dial-in connections to modems. Having obtained this access, we could have modified, stolen, downloaded, or deleted important data, shut down services, and monitored network traffic such as e-mail and data files.

In addition, by posing as a trusted inside computer user, we were able to circumvent State's internal network security controls and access information and sensitive data which would normally be off-limits to most employees. For example, after we gained (administrator) access[7] to host systems on several different operating platforms, such as UNIX and Windows NT, we viewed international financial information, travel arrangements, detailed network diagrams, a listing of valid users on local area networks, employees' e-mail, performance appraisals, and other sensitive data.

Our tests also showed that security awareness among State employees was problematic. For example, many computer users at State had weak passwords that were easily guessed, indicating that they were unaware of, or insensitive to, the need for secure passwords. One way to prevent password guessing is to ensure that users choose complex passwords such as those composed of alphanumeric, upper- and lower-case characters. However, we found no evidence that State was training its users to employ these techniques. We also found little evidence that State was training its users to refrain from disclosing sensitive information. For example, we called a user under the pretense that we were systems maintenance personnel and were able to convince her to disclose her password.

We also obtained access to State's networks by breaching physical security at one facility, and finding user account information and active terminal sessions in unattended areas. For example, in several instances we were able to enter a State facility without required identification. In an unlocked office, we found unattended personal computers logged onto a local area network. We also found a user identification and password taped to one of the computers. Using these terminals, we were able to download a file that contained a password list. This list could have been used later to help hack into State's systems. In another unlocked area, we were able to access the local area network server and obtain supervisor-level access to a workstation, which would have allowed us to even more easily circumvent controls and hide any traces of our activities.

Internet security was the only area in which we found that State's controls were currently adequate. We attempted to gain access to internal State networks by going through and around State's Internet gateways or exploiting information servers from the outside via the Internet, but we were not able to gain access to State's systems. State's protection in this area was adequate, in part, because the department

[7] Also known as "superuser" access, obtaining this access level permits total control of a system's operations and security functions. With system administrator rights, one can start up and shut down a system; add and remove system users; install or delete system software; and read, modify or delete all system data.

currently limits use and access to the Internet. However, State officials have been requesting greater Internet access and the department is considering various options for providing it.

Expansion of Internet services would provide more pathways and additional tools for an intruder to attempt to enter unclassified computer resources and therefore increase the risk to State systems. Recognizing this, State conducted an analysis of the risks involved with increasing Internet use. However, the department has not yet decided to what extent it will accept and/or address these new risks. Until it does so, State will not be in a good position to expand its Internet use.

The primary reason why our penetration tests were successful is that State, like many Federal agencies, lacks the basic building blocks necessary to effectively manage information security risks. First, State did not have a central focal point to oversee and coordinate security activities. Computer security responsibilities were fragmented among three organizations—the Chief Information Office, Diplomatic Security, and Information Management—none of which had the authority to effect necessary changes. Second, State did not routinely perform risk assessments so that its sensitive information could be protected based on its sensitivity and criticality to mission-related operations. Third, the department's primary information security policy document was incomplete. Fourth, State was not adequately ensuring that computer users were fully aware of the risks and responsibilities of protecting sensitive information. Fifth, the department did not routinely monitor and evaluate the effectiveness of its security programs, and it did not established a robust incident response capability.

A key reason why these critical elements of security were not in place was that top managers at State had not demonstrated a commitment to establishing a comprehensive and effective information security program. For example, even though State had reported mainframe computer security to the President and the Congress as a material weakness under the Federal Managers' Financial Integrity Act for the past 10 years,* the problem had not yet been corrected. In addition, information security had often been assigned to low- and mid-level State employees as a collateral duty. Finally, State's top managers had still not developed a comprehensive security plan or ensured that appropriate resources were devoted to improving computer security.

In our report being released today, we recommended that State take a number of actions to address these weaknesses to improve its information security posture. For example, we recommended that the Secretary of State:

- establish a central information security unit with responsibility for facilitating, coordinating, and overseeing departmental information security activities;
- develop and maintain an up-to-date security plan;
- develop policies and procedures that require senior State managers to evaluate the risks to their sensitive information and systems and determine appropriate solutions;
- assign the CIO the responsibility and full authority for ensuring that the information security policies, procedures, and practices of the agency are adequate; and
- defer expansion of Internet usage until State addresses known vulnerabilities and provides appropriate security measures commensurate with risks associated with the planned level of Internet expansion.

In addition, we provided State with dozens of suggested solutions to mitigate the specific weaknesses that our tests identified. We are pleased to report that in concurring with our recommendations, State identified a number of actions it is beginning to take to strengthen its information security program. For example, State advised us that its Chief Information Officer is beginning to address the lack of a central focus for information systems security by establishing a Security Infrastructure Working Group. State also agreed to formalize and document risk management decisions, revise provisions of the Foreign Affairs Manual related to information security, and undertake an evaluation of one of its most significant networks based on our review. Furthermore. State said it is implementing a plan to correct the technical weaknesses identified during our testing. However, State did not agree with our recommendation to defer expansion of Internet use until the department addresses known vulnerabilities. In explaining its nonconcurrence, State asserted that

*The Federal Managers' Financial Integrity Act: 1996 Report to the President and the Congress (United States Department of State, December 1996).

expanding Internet usage is a priority and that the department has a plan to mitigate the risks of expansion.

FAA's Weak Computer Security Practices Jeopardize Flight Safety

Given the paramount need to ensure safe air travel, this Committee also asked us to review FAA's computer security program. FAA's air traffic control (ATC) computer systems provide information to air traffic controllers and aircraft flight crews to ensure safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruptions of air traffic or even loss of life due to collisions.

To determine whether computer security at FAA is effective, we were asked to assess (1) whether FAA was effectively managing physical security at ATC facilities, (2) whether FAA was effectively managing systems security for its current operational systems, (3) whether FAA was effectively managing systems security for future ATC modernization systems, and (4) the effectiveness of its management structure and implementation of policy for computer security. We elected not to perform penetration testing at FAA because, in the early phases of our work, we already had (1) identified serious deficiencies in each of the areas we reviewed, (2) found evidence of ATC systems that had been penetrated and critical ATC data compromised, and (3) determined that FAA had planned to conduct its own penetration tests on select ATC systems.

We found that FAA was not effectively managing physical security at ATC facilities. Known weaknesses exist at many facilities. For example, at one facility, an FAA inspection report disclosed that service contract employees were given unrestricted access to sensitive areas without having appropriate background investigations. FAA's assessment of another facility that controls aircraft concluded that access control procedures were weak to nonexistent and that the facility was extremely vulnerable to criminal and terrorist attacks. Furthermore, we found that FAA did not know if other facilities were similarly vulnerable because it had not assessed the physical security controls at 187 facilities since 1993. FAA also was ineffective in managing systems security for its operational systems and was in violation of its own policy. A review conducted for FAA's Office of Civil Aviation Security in October 1996 by the Volpe National Transportation Systems Center[9] concluded that FAA had performed the necessary analysis to determine system threats, vulnerabilities, and safeguards for only 3 of 90 operational ATC computer systems, or less than 4 percent.[10] FAA officials told us that this was an accurate depiction of the current state of operational systems security. In addition, only one of the nine operational ATC telecommunications networks had been analyzed. Such poor security management existed despite the fact that FAA's 1994 Telecommunications Strategic Plan stated that "vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety." FAA's 1997 Telecommunications Strategic Plan continued to identify security of telecommunication systems as an area in need of improvement. Without knowing the specific vulnerabilities of its ATC systems, FAA cannot adequately protect them.

FAA claimed that because current ATC systems often utilize custom-built, 20-year-old equipment with special purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited. While these configurations may not be commonly understood by external hackers, one cannot assume that old or obscure systems are, a priori, secure. In addition, the certification reports that FAA has done revealed operational systems vulnerabilities. Furthermore, archaic and proprietary features of the ATC system provide no protection from attack by disgruntled current and former employees who understand them.

Additionally, FAA had not been effectively managing systems security for future ATC modernization systems. FAA had no security architecture, security concept of operations, or security standards. As a result, implementation of security requirements across ATC development efforts was sporadic and ad hoc. Of the six current ATC system development efforts that we reviewed, four had security requirements, but only two of the four developed their security requirements based on a risk assessment. Without security requirements based on sound risk assessments, FAA cannot effectively protect future ATC systems from attack. Further, with no security

---

[9]The John A. Volpe National Transportation Systems Center, located in Cambridge, Massachusetts, is a Federal Government organization whose principal role is to serve as a national center for transportation and logistics expertise. It provides research, management, and engineering support to the U.S. Department of Transportation, other Federal agencies, and state and local governments.

[10]Volpe Transportation Systems Center NAS AIS Security Review, Final Report, October 1, 1996.

requirements specified during systems design, any attempts to retrofit security features later will be increasingly costly and technically challenging. As FAA modernizes and increases system interconnectivity, ATC systems will become more vulnerable, placing even more importance on FAA's ability to develop adequate security measures. These future vulnerabilities are well documented in FAA's information security mission need statement and also in reports completed by the President's Commission on Critical Infrastructure Protection. The mission need statement asserts that "information security is the FAA mission area with the greatest need for policy, procedural, and technical improvement. Immediate action is called for to develop and integrate information security into ATC systems." The President's Commission summary report concluded that the future ATC architecture appeared to have vulnerabilities and recommended that FAA act immediately to develop, establish, fund, and implement a comprehensive systems security program to protect the modernized ATC system from information-based and other disruptions, intrusions, and attacks. It further recommended that this program be guided by the detailed recommendations made in the National Airspace Systems vulnerability assessment.

Finally, FAA's management structure and implementation of policy for ATC computer security was not effective. Security responsibilities were distributed among three organizations, all of which have been remiss in their ATC security duties. The Office of Civil Aviation Security was responsible for developing and enforcing security policy, the Office of Air Traffic Services was responsible for implementing security policy for operational ATC systems, and the Office of Research and Acquisitions was responsible for implementing policy for ATC systems that are being developed. The Office of Civil Aviation Security had not adequately enforced FAA's policies that require the assessment of physical security controls at all ATC facilities and vulnerabilities, threats, and safeguards for all operational ATC computer systems. In addition, the Office of Air Traffic Services had not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards. Finally, the Office of Research and Acquisitions had not implemented the FAA policy that requires it to formulate requirements for security in specifications for all new ATC modernization systems.

FAA recently established a central security focal point, the National Airspace Systems Information Security (NIS) group, to develop additional security guidance (i.e., a security architecture, a security concept of operations, and security standards), to conduct risk assessments of selected ATC systems, to create a mechanism to respond to security incidents, and to provide security engineering support to ATC system development teams. This group has developed an action plan that describes each of its improvement activities, but it has not developed detailed plans or schedules to accomplish these tasks.

Establishing a central security focal point is a practice employed by leading security organizations. However, in order to be effective, the security focal point must have access to senior executives that are organizationally positioned to take action and effect change across organizational divisions. One approach for ensuring that a central group has such access at FAA would be to place it under a Chief Information Officer (CIO) who reports directly to the FAA Administrator. This approach is consistent with the Clinger-Cohen Act,[11] which requires that major Federal departments and agencies establish CIOs who report to the department/agency head and are responsible for implementing effective information management.

FAA does not have a CIO reporting to the Administrator. Although the NIS group has access to certain key Associate Administrators (e.g., the Associate Administrator for Civil Aviation Security and the Associate Administrator for Research and Acquisitions), it does not have access to the management level that can effect change across organizational divisions, especially FAA's Administrator or Deputy Administrator. Thus, there is no assurance that the NIS group's guidance, once issued, will be adequately implemented and enforced, that results of its risk assessments will be acted upon, and that all security breaches will be reported and adequately responded to. Until existing ATC computer security policy is effectively implemented and enforced, operational and developmental ATC systems will continue to be vulnerable to compromise of sensitive information and interruption of critical services.

In our report, we recommended that FAA take a number of actions to improve its information security. For example, we recommended that FAA

- develop and execute a plan to inspect the 187 ATC facilities that have not been inspected in over 4 years and correct any weaknesses identified,
- correct identified physical security weaknesses at inspected facilities,

[11]The 1996 Clinger-Cohen Act, Public Law No. 104-106, section 5125, 110 Stat. 684 (1996).

- ensure that specifications for all new ATC systems include security requirements based on detailed security assessments, and
- ensure the NIS group establishes detailed plans and schedules to develop a security architectu· a security concept of operations, and security standards and that these plans are implemented.

Finally, we recommended that FAA establish an effective management structure for developing, implementing, and enforcing ATC computer security policy. Given the importance and the magnitude of the information technology initiative at FAA, we expanded on our earlier recommendation that a CIO management structure similar to the department-level CIOs as prescribed in the Clinger-Cohen Act be established for FAA [12] by recommending that FAA's CIO be responsible for computer security. We further recommended that the NIS group report to the CIO and that the CIO direct the NIS group to implement its plans.

In contrast to State, the Department of Transportation's response to our recommendations was disappointing. The Department only discussed its efforts for timely corrective actions pertaining to 1 of our 15 recommendations. It did not state what, if any, specific action it would take on the remaining 14 recommendations. This noncommitment is troubling considering that several of our recommendations are requesting that FAA adhere to its existing computer security policies.

Learning From Leading Organizations To Face the Challenges in Securing Systems

Poor computer security is a pervasive problem across government. Security problems are often dealt with on an ad hoc basis with too little attention given to systemic issues and problems that underlie individual security lapses or breaches. Frequently, responsibility for computer security is viewed as burdensome and relegated to (1) technical staff who do not have the resources or clout to prompt improvements and/or (2) line staff who lack the training and experience necessary to fully appreciate and mitigate computer security risks.

The problem is further complicated by the complex computing environment most agencies now must have to meet their operating needs. Many agencies have a conglomeration of mainframes, PCs, routers, servers, software applications, and external connections. Because absolute protection over these complex infrastructures is not feasible, developing effective information systems security involves an often intricate set of trade-offs between the (1) type and sensitivity of the information and operations to be protected, (2) vulnerabilities of the computers and networks, (3) various threats, including hackers, thieves, disgruntled employees, competitors, and in the Federal Government's case, foreign adversaries and spies, (4) countermeasures available to combat the problem, and (5) costs. In making these trade-offs, agencies must understand the information security risks to their operations and assets, decide what they are going to do to defend themselves, and determine what risks they are willing to accept.

We have found that many problems contribute to agencies' difficulties in successfully balancing the trade-offs necessary to establish effective computer security. However, an underlying factor is that senior agency officials have not established a framework for managing the information security risks associated with their operations. To better determine how leading organizations handled these trade-offs, we undertook a comprehensive study—at this Committee's request—of eight organizations with superior security programs. These organizations—regardless of business type, size, or management structure—had one overriding tenet: business "owners," not security experts, assumed both responsibility and accountability for computer security. At the same time, however, security specialists played a strong educational and advisory role and had the ability to elevate discussions to higher management levels when they believed that risks were not being adequately addressed.

The organizations we studied managed their information security risks by implementing a continuing cycle of monitoring business risks, maintaining policies and controls, and monitoring operations. This cycle of activity parallels the process associated with managing the controls associated with any type of program. As illustrated in the figure below, all of these activities are coordinated through a central management office or group who served as consultants and facilitators to individual business units and senior management.

Each element of the risk management cycle, in turn, has a number of individual practices which these organizations followed to minimize risk.

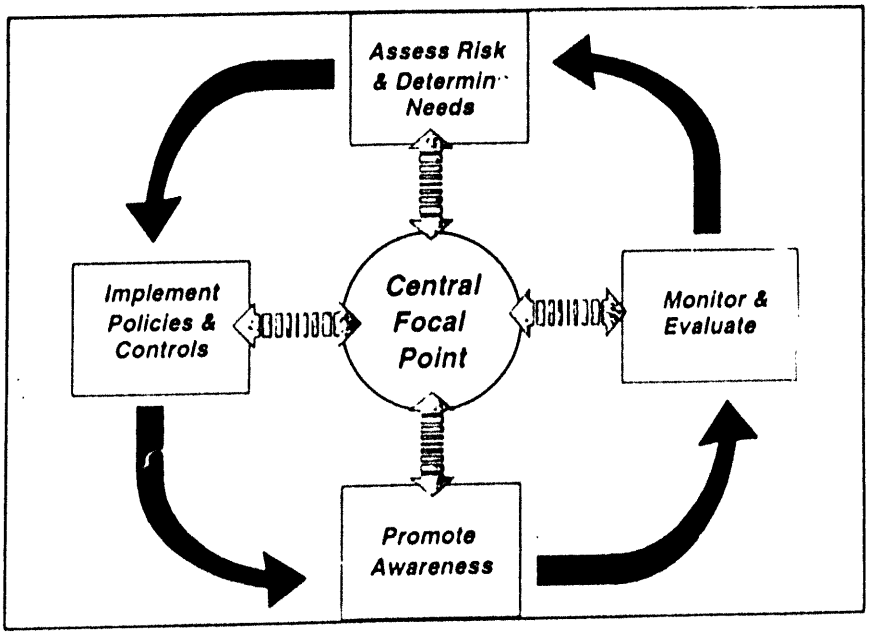
---

[12] Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, Feb. 3, 1997) and Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, Mar. 21, 1997).

We are pleased that the Committee is releasing the executive guide, which summarizes the results of our study, today.[13] We are equally pleased that the CIO Council has also endorsed our executive guide and the 16 practices followed by leading organizations. We are working with the Council and the Office of Management and Budget to encourage agencies to adopt these practices as additional guidance that can be used to enhance the government's ability to protect Federal assets from fraud and misuse, inappropriate disclosure of sensitive information, and disruption of critical operations. And, of course, we are continuing our work for this Committee to review agency computer security programs and to identify solutions that target the underlying causes of security weaknesses. We are also working with the CIO Council to develop improved risk assessment practices and methodologies and have planned a significant amount of work in this area over the next 3 years.

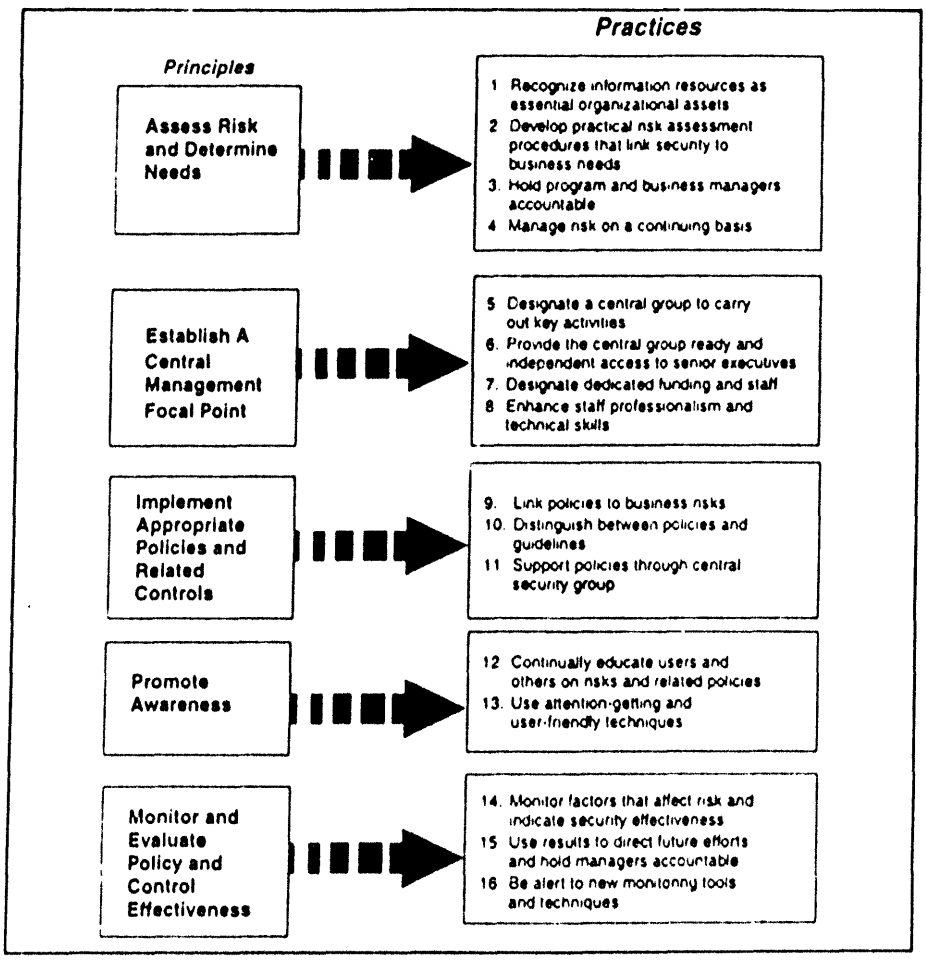
This completes our testimony.

Figure 1: *Risk Management Cycle*



[13] Executive Guide: Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Figure 2: *Sixteen Practices Employed by Leading Organizations to Implement the Risk Management Cycle*



Computer-Related Infrastructure Risks for Federal Agencies

Peter G. Neumann
Principal Scientist, Computer Science Laboratory
SRI International, Menlo Park CA 94025-3493
Telephone: 1-650-859-2375
Internet: Neumann@CSL.SRI.com; Website: http://www.csl.sri.com/neumann.html

Written testimony for the U.S. Senate Committee on Governmental Affairs
19 May 1998

I greatly appreciate being invited to appear before you. Some of you recall my June 1996 testimony for your Permanent Subcommittee on Investigations (Reference 4). I have tried not to simply duplicate that testimony (which is still surprisingly relevant). I begin by summarizing my main points and then examine what has changed in the past two years.

This written statement surveys the primary risks related to computer-communication technology, and what we might do to reduce them. The scope of my remarks broadly includes Federal Government systems, but is also applicable to State, local, and private sector systems as well. (The problems are essentially the same, although the perspectives are quite different.) I address security, reliability, availability, and overall survivability of those systems.

I appear here as a private citizen, although I have several affiliations that are worth noting. I am employed by a not-for-profit R&D institute (SRI International), where I am involved in several particularly relevant projects -- including an advanced system for detecting network misuse and related threats (for DARPA), and a study of the requirements and suitable system architectures for highly survivable systems and networks (for the Army Research Lab). I am a member of the General Accounting Office Executive Council on Information Management and Technology. I am the author of a book (*Computer-Related Risks*) on what has gone wrong and what we should expect to go wrong, and what we can do to reduce the risks involved in the use of computers. (For the record, I include at the end of this testimony some relevant further background.)

The Past and the Present

The final report of the President's Commission on Critical Infrastructure Protection (PCCIP) (Reference 1) addressed eight major critical *national infrastructures:* telecommunications; generation, transmission and distribution of electric power; storage and distribution of gas and oil; water supplies; transportation; banking and finance; emergency services; and continuity of government services. Perhaps most important is the Commission's recognition

that very serious vulnerabilities and threats exist in all of these critical infrastructures. Perhaps equally important if not more so is that all of these critical infrastructures are closely interdependent; a failure on one sector can easily affect other sectors. Furthermore, all of the national infrastructures depend critically on the underlying *computer-communication information infrastructures*, such as computing resources, databases, private networks, and the Internet. The extent to which this is the case is not generally appreciated, and seems sublimated in the PCCIP report. (See Reference 7.)

The existing national infrastructures and the underlying information infrastructures are riddled with vulnerabilities, representing security, reliability and system survivability flaws as well as potential attacks that can affect hardware, software, communications media, and people's lives. Security concerns are important, but it must also be remembered that systems and networks tend to fall apart on their own, without requiring malicious attacks. (The impending Year 2000 certainly gives us such an opportunity on an unprecedented scale.) Because the Government has become totally dependent on commercial system offerings that are typically not capable of satisfying critical requirements, the situation is becoming unstable.

- **Vulnerabilities.** Serious security flaws and reliability glitches are abundant in most computer systems, networks, Web software, and programming languages. These have been widely reported. The extent of the risks is still not widely recognized, although the Eligible Receiver exercise is clearly suggestive of what is possible. Furthermore, there has not been enough work to develop adequate preventive measures. As-yet-undiscovered vulnerabilities may be even greater than those that are known today. Future disasters may involve vulnerabilities that have not yet been conceived as well as those that are already lurking.
- **Threats.** There are many realistic threats to the information infrastructures, including malicious insiders and intruders, terrorists, saboteurs, and incompetent administrative and operational staff, in addition to effects of the environment, natural phenomena, accidental interference, and so on. These threats may come from corporate, national, or terrorist interests as well as individuals. The list of threats is long and multidimensional (and discussed in the PCCIP report). Consequently, it is not possible to predict which threats will be exploited, and under what circumstances.
- **Attacks.** Malicious attacks can come from anywhere in the world, via dial-up lines and network connections, and often anonymously. Thus far, there have been relatively few truly serious malicious attacks on computer systems and networking (for example, see Reference 12, which includes analysis of the Rome Lab case and was briefed to the Permanent Subcommitee on Investigations during its June 1996 hearings), although such activities from both insiders and outsiders appear to be increasing, particularly in financial systems (such as the $588 million Japanese Pachinko frauds and the Citibank case). There have been numerous cases of more than mere nuisance value (for example, the hacking of Web sites of the Justice Department, CIA, US Air Force, and NASA), including many denials of service (for example, flooding attacks that have disabled entire networks). The recent attacks on Pentagon systems by the unsophisticated Cloverdale kids were claimed by Deputy SecDef John Hamre to be "the most organized and systematic the Pentagon has seen

to date" -- but they really indicate only how flimsy Pentagon Internet computer security actually is, as representative of commercial product (un)security. Considering how easy it was for those kids, imagine what could happen if a terrorist group decided to use its resources for seriously nefarious purposes. (I know of several attacks that have never been acknowledged publically, some of which are quite startling.) Although it would be appropriate for the FBI to ratchet up its technical competence, expenditures of funds on prosecuting young system crackers might much better be spent in developing and procuring computer-communication systems that are substantially more secure than what is available today. Also noteworthy are the recent Masters of Downloading attack on the Defense Information Systems Network, and the Tamil Tigers in Sri Lanka. The random interception of a cell-phone conversation involving Newt Gingrich, and the more systematic interception of Secret Service pager messages involving the President (despite demonstrations four years ago at the Hackers on Planet Earth conference of how easy that was to do) are again symptomatic of weak security. Various penetration studies without malicious intent, failed experiments (such as the 1988 Internet Worm), and analyses have demonstrated actual flaws in deployed Web browsers, servers, protocols, algorithms, and encryption schemes. Eligible Receiver demonstrated further vulnerabilities. It is nice that we have so many friendly participants in this struggle to identify the vulnerabilities, although these efforts seem to have little impact on increasing the dependability of the systems thus penetrated. It appears that official concern will remain inadequate to the magnitude of the potential risks -- until we are hit by devastating attacks that demand immediate attention. The rapid acceleration of electronic commerce can be expected to inspire some ingenious massive frauds that systematically exploit various major vulnerabilities in the information infrastructure -- which could be a goldmine for organized crime. The weak security that is endemic today in many commercial systems is truly a travesty that we cannot afford to perpetuate in the future.

- **Reliability problems.** Examples of past accidental outages include the 1980 ARPAnet collapse, the nationwide 1990 AT&T long-distance collapse, the AT&T frame-relay business-network shutdown, many recent outages and saturations of Internet service providers, and many consequences of the spate of Western power outages two summers ago. These incidents demonstrate how apparently isolated events can propagate widely. The Year-2000 problem (Y2K) is of great concern to government agencies and the private sector alike. (See Reference 18 for a recent overview of the dramatic extent of the problem. Also, see U.S. Representative Stephen Horn's Y2K report card, which suggests that many Federal departments and agencies failing badly.) However, the Y2K problem is really just another example of the difficulty of developing software systems that will operate correctly over a broader range of requirements than were considered in the original requirements. (Foresight is not that difficult, but is often co-opted by short-term commercial interests or incredible myopia. For example, I was a co-designer from 1965 to 1969 of a highly innovative advanced secure system that clearly recognized and avoided the Y2K problem -- Multics, a significant research and development effort jointly among MIT, Bell Labs, and Honeywell.) However, if the Y2K problem is causing the Federal Government so much grief, how can the Government expect to do security properly? Date arithmetic is not difficult if you know what you are doing. Security is

much more difficult.

Many of the cases noted above are documented in Reference 3 and in the on-line Risks Forum.

With respect to the national infrastructures and the computer-communication infrastructures, it is clear that the threats are pervasive, encompassing intentional as well as accidental causes. Aviation is a serious concern. Power generation, transmission, and distribution are particularly vulnerable, as is the entire telecommunication infrastructure. However, it is certainly unpopular to discuss specific threats openly, and thus the risks tend to be largely downplayed -- if not almost completely ignored.

To give a more detailed example of the breadth of threats in just one critical-infrastructure sector not examined in much detail by the PCCIP, consider the safety-related issues in the national airspace, and the subtended issues of security and reliability. (See for example, my article for the International Conference on Aviation Safety and Security in the 21st Century, Reference 5.) Alexander D. Blumenstiel at the Department of Transportation in Cambridge, Massachusetts, has conducted a remarkable set of studies over the past 14 years. In his series of reports, Blumenstiel has analyzed many issues related to system survivability in the national airspace, with special emphasis on computer-communication security and reliability. His early reports (1985-86) considered the susceptibility of the Advanced Automation System to electronic attack and the electronic security of NAS Plan and other FAA ADP systems. Subsequent reports have continued this study, addressing accreditation (1990, 1991, 1992), certification (1992), air-to-ground communications (1993), air-traffic-control security (1993), and communications, navigation, and surveillance (1994), for example. To my knowledge, this is the most comprehensive set of threat analyses ever done outside of the military establishment. The breadth and depth of the work deserves careful emulation in other sectors. (See Reference 16.) Further problems relating to the FAA procurement practice and safety considerations have been subjects of various GAO reports.

In general, it may seem very unpopular to expend resources on events that have not happened or that are perceived to be very unlikely to occur. The importance of realistic threat and risk analyses is that it becomes much easier to justify the effort and expenditures if a clear demonstration of the risks can be made. Therefore, it is absolutely vital that you openly understand and acknowledge the pervasiveness of the existing vulnerabilities, threats, and risks, and the likelihood that they are getting worse rather than better. The General Accounting Office (e.g., Reference 12) and the National Research Council (e.g., Refererces 2, 9, and 17) are two major sources of objective analysis.

The risks noted above are critical to U.S. Government departments and agencies, particularly those that are concerned with the critical national infrastructures -- such as the Departments of Defense; Energy; Health and Human Services; Commerce; Transportation; as well as the FAA and the Social Security Administration. (Ironically, almost all of those organizations are already seriously threatened by the Y2K problem.)

Conclusions

- **Interconnectivity.** Computer systems have become massively interconnected, dramatically more so than a few years ago. We are now dependent on people and systems of unknown and unidentifiable trustworthiness (including unidentifiable hostile parties), within the U.S. and elsewhere. Our problems have become international as well as national.

- **Risks.** The fundamental vulnerabilities in the existing computer-communication infrastructure are pervasive, and the situation is not getting better. Although some old vulnerabilities are occasionally removed, others remain, and new vulnerabilities are continually being created. Electronic commerce is particularly at risk. The national infrastructures are also at risk. Because of the interdependence of the infrastructures, the risks tend to propagate: each component that is compromised increases the danger that other components will also be compromised. Multidisciplinary preventive measures are essential, but most measures to date have been narrowly conceived.
- **Diversity.** Diversity of systems, algorithms, techniques, and implementations is one of our biggest allies. It is extremely unwise to put all one's eggs in a single basket, especially when that basket is as full of holes as is increasingly the case today.
- **Privacy.** Privacy is becoming an orphan step-child, with flagrant commercial abuses. There have also been various cases of misuse of Government databases, including IRS data (not to mention rogue operatives) and law-enforcement data (Reference 13). In general, we have been lucky, but should not count on that in the future as the stakes and risks increase.

- **Cryptography.** Cryptography is an absolutely essential ingredient in achieving confidentiality, user authentication, system authentication, information integrity, and nonrepudiability. The Adminstration's cryptographic policy has failed to realistically recognize this need, despite the essential nature of strong nonsubvertible cryptography in protecting the national infrastructures and the information resources of the Government and Federal agencies. U.S. crypto policy has instead focused on limiting the use of strong cryptography, rather than on encouraging its use in vital systems -- including the critical national infrastructures. It has deterred efforts to improve security, and is beginning to drive the cutting-edge applications of cryptography abroad. (See References 8 and 9 for an elaboration of difficulties related to U.S. crypto policy, and Reference 6 for my Senate Judiciary Committee testimony.)

- **Authentication and passwords.** Reusable user passwords present serious risks, especially when they transit unencrypted communication paths that can be intercepted, or can otherwise be obtained. (Many of the familiar penetrations have involved compromise of reusable passwords.) The use of cryptographically based

authentication (with one-time tokens rather than often-reusable passwords) is essential to the security and survivability of our infrastructures. Even though cryptography used for authentication is treated differently by export controls, those controls have had the effect to dumb down the needed authentication techniques.

- **System development practice.** In general, efforts to develop and operate complex computer-based systems and networks that must meet critical requirements have been monumentally unsuccessful -- particularly with respect to security, reliability, and survivability. The U.S. Government (and almost everyone else) has experienced repeated difficulties in developing large systems, which are increasingly dominated by software. Significant problems have arisen, leading to cancellations of the en-route air-traffic control system upgrade, the IRS Tax Systems Modernization effort, law-enforcement systems (e.g., the fingerprint system), procurements for military and commercial aviation and defense systems, and the $300 million California Deadbeat Dads' and Moms' database system -- with expenditures of billions of dollars down the drain. (In the case of the federally mandated state database of deadbeats, as of the October 1995 deadline there were still 16 states that were unable to comply with the requirements.) However dire it turns out to be, the Y2K problem is merely the tip of an enormous iceberg relating to our inability to use greater foresight in developing complex systems. As a nation, we desperately need a better ability to develop complex systems -- within budget, on schedule, and likely to meet their stated requirements. The shuttle is one successful example of a large and very complex system development in which software goals were met adequately, although the costs of that effort were not insignificant and the risks were understood in advance better than in other systems. The development of robust hardware-software systems is an extremely widespread problem, and is not limited to either government or private-sector systems. (References 3 and 11 provide numerous additional examples of development fiascos.)
- **System use.** Even if a system is developed according to the stated needs (which is very rare), the practice of using such systems seems to be exceedingly sloppy. Employees are often poorly trained to cope with the idiosyncrasies of the systems they must use. Individual data items are often incorrect, particularly in IRS, social services, law enforcement, and motor-vehicle information systems. Privacy requirements are often flagrantly disregarded, or else nonexistent. Systems are sometimes unavailable.

Recommendations

- **Systems and networks.** We must improve our nation's ability to develop complex systems. Such system efforts are characteristically short-sighted, over-budget, late, and functionally inadequate with respect to system and enterprise survivability, security, reliability, and performance -- all of which must be more comprehensively built into the systems.
- **Personal-computer inadequacies.** We must accept the fact that existing personal-computer operating systems typically do not provide a sufficiently robust base on which to build critical applications that can perform dependably in the face of

threats to reliability and security. The marketplace is a marvelous incentivizer of technological innovation, but not an adequate motivation for really secure, reliable, and survivable systems. Overreliance on single systems and single developers is a disaster in the making, especially when those systems are not capable of fulfilling the real requirements.

- **The role of the U.S. Government.** Given the difficulties in system development and the fundamental inadequacies in baseline commercial products, the Government must rise to the challenge in several dimensions.

-- The U.S. Government must get its own house in order. It must strive to improve the security, reliability, and survivability of its systems and networks. To do this, it must streamline its procurement process, with depth of understanding in what is being procured rather than merely pro forma attention to bean counting. The specified requirements must demand better systems, and contracts to the lowest-bid proposal without a reasonable chance of succeeding should be avoided. The procurement process must include technically knowledgeable Government personnel (not just contractors acting as project managers).

-- Developers must somehow be encouraged or perhaps required to satisfy meaningful requirements for security and reliability in their baseline products. Y2K is merely one example. If you are overly concerned with the Y2K fiasco, you may be blindsided the deeper problems. Unfortunately, security is in the long run an even more critical problem.

-- You must have an accurate assessment of the appalling state of current systems with respect to security, reliability, and survivability in the face of realistic threats. You also need a realistic assessment of what is required to achieve sufficiently robust infrastructures. One way to do that might be to consider the computer-communication infrastructure necessary to provide the ability for Senators to vote remotely (for example, from a hearing room or while traveling). You would need a meaningfully secure system with no unauthorized access paths, strong cryptography, and nontrivial authentication with smart cards or biometrics. Even then, you would have only an inkling of the more general problem faced by the critical national infrastructures and digital commerce using the Internet and dial-up lines.

-- Funding vital research and prototype development is essential to help close the gap between commercial products and what is possible but not commercially desirable. Research on the composition of systems out of subsystems is particularly important, because seemingly simple combinations often result in complex and unpredicted behavior. This is also true of computer networks. In addition, we must find better ways of getting good research prototypes into the marketplace. Surprisingly perhaps, free software is sometimes preferable to proprietary products.

-- Better teaching and practice of good system engineering and software engineering must be encouraged, not just the fostering of computer literacy. Much deeper knowledge and experience is essential pervasively.

-- Better training of users is essential, aided by the development of systems with interfaces that are more user friendly.

- **Learning from the past.** We must have a better understanding of past disasters and what can be done to avoid them in the future. Past cases involving losses of lives (particularly in aviation and medical care), serious injuries, long-term effects on human well-being, and financial integrity and stability of individuals, organizations, and governments, are documented in References 3 and 11.
- **Cryptography policy.** Government policies relating to cryptography are now noticeably interfering with efforts to improve the security of our infrastructures. Furthermore, even the best cryptography can be compromised if the systems in which it is embedded are not adequately secure. Thus, we are in somewhat of a Catch-22 situation: we need stronger computer systems in which to ensure that good cryptography cannot be compromised through penetrations or other misuse, and we need strong cryptography to ensure secure communications and better computer systems. Neither good cryptography nor good system security is adequate by itself. We need both. We also need better Internet protocols; the existing protocols are fundamentally inadequate. The existing computer-communication infrastructures are so incredibly weak with respect to security that it is very unlikely that key-recovery and key-escrow infrastructures will be adequately robust or able to withstand serious misuse. Consequently, claims that they will increase security are generally fallacious. Former NSA Director Mike McConnell has publicly questioned the sensibility of this approach. A recent NSA report honestly and openly acknowledges some of the technical realities, risks, and other problems with key recovery (Reference 20). Commerce Secretary William Daley recently stated that export controls on U.S. cryptography will result in ``foreign dominance of this market'' and could result in serious losses to U.S. companies. The FBI's lobbying for extensive access to cryptographic keys and unencrypted versions of otherwise encrypted information has never honestly addressed the problems and risks examined in considerable detail in three objective reports (References 8, 9, and 10); the FBI is single-mindedly pursuing a strategy that simply cannot result in cost-effective systems with adequate safeguards, and is ignoring various logical alternatives. Although various cryptography bills have been introduced in the Congress, I believe that the E-PRIVacy bill (Encryption Protects the Rights of Individuals from Violation) newly introduced by Senators Ashcroft, Leahy, and Burns is very close to the mark, and should be considered seriously.
- **Foresight.** It is much wiser to anticipate problems that are likely to become critical, rather than to wait until disasters strike. Although it may be painful to accept the realities, it is certainly a better strategy in the long-run. The time to act is now.

In short, there are only a few minor changes for the better that have occurred over the past two years. The needs for security are much greater, because of the rapid growth of the Internet, the World Wide Web, and electronic commerce. However, technological improvements seem to have been undermined by new vulnerabilities and administrative laxity. Security concerns have also been sidetracked by the impending Y2K problem. The

awareness of risks has generally increased, due in part to the report of the President's Commission on Critical Infrastructure Protection. But the PCCIP report has not yet led to actions that can noticeably decrease the risks overall. Additional recommendations are contained in Willis Ware's recent report (Reference 19) relating specifically to the subject of the PCCIP report. Security in personal computers has not increased appreciably, and has actually decreased when PCs are networked. Firewalls are touted as the most recent magic bullet, but they are not an adequate answer, especially in the presence of the demand for World Wide Web access that must pass through the firewalls and other would-be violations of the overall desired security policies. Diversity seems to be dwindling in many Federal system procurements, particularly in the Pentagon -- which seems increasingly content to use systems that cannot meet its long-term needs for reliability, availability, security, and survivability under stress; today's personal computer systems are basically incapable of satisfying critical needs, and not much improvement is expected in the future. For example, relying on Microsoft to develop much more robust operating systems and networking is not likely to succeed; such systems are simply not in Microsoft's current business model. Diversity is absolutely essential in attaining survivable systems. Somehow we must find ways to encourage the development of better commercially available operating systems, network protocols, networking software, secure Webware, secure use of good nonsubvertible cryptography, and extensive authentication infrastructures. Understanding the negative implications of U.S. cryptography policy would be a very important step forward. Overall, considerable foresight is absolutely essential now to avoid continuation of the problems of the past, which otherwise will escalate badly in the future. What we do now will have very long-lasting effects.

The Future

There is much to be learned from the past system development cancellations and from systems that have not met their safety, security, and dependability requirements. The reasons for those failures are startingly varied and must be thoroughly understood before measures can be successfully taken to avoid similar problems in the future. Careful documentation of those failures would be a useful step forward.

The future of the Internet and electronic commerce is very bright from the point of view of what is possible. The future of our national infrastructures and our computer-communication infrastructures is much more cloudy if we acknowledge the vulnerabilities, threats, and potential risks, and the very slow progress in recent years. The PCCIP report suggests that dramatic action is needed just to protect the national infrastructures. Many of its conclusions represent a step in the right direction, and its recommendations deserve careful analysis. In addition, electronic commerce demands the availability of much more robust information infrastructures. Education, research, advanced development, foresight, an altruistic sense of what is really needed in the future, and awareness are all very important. Good system engineering and software engineering require knowledge, training, experience, and above all engineering discipline. Greater recognition of the problems is perhaps the most vital next step. Much more widespread computer literacy is essential, and the Senate is an excellent place to start.

Final Remarks

I appreciate this opportunity to give you my own views, based on many years of analyzing past experience. The situation may be much worse than I have indicated, but basically we will never know unless attacks occur. Massive coordinated attacks are possible, as the PCCIP report says. However, until high-visibility disasters occur, few people are willing to admit that something drastic needs to be done. It may take a Chernobyl-scale event to raise awareness levels adequately, perhaps bringing several of the national infrastructures to their knees simultaneously. (For example, January 1 in the year 2000 might be considered as an ideal time for a terrorist organization to strike -- assuming that such a cataclysm does not happen on its own.) Furthermore, following a disaster, there is a strong temptation to focus on narrow palliative measures that reduce the likelihood that the exact same causes will result in similar disasters, without looking ahead to bigger problems. It is difficult for decisionmakers to look at the broader picture. However, draconian legislative actions are not needed; what is most needed is a deep and objective understanding of the vulnerabilities, threats, and risks. I feel somewhat like Cassandra (whose correct prophesies of disaster were never believed); unfortunately, I will receive very little joy if someday people recognize that I was correct.

As I indicated at the beginning of this written testimony, I have tried to stress only the major points. Further details are provided in my testimonies for your Subcommittee on Investigations in June 1996 (Reference 4) and for the Senate Judiciary Committee in November 1997 (Reference 6), as well as in my RISKS book (Reference 3) and the materials cited in the appended list of illustrative risks (Reference 11). I recommend that you peruse these sources, and that you personally use the Internet and surf the Web, if you do not already: much good information is available (along with some not so good).

Above all, you must recognize that there are no easy answers. You cannot simply procure the systems that are necessary to achieve robust security, reliability, and overall system and network survivability. Such systems do not exist today in the commercial marketplace; in fact, unless something dramatic happens, they are not likely to exist in the future. Whereas very significant progress is being made in the research community, it is not finding its way into commercial systems. This pipeline somehow needs to be nurtured.

Please feel free to follow up after my oral testimony with any questions that may occur to you.

REFERENCES

1. Tom Marsh, ed., *Critical Foundations: Protecting America's Infrastructures,* President's Commission on Critical Infrastructure Protection, October, 1997 (http://www.pccip.gov).

2. David D. Clark, W. Earl Boebert, Susan Gerhart, John V. Guttag, Richard A. Kemmerer, Stephen T. Kent, Sandra M. Mann Lambert, Butler W. Lampson, John J. Lane, M. Douglas McIlroy, Peter G. Neumann, Michael O. Rabin, Warren Schmitt, Harold F. Tipton, Stephen T. Walker, and Willis H. Ware, *Computers at Risk: Safe Computing in the Information Age*, National Research Council, National Academy Press, 1991, 2101 Constitution Ave., Washington, D.C. 20418, 1996.

3. Peter G. Neumann, *Computer-Related Risks*, Addison-Wesley, 1995. ISBN 0-201-55805-X.

4. Peter G. Neumann, Security Risks in the Emerging Infrastructure, written testimony for the U.S. Senate Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 25 June 1996 (http://www.csl.sri.com/neumannSenate.html). See *Security in Cyberspace*, Hearings, S. Hrg. 104-701, 1996, pages 350-363, with oral testimony included on pages 106-111. ISBN 0-16-053913-7.

5. P.G. Neumann, *Computer Security in Aviation: Vulnerabilities, Threats, and Risks*, International Conference on Aviation Safety and Security in the 21st Century, White House Commission on Safety and Security, and George Washington University, 13-15 January 1997 (http://www.csl.sri.com/neumann/air.html).

6. Peter G. Neumann, *Security Risks in Key Recovery*, written testimony for the Senate Judiciary Committee, 9 July 1997 (http://www.csl.sri.com/judiciary.html). Written and oral testimony are being published by the Government Printing Office.

7. Peter G. Neumann, *Computer-Related Risks and the National Infrastructures*, written testimony, published in *The Role of Computer Security in Protecting U.S. Infrastructures*, Hearing before the Committee on Science Subcommittee on Technology, U.S. House of Representatives, 105th Congress, First Session, Number 33, 6 November 1997, U.S. Government Printing Office, 1997 (ISBN 0-16-056151-5), including oral testimony (pages 61-63), written testimony (pp. 64-99, http://www.csl.sri.com/neumann/house97.html), written responses to written questions (pages 148-161, http://www.csl.sri.com/neumann/house97.ans).

8. Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, 27 May 1997 (ftp://research.att.com/dist/mab/key_study.txt or .ps; http://www.crypto.com/key_study).

9. Kenneth W. Dam, W.Y. Smith, Lee Bollinger, Ann Caracristi, Benjamin R. Civiletti, Colin Crook, Samuel H. Fuller, Leslie H. Gelb, Ronald Graham, Martin Hellman, Julius L. Katz, Peter G. Neumann, Raymond Ozzie, Edward C. Schmults, Elliot M. Stone, and Willis H. Ware, Cryptography's Role In Securing the Information Society

(a.k.a. the CRISIS report), Final Report of the National Research Council Cryptographic Policy Study Committee, National Academy Press, 2101 Constitution Ave., Washington, D.C. 20418, 1996 (executive summary at http://www2.nas.edu/cstbweb).

10. Susan Landau, Stephen Kent, Clinton Brooks, Scott Charney, Dorothy Denning, Whitfield Diffie, Anthony Lauck, Douglas Miller, Peter G. Neumann, and David Sobel, *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy,* Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM), June 1994 (http://info.acm.org/reports/acm_crypto_study.html).

11. Peter G. Neumann, *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology* The most recent version is at ftp://www.csl.sri.com/pub/illustrative.PS, in PostScript form.

12. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* U.S. General Accounting Office, May 1996, GAO/AIMD-96-84.

13. Laurie E. Ekstrand, "*National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information,*" U.S. General Accounting Office testimony before the U.S. House of Representatives Subcommittee on Information, Justice, Agriculture, and Transportation, of the Committee on Government Operations, and the Subcommittee on Civil and Constitutional Rights, of the Committee on the Judiciary, 28 July 1993.

14. Peter G. Neumann, *Security and Integrity Controls for Federal, State, and Local Computers Accessing NCIC,* SRI Technical Report for the FBI, 29 June 1990.

15. Phillip A. Porras and Peter G. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, Proceedings of the National Information System Security Conference, October 1997. A preprint is available on-line at http://www.csl.sri.com/intrusion.html, along with other information on current work and historical background.

16. Alexander D. Blumenstiel, *Guidelines for National Airspace System Electronic Security,* DOT/RSPA/Volpe Center, 1987. This report considers the electronic security of *NAS Plan* and other FAA ADP systems. See also Alex D. Blumenstiel and Paul E. Manning, *Advanced Automation System Vulnerabilities to Electronic Attack,* DoT/RSPA/TSC, 11 July 1986, and an almost annual subsequent series of reports -- for example, addressing accreditation (1990,.1991,.1992),.certification (1992), air-to-ground communications (1993), ATC security (1993), and communications, navigation, and surveillance (1994). For further information, contact Alex Blumenstiel at 1-617-494-2391 (Blumenstie@volpe1.dot.gov) or Darryl Robbins, FAA Office of Civil Aviation Security Operations, Internal and AIS Branch.

17. Fred B. Schneider and Marjory Blumenthal, editors, *Trust in Cyberspace?* (working title, in near-final draft), National Research Council, National Academy Press, 2101

Constitution Ave., Washington, D.C. 20418, Final report of the National Research Council Committee on Information Trustworthiness, summer 1998.

18. *Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships,* U.S. General Accounting Office, May 1998, GAO/AIMD-98-85.
19. Willis H. Ware, *The Cyber-Posture of the National Information Infrastructure* Critical Technologies Institute, RAND, 1998. ISBN 0-8330-2621-6.
20. *Threat and Vulnerability Model for Key Recovery,* NSA, 1998.

Personal Background

I have been involved with the U.S. Government in different technological contexts for many years, including (among others) national security, law enforcement, air-traffic control, and NASA. My first computer-related job was for the Navy in the summer of 1953, 45 years ago in July 1998. More recently, I served on the IRS Commissioner's Advisory Group for 2.5 years, concerned ostensibly with privacy issues, but also seriously troubled by the now failed modernization effort. My current role on the GAO Executive Council on Information Management and Technology has been extensively concerned with the Government's difficulties in handling the Y2K problem.

I have long been concerned with security, reliability, human safety, system survivability, and privacy in computer-communication systems and networks, and with how to develop systems that can dependably do what is expected of them. For example, I have been involved in designing operating systems and networks, secure database-management systems, and monitoring systems that seek to identify abnormal patterns of behavior. I have also been seriously involved in identifying and preventing risks. Some of this experience is distilled into my book, *Computer-Related Risks* (Reference 3).

In activities directly related to the computer-communication infrastructures, I was a coauthor of the 1988-90 National Research Council study report, *Computers at Risk* (Reference 2). Specifically addressing cryptography and its applications, I was a coauthor of a recent report on U.S. cryptography policy (Reference 8) and a member of the National Research Council committee (1994-96) study of U.S. cryptographic policy (Reference 9). I participated in an earlier study of the same subject sponsored by the ACM U.S. Policy Committee (USACM) (Reference 10).

Over the years, I have had several opportunities to consider the security needs of the FBI. From 1987 to 1989, I served on an expert panel for the House Judiciary Committee Subcommittee on Civil and Constitutional Rights, addressing law-enforcement database systems at the request of then Congressman Don Edwards. In 1991, at the request of Al Bayse, then Deputy Director of the FBI, I wrote a report on security requirements in the use of the national (NCIC), state, and local databases (Reference 14). In addition, the SRI Computer Science Laboratory had an ongoing project to study the application of our

technology for misuse and anomaly detection ("intrusion detection") to FBI internal applications. The most recent incarnation of that technology is summarized in Reference 15, describing our ongoing work for DARPA.

I am a Fellow of the American Association for the Advancement of Science, the Institute for Electrical and Electronics Engineers, and the Association for Computing (ACM). My present title is Principal Scientist in the Computer Science Laboratory at SRI International (not-for-profit, formerly Stanford Research Institute), where I have been since 1971 -- after ten years at Bell Telephone Laboratories in Murray Hill, New Jersey. I have doctorates from Harvard and the Technische Hochschule, Darmstadt, Germany (the latter obtained while I was on a Fulbright from 1958 to 1960). I am a member of the ACM USACM committee, chairman of the ACM Committee on Computers and Public Policy, and Moderator of its widely read Internet *Risks Forum* comp.risks), available by subscription at risks-request@CSL.sri.com, and archived with a lovely search engine at http://catless.ncl.ac.uk/Risks .

Illustrative Risks -- A Few Excerpts

Peter G. Neumann

This is a summary of just a few items from my archives related to risks arising in our use of computer and communication technologies, excerpted from my ongoing compendium index, Illustrative Risks to the Public in the Use of Computer Systems and Related Technology. Details on many of these items can be found in my book, *Computer-Related Risks*, and references to other are given in the full compendium index (Reference 11 of my 19 May 1998 testimony, http://ftp.csl.sri.com/pub/illustrative.PS). Peter G. Neumann, Computer Science Laboratory, SRI International, Menlo Park CA 94025-3493, 15 May 1998. Neumann@CSL.sri.com, http://www.csl.sri.com/neumann/

INFRASTRUCTURAL PROBLEMS

Telecommunications Infrastructure

- 1990 AT&T long-distance collapse.
- AT&T frame-relay network interruption. (both have the same basic propagation as in prior 1980 ARPAnet collapse!)
- SS7 outages due to faulty software patch.
- 4-hour #4 ESS closed 3 NY airports.
- Many local outages. Also, numerous outages of 911 emergency system, and some outages of 411 directory-service systems as well.

Computer-Communication Infrastructure

- 1980 ARPAnet collapse.
- 1986 severing of 7 trunk lines in one cable cut New England off from the ARPAnet.
- 1997 Internet black hole in routing tables cuts off 50,000 sites.
- Various Internet Service Provider outages.
- See below for computer-specific problems.

Commercial Aviation

- Various losses of planes attributable to avionics computer problems (KAL 901 altimetry in GPWS.
- Air New Zealand crash due to incorrect course data.
- Lauda Air thrust-reverser deployment in mid-air.
- Software flaw in 747/767 proximity switch suppressed?
- Northwest 255 computer failed to warn of unset flaps.
- China Air A300 due to complexity of the human interface.
- A330 Toulouse accident blamed on experimental software.
- Chinook helicopter engine software).

- Also many cases attributed to "pilot error" where computer systems were also involved (KAL 007.
- Air France A320 with safety controls off.
- Indian Airlines A320.
- French Air Inter A320.
- Cali crash where two different airports had the same codes.
- Ilyushin IL-114 crash.
- SAS MD-81 crash due to auto thrust problem.
- Numerous cases of air-traffic-control system outages, involving computers, telecommunications, power, radars, controller error, etc. You may recall major outages in Chicago, Oakland, Miami, Washington, Dallas-FortWorth, New York, Pittsburgh, etc. Causes very diverse. Local outages can have nation-wide implications.
- Recent case of a radar blip that caused Air Force One to disappear from screens.
- Ghost planes appearing on screens.
- Software problems with the development of TCAS, the collision avoidance system.
- Several mid-air collisions and near-misses (some not reported?)
- Missile over Wallops Island near American Airlines flight 1170.
- Spoofed air-traffic control: Miami masquerader, Roanoake Phantom, Manchester UK.
- Software development upgrades seriously problematical, especially the Air Route Traffic Control System, cancelled after many billions of dollars.
- The Denver baggage system is an example of a seriously delayed and cost-overrun development.

Nuclear Power

- Chernobyl experiment with emergency-shutdown recovery system -- related deaths now over 10,000, half million people contaminated.
- Three Mile Island.
- Considerable controversy over software reliability in the U.K.
- Electromagnetic interference has shutdown several plants.

Conventional Power

- Massive 1984 and 1996 Western power-grid outages computer related.
- October 1997 San Francisco outage blamed on sabotage.
- Los Angeles earthquake affected Pacific Northwest power.
- Prolonged Quebec outage due to ice accumulation.
- Various local outages due to squirrels, rats, etc.

Space (Extrastructural rather than infrastructural?)

- First launch of Columbia delayed by software synchronization bug.
- Voyager 2.
- Mir software problem.
- Mars Rover Pathfinder.

- Hubble software.
- Titan 34D, Nike Orion, Delta-178 failures. Titan 4 test-stand SRB explosion.
- Software flaws in Mariner 1, Gemini V, Atlas-Agena.
- Ariane 5 math error.
- Soviet Phobos 1, 2 problems.

Defense

- Patriot software problems, clock drift.
- USS Liberty warnings lost.
- Stark defense against Iraqi Exocets involved technology problems as well as officers.
- Thousands of false missile alerts (e.g., Stansfield Turner's book).
- Tomahawk cruise missile failures.
- Sgt York anti-aircraft gun software problems.
- Fantasy of Star Wars defense.
- Sea Harrier 1 auto-aim software bombed its own carrier.
- F-15s friendly-fire shootdown of U.S. Black Hawks over Iraq (human errors involved).
- 24% of our Gulf War deaths reportedly due to friendly fire.
- Iran Air 655 Airbus shot down by USS Vincennes (computer interface problem involved)

COMPUTER-COMMUNICATION SYSTEM PROBLEMS

Security Vulnerabilities

- Continual discovery of new security flaws in operating systems, Web browsers and servers, databases, networking, applications, programming languages, weak cryptography and poorly implemented cryptography.
- Security flaws offer rampant opportunities for penetrations, Trojan horses, viruses, misuse of many kinds, particularly in networked personal computers.
- The President's Commission suggests many vulnerabilities.
- The Eligible Receiver results indicate pervasive vulnerabilities.
- GSM security flaws. Electromagnetic interference on all sorts of systems, including aircraft controls, automobile systems, pacemakers and other medical systems.

Security Penetrations

- Cloverdale kids beak into Pentagon systems.
- Hackers claim major U.S. defense system cracked.
- Rome Lab breakins from Argentina.
- Websites altered by penetrators: Department of Justice, CIA, Air Force, NASA, among others, more recently the Army.
- Many intentional denials of service (e.g., on ISPs, flooding attacks), sabotage, blackmail.
- Cell-phone fraud, credit-card fraud, piracy, etc.

- Satellite uplink takeovers.

Security Misuse by Insiders

- Numerous cases, many not reported openly.
- Pinkerton $1M.
- Many misuses of law-enforcement, IRS, SSA, DMV, and other systems.

Accidental security leaks

- Sale or theft of used equipment often includes sensitive information!
- Software also often accidentally releases sensitive information.
- Newt Gingrich's phone call interception because of unprotected cell phone use.
- Unencrypted Secret Service pagers intercepted, despite demos of the vulnerabilities 3 years before at Hackers on Planet Earth. (These two cases suffered from the absence of any meaningful security.)
- Many privacy violations.

There are many other types of security problems. We enumerate just a few cases of a few types.

Year-2000 and Related Problems

- As of March 1998, only 35% of Federal Agency computer systems checked for Y2K compliance, with 3,500 systems remaining to be checked. The IRS is expected to spend a billion dollars. Worldwide estimates of the costs involved reach a trillion dollars, excluding lawsuits. Serious questions about effects on the aviation industry and the financial industry. There are serious risks associated with testing, for example if you set clocks ahead to see if there are any problems, you could have problems when you set the clocks back! There are also many recorded leap-year problems, summer-time conversion problems, and clocks expiring at various times because the clock field overflowed. For example, some GPS unit clocks will reset to January 1980 in August 1999. Overall, clock arithmetic is a problem, but the Y2K problem is unprecedented in its scope and pervasity.

Human Well-Being

- Health and safety: Risks in medical devices. Several deaths from Therac 25 software in therapeutic radiation device, also in Zaragoza Spain cancer mistreatment. Several deaths due to electromagnetic interference on pacemakers, also affects other medical equipment. Many privacy problems with health data.
- Other accidents and environmental risks: Exxon Valdez. New Orleans Bright Field crash. Three separate Willamette River raw sewage dumps blamed on computer systems. Numerous deaths and accidents due to malfunctioning robots. 1983 Colorado River flood due to computer faulty computer data and models. Union Carbide leak (after Bhopal) due to database error. Dutch chemical plant explosion due

to wrong input. Trawler Antares sunk by submarine -- computer showed separation of 3 miles. Numerous computer-related train crashes, even a few roller-coaster crashes. Automobile microprocessor software problems.

- Financial losses: Largest computer error in US banking history: $763.9 billion. Bank of New York overdraft of $32 billion due to program counter overflow. Many other cases.
- Financial frauds: Citibank penetration perpetrated from Russia. Many cases of computer-assisted bank and commerce frauds. Many cases of credit-card information being misused. Telephone fraud. Counterfeit pachinko cards ($588 million).
- Privacy: Massive incursions on personal privacy resulting from the ready availability of personal information. For example, Rebecca Schaeffer murdered by someone acquiring her address from the DMV; Arizona ex-law-enforcement officer tracked down and killed ex-girlfriend, using computer databases.
- Name and identity confusions: Many cases of false arrests and other inconveniences.
- Identity theft: A rapidly increasing problem, linked with increasing fraud and extensive inconvenience to the victims.
- Aggravation due to data errors and misinterpretation: IRS, law enforcement, Social Security Administration long-term underpayments, huge number of other cases.
- Spamming: Massive annoyance, but filtering is not an effective solution.
- Censorship: Very difficult to do sensibly, and often unconstitutional.
- Whistle-blowing: The shoot-the-messenger attitude prevails. There is a serious need for whistle-blowers, but there are also serious risks to those individuals.
- Elections: Many serious questions raised about computers used in elections, many irregularities, errors, reversed results, suspected frauds, lawsuits, etc.

TESTIMONY OF

L0PHT HEAVY INDUSTRIES

1. INTRODUCTION

Who We Are

For well over a decade, the members of the L0pht {Brian Oblivion, Weld Pond, Mudge, Space Rogue, John Tan, Kingpin, and Stefan von Neumann} have been involved with technology and security. Whether it was understanding how telephone switches operate, computers hook up to networks, or how math could be used to write 'secret messages' - we were and are driven by a need to understand our surroundings. Often times this new understanding leads us to figure out what things are capable of doing, not just what they were meant to do. Quite often this means tricking programs to bypass security. This can be something as innocuous as listening in to 'private' conversations all the way to the possibilities of stealing ones identity to commit crimes.

For the past four years the seven of us have been working together at a little "club-house" we affectionately refer to as the L0pht. This has come to be known as the top hacker collective in the United States.

One of the most intriguing aspects of the L0pht is the diversity of its technological savvy. Everything from satellite communications, smartcards, cryptography, operating systems, hacking, phreaking, networking protocols and high voltage electrical systems has a champion at the L0pht. Individual members have worked on or for DoD contracts, military field operations, large private sector firms, and federally-funded space agencies; performing, among other things, physical security audits, network security audits, and source code analysis.

The individuals, which make up this collective, have varying interests and backgrounds. Commercial sector computer security, computer and network administration, software programming, electronic engineering, hired hacking, and cryptanalysis are all Backgrounds that are present at the L0pht. From the standpoint of attacking hi-tech security mechanisms this works tremendously to our advantage. Currently the world is largely embracing software components as security solutions - which is fine as we have some of the top software engineers / reverse engineers. When smartcards and physical tokens become more mainstream, we are poised with a brilliant hardware group. Physical hi-tech security is very well covered as well. As the emphasis moves between hardware, software, and combinations of the two we are able to (and do) move with it - always attempting to remain at the epic. Perhaps this is why we have achieved respect both from the 'good-guys' and the 'bad-guys'.

Articles written by the L0pht or about the L0pht have appeared recently in or at www.microsoft.com, www.lotus.com, C|Net, Infoworld, EE-Times, Wired Magazine, LA Times, NY Times, Washington Post, BBC, LAN Times, Phrack Magazine, 2600 Magazine, New England Cable News, Byte Magazine, The Jim Lehrer News Hour, Information Week and many others.

The L0pht has issued at least 19 Security Advisories to the general network security community. These advisories have prompted several CERT advisories along with patches from Microsoft, Sun, FreeBSD, Cygnus (Kerberos), and BellCore.

Of course the question of why we even bother must be brought up, though it is not an easy question to answer. Perhaps an easier question to answer is what are not the reasons we do this. We are not involved in this for monetary gain as we provide our information to the public free of charge and end up paying any expenses out of our own pockets. We do not spend our time breaking, defeating, and researching hardware and. software to be appreciated by the industry. Often times companies become quite irate that we were able to show how weak their flagship product is. In fact, there are seven unique individuals who all have their own reasons for doing this. It largely boils down to the notion that if we can and do engage in this without any financial aid or backing and can find that the entire infrastructure is incredibly fragile, how can people as a whole be expected to trust and use this vehicle? Perhaps we would like to become the 'consumer reports' group that does not have any ties or alliances to the large corporations and simply publishes and benchmarks who is attempting to help the end user and who is selling snake oil. It has become apparent that such a non-biased organization does not currently exist. The following seven short paragraphs were composed by the individuals who make up the L0pht. It is hoped that this will shed insight into the dynamics and personality of the L0pht as a whole before we go into our observations on the current state of network and computer security.

Where We Came From

Brian Oblivion's involvement in the L0pht began in early 1992, when his wife, fed up the accumulated electronic test and computer equipment in the kitchen, demanded that it had to go. A "loft" space was acquired close-by and the equipment transferred. In order to defray the costs of the turn of the century warehouse, others were contacted on an intimate electronic bulletin board system (BBS) in the Boston area, the Black Crawling Systems. It began as a "storage locker" for excess equipment, but eventually a small lab was setup as well as an internal network, and that is when the research began. The actual L0pht was born in late 1993, when our Linux box [a personal computer running a UNIX'ish type operating system] went up on the Internet via a 28.8 link to a local Internet Service Provider. Brian Oblivion is the last surviving original member of those that procured the space in the South End of Boston. He has watched as a group of loosely organized individuals storing equipment in a warehouse, has turned into a highly organized security "watchdog" group. Struggling for existence, the group had to produce some products to keep the physical space alive while at the same time continuing the basic premise for why they do what they do: To have fun. Pushing the envelope, examining security systems and providing "Full Disclosure" to all of those in the Security Industry of our findings. Brian Oblivion concentrates on wireless and satellite communications networking technology and security. Being an Amateur Radio operator, he also supports the wonderful grassroots research and development capabilities of the United States and is a proponent of protecting the Amateur Radio Frequency bands from being annexed by the commercial sector. He is also a strong

advocate of the free unrestricted use of encryption technology, thereby raising the overall state of National Security. He hopes to be an influential member of the process to revisit the antiquated encryption export laws still in United States Code.

John Tan's involvement stemmed from encouragement in early childhood when teachers and other students recognized his technical talents. He found it easier to contribute to a team best by building knowledge and skill in as many areas as possible, with special focus on a few specific areas. Because his social involvement bridged both those labeled 'computer geeks' and the rest of school's societies, he earned the label 'hacker'; more so because he used the technologies around him to implement new and exciting ideas in the real world, surprising the mainstream with what the technologies could do. The L0pht maximized Tan's ability to implement new and exciting ideas by pooling his resources with the resources of 6 other enthusiasts who share equivalent 'knowledge space' but have different specialized areas of knowledge and resources themselves. Through the L0pht John Tan would like to see influence in industry and government as well as the media for sending a clear, consistent message to all parties as to where we as an electronic society are and where we need to go. Whether it's contributing technical savvy to a business environment, contributing to the various computer communities, being interviewed by the press or even invited to testify before the U.S. Senate, it really boils down to a matter of pride for John Tan.

Space Rogue brings several skills and abilities to the L0pht collective that are essential to survival. Along with strong technical skills coming from many years as a computer systems administrator with hardware service and maintenance responsibilities, Space Rogue brings real world experience stemming from 8 years duty in the Armed Forces. The calm, cool, demeanor is only pierced by bursts of excitement upon completing unusual hacks that cross most standard boundaries. To Space Rogue a successful hack ends up taking any number of forms - from sheer determination in finishing an arduous task to merging and combining data from disparate sectors of life and extrapolating new useful information all the way to technology reclamation. Privacy, freedom, and curiosity drive Space Rogue and are a common thread with his interactions amongst the other L0pht members.

Mudge started tinkering with computers in 1975. His father encouraged his learning and allowed him to travel down different routes without the stigmas of believing there are accepted versus unaccepted ways of looking at problems. He received degrees in music and has held positions varying from software development to code breaking for large organizations. Recently Mudge pointed out to the public several intrinsic problems with Microsoft's encryption, BellCore's One Time Password Authentication schemes, and the Kerberos authentication/encryption scheme. One of his strongest drives is knowing that the L0pht is attempting to keep information flowing and offering insight and knowledge back to the community that they were born from. The belief that individuals are still capable of impacting and helping to shape the future with regards to technology and legislation is very pronounced for him. A well respected computer security expert in his 'official day job', Mudge is a strong proponent of 'Full Disclosure' and the belief that shrouds of secrecy and corporate bureaucracy can be

pierced by logic and intellect, often time leaving large corporations caught with their pants down and championing the underdog. Much of this comes from the strong upbringing and background in the Unix operating system and the mentality that went into its creation.

After Weld Pond graduated from college with a degree in computer engineering he set off to work at a large software company in Cambridge. After a few years absence from the computer underground he decided to get back into the scene in his new home, Boston. He hooked up with a local computer underground BBS operator and a core group of talented hackers who had just formed the L0pht. To have a place tc go to physically work with other hackers was a new concept the L0pht was pioneering. It allowed for shared resources and an organization that permitted working on larger hacking projects together. There was a synergy between the hackers who had different expertise. Weld was hooked. By leveraging the expertise gathered working his day job on Microsoft Windows and web server programming Weld focused his sights on breaking software that he knew best. These were products such as the Windows NT operating system and Lotus' Notes (now named Domino) software. Several vulnerabilities were found and reported to the manufacturers and the Internet community so they could better protect themselves. Weld is also a licensed amateur radio operator who is interested in radio communication systems, especially those that use data transmissions. He also enjoys keeping up with the latest in encryption technology and is an avid cypherpunk, a member of the cypherpunks Internet mailing list.

As a member and resident of the L0pht, Stefan von Neumann draws upon and contributes to the collective's wealth of information and skill. He has 16 years experience hacking in such varied subjects as telephone communications, electronics, computer networking and hardware, and high-power systems. Stefan joined the L0pht in 1993 before L0pht had taken on its current role as an unofficial watchdog organization. He has investigated security flaws in software and hardware from Apple Computer, Inc. and has found flaws in the current system of distributing Internet data over cable television systems. He is currently most interested in and concerned with new communications media being developed. Digital communications are now sent over consumer-level cable television systems, radio-frequency broadcasts, infra-red light broadcasts, but are planned for transmission over electrical power distribution systems. Stefan is currently investigating whether these new transmission methods are vulnerable to exploitation.

Kingpin, the youngest of the seven, has been a member of the L0pht since 1993. His specialties include microprocessor and embedded system design, electronic physical security, smart cards, wireless data transmissions and low-level software design. From his younger days of exploring the telephones and other computer systems via modem, his interests have matured into the electronics and engineering fields. To Kingpin, the L0pht is a place to go to sit back and relax after a hard day, think about and experiment with new ideas and explore just about any obscure or new technology there is. The L0pht has not only kept Kingpin from illegitimate activities, it

has helped him focus his energy on positive projects. Kingpin's research topics vary quite often, as he prefers to explore the many facets of electronics and technology. Previous works include a POCSAG pager decoder, experiments with the insecurity of police mobile data terminals and surveillance/counter surveillance tools. Current research involves experimentation in eavesdropping and monitoring of stray electromagnetic fields from computer terminals.

Hackers Are Not The 'Bad Guys'

Computer Hackers are not, by default 'bad guys'. As with any group, especially a group with a large percentage of teenagers, there are trouble makers. But, in general, hackers are respectful of other people's rights. They do not cause damage for fun. We think hackers are a national resource that should be harnessed instead of harassed by law enforcement. Hackers have a 'can do' attitude.

We would consider most of the great inventors of our time, such as Thomas Edison and Alexander Graham Bell, hackers. They took what was available to them and made something work. This is basically what hackers do. The following example illustrates the difference between 'regular' software or hardware engineers and hackers.

During the Apollo 13 crisis the Houston ground team assembled to discuss how to abort the mission. The NASA man in charge was directing some questions to the Grumman engineer about the LEM and the Grumman engineers said, "That's not what it was designed to do." The NASA man said, "I don't care what it was designed to do. I want to know what it CAN do." They then hacked the functionality of the systems in ways that were never intended by the designers.

Why What We Have To Say Should Matter To You

Through our independent research and exploration we have found Internet and computer security to be almost non-existent. In many cases where devices and software/hardware are in place for security protection we have found that the components are either incorrectly set up or do not perform as advertised. Anyone can make a faulty computer program and sell it on the Internet as secure. If a car manufacturer did this they would be hauled off into court. With automobiles you are required to show some understanding and proficiency before you are given a license to drive. Off the shelf computer software is purchased and attached to the Internet all the time. Perhaps software manufacturers should be held accountable for robust products and possibly for educating customers in certain situations. We hope to touch upon some of our concerns and findings in the rest of this paper. We believe that our perspective is unique as it crosses the boundaries of good-guys versus bad-guys and instead looks at the situation with the ability to step back and take from both vantage points.

2. SOME OF OUR GENERAL FINDINGS

The Infrastructure Is Extremely Fragile

One of the core problems with the security and robustness of the Internet is that it was not designed to be bullet proof by today's standards. The underpinnings of the network protocols have been around for roughly 20 years now. A Tremendous amount of change has brought about new ideas and it is only logical to weld these additions on to the existing vehicle as opposed to scrapping the vehicle and starting over again. The problem comes from the weakness of the foundation. For instance, when the Army looked for a new jeep, they commissioned a design that started from the ground up and got the Humvee, a completely new and improved design. They did not take a Yugo and attempt to buttress any shortcomings. One instance of the infrastructure fragility, comes in the example that it would be trivial for one individual to knock the majority of the United States off of the Internet while remaining almost totally untraceable. We have been able to confirm this and several other attacks, in our own labs, that would make the Internet as a whole, unusable for as long as was desired. While the benefits of commerce over the Internet are clearly present, the simple fact that the Internet was not designed for this type of activity, should be kept in the minds of Corporate America.

Allow us to offer an example: In the matter of under 30 minutes, the seven individuals here could very trivially make the Internet unusable for the entire nation. Internet communication would be terminated between the US and all other countries, while internally none of the major backbone providers (MCI, AT&T, etc) would be able to route network traffic to each other [We have contributed these findings, along with many others, to the appropriate agencies]. Now throw into this example the notion that telephone switches, power grids, and other critical pieces of infrastructure are becoming more and more dependent upon the continued operation of the Internet. The fact that we, without funding or aid, have discovered several of these problems leads us to believe that others have found these and many more.

The Tower-To-Aircraft Insecurity

With the introduction of ACARS (Aircraft Communications Addressing and Reporting System) this decade, the problem of a phantom controller is amplified. A phantom controller, armed with a surplus transceiver capable of transmitting and receiving in the aircraft control frequency range, and a computer and interface capable of decoding the ACARS data streams which contain Latitude and Longitude of aircraft in flight, would have a greater ability to convince unsuspecting aircraft pilots of his validity.

Software and plans to build a decoder for ACARS transmissions are easily available to download off of the Internet. The software provides the user with the position of the aircraft in his area of operation, which is normally superimposed over a map of the local geographical area. Receiving the ACARS transmissions should not be considered a crime, nor should they necessarily be encrypted. Rather, to disable the

ability for a "phantom controller" to issue commands to pilots, a method of authentication of Tower-to-Aircraft communications is clearly needed.

The General State Of Security In Commercial Products Is Abysmal

Corporate America has decided to place tremendous importance and effort into conducting business over the Internet. At the same time it seems that they have placed extremely little effort into helping their customers with regards to liability and security (All the while marketing and advertising their products as "secure"). For instance, Microsoft held its head up and basically stated "use us as opposed to Unix [a non-Microsoft operating system] -- we're more secure as you can see since Unix has been around for 20 years and people have found problems with it over that timeframe. We are more secure than Unix because we are NOT Unix". As it turns out, not only did Microsoft have just as severe, if not more severe, security problems, but they showed the world that instead of looking at the competition and improving upon or fixing problems they saw, they simply reintroduced them. Those who do not learn from the past are forever doomed to repeat it could become Microsoft's new technological slogan. This is not due-diligence. How can people or companies expect to be secure when not only the foundation but all of the additions are fragile and weak.

The market place for products strictly addressing security is even more appalling. When pressed, many of these companies will reluctantly admit that they have no real world experience with computer security in their engineering departments. You have the equivalent of engineers designing home security systems without any knowledge of standard burglary M.O.'s. As an unknowing consumer, which the government agencies are as are all of the other consumers of these products, it does not even seem suspect that the alarms are only on the roof and not the doors or windows which have been installed in your house without locks.

One particular piece of software we looked at cost well over $30k per copy. It was supposed to catch hackers as they were breaking into a company. Unfortunately, we were able to show that even an attacker with very little understanding about computer security was able to trivially bypass the auditing system. In essence, it did not work in the real world.

We found a separate piece of software that was sold to help secure networked computers which ended up accidentally defeating the security of the system on it's own. The act of biting ones nose off to spite ones face is alarmingly common in this marketplace.

Independent, non-biased testing organizations are crucial. Everything to do with Microsoft is extremely biased because they wield so much power. This is a problem. It seems that only totally independent groups like the L0pht or individuals are willing to publicly stand up and shout "The emperor has no clothes" when it comes to looking at the approach to security in their products. Coopers & Lybrand wrote a security white paper on Windows NT saying how great it was. This is exactly what the industry does

not need. Ziff-Davis and the other computer centric magazines will not refute Microsoft claims no matter how outrageous they are. In some of our official 'day job' capacities, we have been asked by our employers to not go public with some of the problems that we have found for fear of losing the standing our employers currently have with Microsoft. This is not the route to more secure systems.

Time will determine whether or not current recommendations in the Report of the President's Commission on Critical Infrastructure Protection, October 1997, for a joint venture between the National Security Agency and the National Institute of Standards, will fill this void. This joint venture, recently announced as the National Information Assurance Partnership (NIAP) is to promote the development of objective criteria for testing and assessing the functionality and assurance of security technology and products. Tests, test methods, tools, security metrics and reference implementations will be produced and offered to private-sector laboratories to conduct investigations and produce certifications. We feel this is an admirable first step in creating an infrastructure to help police the products flooding the security market.

Example Of Large Auditing Firm Problems

So, should government agencies and others that are concerned about their computer and network security go to outside firms for external audits? Absolutely! However, there is still no way of knowing what you are paying for unless you already have the expertise in-house. The L0pht recently was given the opportunity to audit one of the larger network security auditing firms (which will be referred to as "Corp A"). Corp A had spent a relatively large sum of money and hired outside consultants to configure and install firewall software to protect their own company from the Internet. The software had been configured incorrectly and within the first day of the audit we had broken into their financial and development machines from the Internet. One week later we had control of every multi-user machine on their network. Even after this audit and presentation of the vulnerabilities, Corp A remains vulnerable to the same problems as they have chosen not to close the holes we pointed out to them. Corp A also continues to offer consulting and 'security' audits to corporations and agencies.

A second firm (which will be referred to as "Corp B") was contracted to perform a security audit on one of our employers. Being curious as to whether Corp B's services were valuable we were asked to perform the same audit against the same targets concurrently. Corp B handed our employers a clean bill of health while we handed our employers copies of all the sensitive data stored on the target machines. The attack we used to get into the systems was one of the first vulnerabilities any novice cracker would have attempted. Corp B did not find this hole yet claimed that they would attack the system as if they were the "hackers" that the company should be protecting itself against.

Example Of NASA / Pentagon Problems

The FBI, CIA, NSA, Pentagon, Lawrence Livermore National Labs, and NASA are just a few of the areas on the network that can and do attract cracker interest by name value alone. Agencies like NASA and various national laboratories have further problems based upon the open computing environment that has become part of their world. These open environments are usually born from academia. There is a tremendous amount of trust and sharing of information involved which becomes engrained in daily operations. When organizations that are steeped in these practices connect to public networks there is almost never any security in place worth mentioning. If security was attempted, many times the employees will either accidentally or purposefully thwart the security mechanisms in order to achieve the open trust model again. It is no big surprise, nor is it a difficult feat by any stretch of the imagination, that these organizations are broken into quite frequently and repeatedly. Yet, even without any technical merit or secret techniques, break-ins to LLNL and NASA will almost guarantee big press coverage.

Excusing organizations such as Universities, LLNL, and NASA, as research is their prime directive - not security, is almost [but not quite] understandable. What excuses do agencies such as the FBI, CIA, and NSA have for publicly connected systems that are not properly secured?

Computer intrusions into military computers connected to public networks are not new and the government has known about these problems for a long time but has not adequately responded. In 1991 during the Gulf War some crackers from the Netherlands penetrated 34 DoD sites. They obtained information related to personnel, logistics and weapon system development. The telling fact is that publicly know vulnerabilities were used to break into the systems. This information was given at Hearings before the Subcommittee on Government Information & Regulation, Committee on Governmental Affairs, United States Senate, 20 November 1991.

If a computer is broken into using a vulnerability that is publicly known then the person responsible for securing that system is not doing their job. All of the recent press "computer cracks" have been through known vulnerabilities. If the system manufacturer has released a workaround or a patch it should be installed on the vulnerable systems. If there is no fix it may be necessary to turn off some services or disconnect the machine from the network to protect it.

Manufacturers of software need to respond quickly to these known vulnerabilities, especially if they are touting their software as 'secure' as everyone seems to be these days.

Sometimes a system is broken into using a previously unknown vulnerability. There is really nothing a system administrator can do for this case except to badger the manufacturer of the software to test their products more thoroughly before selling them. The software industry is highly competitive and companies gain huge advantages to

being the first to market a particular feature. Unfortunately, quality and security can suffer in this time to market rush.

This raises an important issue now that DoD and other government agencies have decided to embrace 'off the shelf' software. They are now buying software that has reduced cost but may have many features that they don't need which could lead to security problems. The software could have been rushed to market. These 'hidden' security costs need to be accounted for.

Why Trust Models Do Not Work On The Internet

Trust between systems on the Internet is a very convenient way of facilitating work. In organizations it is often essential for productivity ; the R&D file server needs to trust the developers' machines as they are all contributing to the same project. It does not make sense for all of the individuals to be isolated into little pockets when they need to share their information with each other. This type of interaction is seen in the real world over and over. This was indeed how the Internet grew up.

However, without boundaries between groups that should have access to items and data and groups that should not - trust is extended indefinitely. As with any trust model you are only as strong as your weakest link. If person A trusts person B with a secret and person B trusts person C, person C will be able to learn person A's secret. Take this notion and throw several million people into it. Now, quickly point out which one of these millions of people is the weakest link. Not a very easy task, especially when several thousand are in the 'pretty weak' category to begin with. Welcome to the Internet as it is today.

How does one extend trust in secure fashions to remote offices that are only connected to each other over the Internet? What does the mobile or remote employee do? There are many cases where making a tight bubble around the group that needs to trust each other becomes quite difficult. It needs to happen but cannot and will not without education of end users and administrators.

Think about the following situation: A power company has their central power grid control and maintenance system remotely accessible to their field technicians. Since they have hundreds of field technicians they have one access account - 'maintenance' with a password of 'electric'. Trust has just been extended all across the area that the field technicians move throughout. If the system is connected to the Internet and the technicians access it that way then this notion of trust can be very dangerous. This does not even bring into play the lack of auditing, authentication, and non-repudiation. Do you think that nobody engages in activities like this? Federal Express uses this model for the lock combinations on their package 'drop-boxes'. It did not take the underground world long to learn this and take advantage of it.

It's Not Just That The Data Gets From Point A To Point B Safely

Many people still remember when families in the same area had 'party-line' phone service. If you needed to use the phone you would pick it up and listen to see if any of your neighbors were already utilizing the line. Out of common courtesy one was expected to hang up the phone if it was already in use. This is how large parts of the Internet operate. Computers share a common connection and look at the addresses on the data that go across. Each system has to examine at least the beginning of the data to see if it is intended for itself or someone else. If the data is intended for the machine that looked at it, the data is further examined in more detail. There is very little stopping systems from examining data not destined to them that traverses the shared media.

This problem has been known about since the beginning of the shared media implementation. One of the main routes that companies are taking in securing this is to protect the information as it travels from point-A to point-B. Encryption is being used to guarantee that others cannot look at information that is not intended for them while it is in transit. While this might protect a company from someone stealing credit cards as they are transmitted back and forth it misses a very important area: What happens to the information at the end-points. This becomes even more disturbing when one notices the false sense of security that is created. The buzz words of "it's safe because it's encrypted" seldom make us sleep well at night. Banks have strong vaults at the end points and then move their valuables back and forth in armored transports. People are currently being sold the notion that their information is safe because, through whatever add-on components, the armored transports can be used over the Internet. Nobody is being told the truth that the end-points the delivery goes between are paper bags - not vaults. In the cases where the encryption has been implemented correctly we have often found that the security around the final containers was woefully inadequate.

There Is No Independent / Non-Biased Organization To Watchdog The Claims Of Network Security Products

Software is totally different from other 'certified' products such as an automobile crash test. When you add a new tail light to a car the component is fairly isolated from the rest of the car. If it fails it usually does not make the car drive off the road or even stall. Software features, on the other hand, can cause catastrophic failures in completely different parts of a software system. Security component changes can have wide ranging effects because they are so central to operation of a computer system. You can crash test a model of a car and it doesn't matter what kind of radio it was purchased with or if they made minor changes to it. The crash test is still valid. Software that is certified cannot be modified AT ALL or it will need to be recertified.

Unlike a car, which only has a few configurations, software is almost infinitely configurable. There are many settings and services that can be enabled or setup in many ways. A slightly different configuration could have a huge security vulnerability where another may not. This means that not only does the underlying operating system or application software need to be certified but each unique computer system with its own unique configuration needs to be certified.

It is going to be very difficult to certify security in software but it must be done. Otherwise there is no way to know what you are buying and there is no liability on manufacturers. If you configure NT properly and someone still breaks in and disrupts your online commerce site Microsoft just says, "sorry". Even Kryptonite backs their bicycle locks with a warrantee to replace your bike up to $1000. The Kryptonite locks cost roughly $30, while corporations throw millions of dollars at Microsoft without any liability.

Certifying products is going to be expensive. It is also going to take time. There are only so many people who have the expertise to try to break software security. Certifying individual computer systems with their unique configurations can probably be done in an automated way with scanning software, but certifying the operating system or application software will take much more detailed human review.

Education Is Necessary

One of the prime missions of the computer underground is the spread of knowledge. Hackers proudly publish their discoveries: first on BBSs, then on Internet mailing lists , and now most often on our own web sites. The L0pht has always maintained a large online library for anyone to connect to and learn. The culture of learning as much as you can about different subject permeates the hacker culture.

Unfortunately the rest of society is not so enthused when it comes to learning about computer and communications security. Most people who operate these systems want to know the bare minimum it takes to do their jobs and nothing more. Currently, knowing little or nothing about computer security is the standard for people who operate these systems. Knowledge of computer security must become a requirement for people who connect any machine to a public network.

Nearly every part of society: individual citizens, libraries, schools, corporations, and federal, state, and local government are connected to the Internet now. Every part has resources they need to protect. The level of education for these different parts varies widely. Corporations or government agencies that have valuable resources to protect usually have some education when it comes to computer security but even here we have seen huge problems. Others usually have no education of the subject.

It is clear that more education is required but where will it come from? Manufacturers of software and computer systems is a good place to start. Just as a car owner's operating manual covers safety features and good operating practices, computer owner's manuals should do the same. Car manufacturers are held liable if features of their cars are hard to use correctly or if car owners are not warned properly about how to use them. If computer manufacturers were held to the same standards then they would have a vested interest in educating their users.

Educating individual users who may just use a personal computer at home on the Internet is important. Any computer connected to the Internet can be used by to attack

any other computer. This means that attackers can use other people's computers as 'stepping stones' to reach their final target. This gives the attacker more anonymity and power to direct an attack from several places at once. So not only can an individuals file's be stolen or destroyed but their computer could be used unwittingly in an attack of another system.

This is why everyone needs to be made aware of basic computer security procedures such as using strong, unguessable passwords, configuring their computers properly, and not becoming the victim of computer viruses.

It Is Not To Difficult To Raise The Bar

The objectives of any security effort should be to decrease risk to assets through application of security mechanisms. The level of security is most often determined by the cost to protect assets versus the value of said assets. Through this practicality, an industry has risen to address security by enabling the owners of computer systems via low cost, robust, unobtrusive solutions to the core problem areas in computer and network security. Application of these security technologies is key to the execution of a number of the components of a diligent security effort.

A security effort may consist of a wide range of in-house and out-sourced staff. Traditional computer and network security efforts range from models where the administrators bear a distributed responsibility for security with little or no guidance from management to organizations with a security department responsible for writing policies, education of users and management, administering users, vulnerability testing and administering firewalls. Some go further yet and have fully matured into organizations adding real-time intrusion detection and incident response capabilities to their arsenal. Security efforts at the classified level should potentially include an R&D effort, seeking out new attack methods, automating probes for identifying vulnerable systems, and fabricating a defense method potentially incorporating identification of the attacking system and/or a counter-attack.

Policies, standards and procedures will define the success of the security effort. Policies document the network owner's expectations and buy-in to the security effort. Standards and low level procedures will guide computer and network administrators in running a secure network. Together, this documentation may be used as a tool by the administrators to prevent insecure computing practices by the user community and vendors as well as other administrators. Upper management buy-in is essential for the enforcement of any of these important elements of a security effort, especially where computer based enforcement mechanisms are not available.

No security effort can expect to stop all attacks. A professional security effort should however, be able to fend off the "ankle-biters" who are simply using programs and scripts written to document and test for well known vulnerabilities in systems. If your system is penetrated by an ankle-biter, then the security effort at the organization

is being utilized as the problems being assessed or the findings are being ignored. There are a number of suppliers of vulnerability testing software. Several commercially available Network scanning tools will assess the security of a specified computer across the network. Such tools are effective for assessing the level of risk that individual machines might present against the novice or "ankle-biter" level of attackers. One must not get too confident about the results of these tools as they are not a panacea and different vendors' tools work better than others. Still, they are an excellent starting point in auditing your systems. Once inside a system, an intruder typically has only partial access to the system. The Information Security department needs to worry at this point about where the intruder can get to and what levels of access they can fool the system into giving them. There are several free software packages which we have found to work better than most of the commercial ones available that assess a computer from the "inside"; helping prevent an intruder from elevating their level of privilege once inside the system. Together, these two programs or ones like them may be used on a regularly scheduled cycle to help satisfy this component of the security effort. Even in places that are pursuing this form of due-diligence we all too often find that even though the tools might be in place to "raise-the-bar" the results are being ignored.

Before even attempting to assess the level of risk to a computer or network, there are some baseline measures which may be taken which work toward "raising the bar" so administrators are not over-whelmed after the first risk assessment. The single act of using encrypted communications to interactively communicate with Internet hosts takes away from many of the passive monitoring attacks. Another measure is to assure that all computers are "up to patch level" meaning, all software on all computers is the newest version with all the latest "fixes" from the company that wrote the software. This ends up being helpful in preventing older attacks but the administrator and administration must keep in mind that the patches out of the vendors are usually 6 months behind the date that the attackers know of the problem. In addition, this would not be as much of a problem if the vendors were producing more thoroughly tested and robust software from the beginning. Firewalls and other mechanisms which enable finer granularity of access control to be placed on components of the network and local file system access are essential, largely due to the lack of security measures in the existing infrastructure.

Once policies, secure computing mechanisms, and a risk assessment cycle are in place, an effort should be made to educate the users of the computers as to the policies that affect them. They should be provided with a publication of some sort documenting "appropriate use" of the computing facilities and their responsibilities with regard to the security of those facilities. The user community should then be assisted in adjusting to any necessary changes in behavior and periodically updated to changes and refreshed on important policies. Finally, the public must be educated so that it may, in an informed manner, endorse government initiatives to ensure security as well as governments response to incidents it encounters. Additionally, well trained administrators are essential in responding to the findings of a risk assessment. Administrators must not only be trained in their specific job function, but also must

understand security and secure computing practices as well as how to deal with threats and incidents.

The thought of intrusion detection is a sign of maturity in a security effort, even if many of the implementations for this are not adequate for the real world. Network intrusion detection will work best at the end nodes for many reasons, not the least of which is the different ways that end nodes handle data that is sent to them that cannot be inferred from a passive monitoring point in the middle of the network.

A truly mature and professional security effort will have a well defined series of incident response procedures in place. In the event of an intrusion, a well planned response will have a far better chance of yielding positive results. Ill conceived responses may reveal an immature security organization or turn a simple intruder into a malicious intruder. A well planned response will take into account the nature of the intrusion, the consequences or potential consequences, the originating state or country, the skill level and information available on the intrusion among other things. Procedures, scripts and templates should be put into place with legal council to assure a consistent, predictable response to incidents. Just like car alarms and car thieves, if someone really wants to steal your car they will be able to. However, if they are just looking for an easy mark they will walk to the next car that does not have an alarm installed. Similarly if your company achieves a reputation for going after attackers then the word will spread and attackers will look for easier marks.

For an administrator to respond to newly discovered vulnerabilities, the administrator must understand the attack method and decide for themselves how to defend against it. Regardless of the availability of a "fix" from the vendor, the vulnerability exists and must be defended against once identified. Any clearinghouse for computer security information must fully disclose all information pertinent to a vulnerability within a short time of its discovery. Vendors and "old-boy" networks of information exchange alone do not work. Vendors should be given advanced notice to prepare a "fix" but must not delay the timely announcement of the vulnerability to the consumers affected. A detailed description of the attack is necessary for administrators to decide best how to protect themselves from the threat. This is especially essential when there is no vendor provided "fix" available. This particular approach is what has earned the L0pht its reputation. We have provided a valuable service to systems administrators over the last four years where others have consistently failed to provide that value.

By applying these technologies in a meaningful way, network administrators may "raise the bar", fending off the ankle-biters in an automatic fashion, allowing them to concentrate their efforts on being proactive and responding to the serious threats as they arise. This is key to the success of the success of the security effort. By achieving such a baseline of security, public confidence is increased as the majority of attacks are thwarted and those that are successful illicit a meaningful response. Again, the technologies are readily available and are even low cost or in many cases free. When proper policies, education and incident response are not in place however, the

implementation of the technologies will fail. Unfortunately these are the components of the security effort that you can not buy; you have to build them.

3. WHAT WE WOULD LIKE TO SEE HAPPEN

Understanding Of The New Threat Model

It sure seems as though the era of 'our hardware' versus their hardware', our software' versus 'their software', and 'us' versus 'them' has faded into the background. Our hardware is the same Intel/AMD/Motorola/Sparc processors as theirs is. We all run the same operating systems and the 'us' versus 'them' has been replaced with 'us' referring to the government and 'them' now being 3 billion people with Internet access and no geographical or profound political boundaries. Now the government has to contend with a new threat that contains no cold hard boundaries.

How does the government turn it's eyes inward on the people it is sworn to protect and in many cases not legally allowed to watch. Does big brother rear it's ugly head, or is McCarthyism to come back en vogue? Neither of these options will work. Neither will the key escrow that the government is attempting to push for.

From a defensive standpoint the playing field needs to be raised to the level where auditing and accounting mechanisms are robust enough and the tools you are attempting to protect become reliable enough that even when someone attacks you it is instantly obvious and detectable.

Offensive standpoints should be looked at from various angles remembering that crippling or weakening the common components only ends up penalizing the legitimate users.

Understanding Of Severity / Skill Level Of Attacks

The media has been largely atrocious in their understanding of hi-tech attacks. When a street thug shoots and kills somebody you seldom see the press jump up and say 'brilliant misfit who understands spontaneous combustion and projectile ballistics kills teen'. Did the street thug understand the chemical reaction that was happening when the hammer of the gun made contact with the bullet in the chamber? Probably not. Yet every time a machine is 'cracked' on the network the media jumps up and praises the misunderstood "brilliant child". Yes, there are some very ingenious hacks and hackers out there on the net, the same way that people who invented guns and gunpowder were very bright. The few ingenious hackers out there might put together a program that demonstrates a flaw or vulnerability ; this does not mean that everyone who follows the cookie cutter instructions and executes the program is at the same level. Much the way that everyone who pulls the trigger of a loaded gun does not necessarily understand trajectories, velocity, and combustion. With the sensationalism attached to largely trivial attacks there is no surprise that more and more people will

want to, and be able to, cash in on their 15 minutes of fame by going after high profile targets. We don't believe these particular people should be feared nor do we feel that harsh repercussions are appropriate. If the gun analogy was in use this would be a situation where it is easy enough to provide all people with bullet proof vests that are unseen and always worn. The people you would not be protected against are at a much higher level. The point is that these people would now be the minority. The majority of the problem would be addressed and that is a great start.

Yes, there are people out there that are amazingly adept and technically skilled. You will not see the media talking about them. Our government has them as do other governments [along with plenty just being out there on their own]. You will not be able to keep these people out in most situations. If the L0pht had to or wanted to achieve access to a computer on a network badly enough we could and would. The difference is being able to differentiate between the real concerted and skilled attacks and the noise level created by all of the joy riders and door knob turners.

Willingness Of Corporations To Consider Security Aspects From Product Inception As Opposed To 'Afterthought'

Just as in any engineering project such as building a car or a building, the earlier in the process that critical features are designed in, the better the end product. It is cheaper to build and it works better. Just like a car sunroof that is not installed in the factory sometimes leaks, security patched onto an operating system after the fact can also leak.

Security needs to be thought about and designed into software or communication systems at the very beginning of the design process. It is cheaper in the long run for manufacturers to do it this way but market pressures usually force a short term mentality. They think that if a problem is discovered they will patch it later. The problem with this is that computers may lie vulnerable to attack until the manufacturer is notified of a problem and then fixes it.

The L0pht always makes its security vulnerabilities public but there are many people and organizations in the world that do not do this. They keep secret the flaws they have found and use them in attacks knowing that they will always succeed. If manufacturers keep up with the 'ship it and patch it later' mentality then the unpublished vulnerability is always going to be a risk.

Security must be designed into the initial architecture of the computer and communications systems by people educated in good security design. Then as the product is built security code reviews must be done by security experts on the software's source code. Finally extensive testing must be done to see if the system can withstand attacks. The earlier problems are found in the development process the cheaper it is to fix and the better the end result. Problems found after a system is deployed can have severe consequences to the users of those systems.

Use Of Authentication And Encryption

For some time now, Authentication has been in use within governmental and military telecommunications systems. However, authentication has been lax in sensitive utility, financial, law enforcement, and medical communities. For example, medical records, when transferred from one site to another should be encrypted when sent over an unsecured channel such as the Internet. However, an agency wide change in policy that is to be received by many individuals would be better served by authentication.

One should authenticate almost always where time and resources exist. Encryption should be used when the content of the transmission is sensitive or of a compromising nature and usually intended for one recipient. Authentication should be employed if the information within the transmission is common or to be received by many recipients.

The L0pht recommends that a plan to implement Authentication in Law Enforcement (National and State agencies) and National Infrastructure Communications system be employed in dispatch communications to prevent the transmission of unauthorized commands over the radio channel, while encryption should continue to be used to protect sensitive tactical operations.

The amount of radio and data communications equipment in the surplus markets coupled by inexpensive powerful computers, renders the ability for non-trusted parties to monitor and participate on digital communication channels relatively easy. This statement alone defines the requirement for authentication systems like those currently used in the military arena, to be transferred into commercial and public two-way communications systems.

Whether to use authentication or encryption depends on the sensitive nature of the transmission and the intended audience. The location of aircraft and air traffic control is useful to many agencies that do not necessarily need to transmit to control towers. There is actually no need to encrypt air traffic control communications. Rather, you want to be sure that an instruction from the Control tower is indeed from that source. Hence the control tower should authenticate its transmissions to the aircraft in the area.

Complete encryption of radio dispatch communications is counter-productive as many civil and local organizations utilize these communications during environmental and national emergencies. Amateur Radio operators use these communications to better coordinate relief assistance and provide emergency communications when traditional methods are disabled. It is important to not alienate these resources.

POCSAG, RDLAP, ARDIS, FLEX, MDC4800, AX25, CDPD and a host of other communications should be encrypted. These are private communications protocols intended only for the recipient. You don't want people viewing NCIC records being

transmitted from the Police Head-end to the patrol car. You don't want people pulling peoples identities, birth dates and social security information out of the air. More and more automated computer security systems page System Administrators when an intruder is detected or when a system resource is failing. Shipping manifests can be pulled out of the air by eavesdropping on the wireless digital transmissions from PDA's (Personal Digital Assistants) in ship and train yards.

The "security" on many of the wireless transmission services are practically non-existent. In the case of paging services, the POCSAG, FLEX and GOLAY signals are all sent in a clear text, non-encrypted form. This allows for any radio enthusiast, with a handful of off-the-shelf electronic components, to receive these transmissions which might contain sensitive information. Take the case, for example, of the person who intercepted (and subsequently released publicly) the paging traffic related to one of President Bill Clinton's trips. Information within these paging transmissions involved where and when President Clinton's airplane would be landing, where to pick up associates, and the overall movements and actions of the travelling party.

The mobile data terminals, terminals used in the police cars to transmit and receive criminal records, warrant information and license plate information, are another case of clear text data transmissions. Using the same electronic components mentioned above, one can easily intercept the transmissions from the police station "base" to the police car and vice versa. By doing so, one receives various information related to the NCIC database, identities, birth dates, addresses, social security information, and car and license plate information. It is also trivial task to not only intercept this traffic, but generate your own radio transmissions, spoof authentication, and gain access to these same databases from the comfort of your own home.

Sensitive information, such as mentioned above, should be encrypted. The transmission methods of police departments around the country are still plain text and only a handful of police departments have upgraded to a more secure digital transmission method.

One should never put inherent trust into a transmission medium just because it is uncommon. New transmission methods are being hailed as "Secure" when they are not. Over and over you hear claims that Spread Spectrum systems are inherently secure because of they way they "spread" the spectral density of a transmission over an area of the frequency spectrum. A frequency hopping system transmits a portion of the message on a frequency and then jumps to the next frequency, transmits a portion, then jumps to the next frequency, ad nauseam. These systems have been used for the past 30 years in the military sector and many papers on how to intercept and jam these communications methods are available publicly. Governments and commercial endeavors alike think individuals with mal-intent are stupid and do not read the research papers put out by the IEEE, CTIA, and academia. We beg to differ. They are out there and they read these materials.

There are two major reasons the United States telecommunications and communication manufacturers do not secure their networks:

1. They are under pressure from Law Enforcement to provide a backdoor (key escrow) into their crypto system, and to be financially responsible to provide this back door, into their crypto system. This makes their system undesirable for export because other countries do not want the United States to potentially have a back door into their communications infrastructure.

2. They cannot export strong cryptographic systems overseas due to restrictive United States crypto export policy.

These two factors, in our opinion, are large contributors to the lack of security in the National Information Infrastructure.

Change In Current Legislation

Enabling restrictive laws such as the Cellular Telephone Protection Act will lead to a slippery slope. The CAUSE of the problem needs to be treated, not the EFFECT. Upgrading the cellular telephone system to use an encrypted digital transmission method will remove, at least temporarily, the problems of cellular phone cloning and fraud, as well as ensure privacy between the two communicating parties Prohibiting citizens from using a scanning receiver simply will not rid the problem, merely hide it.

The L0pht finds that The Cellular Telephone Protection Act (S.493) does nothing to solve problems and criminalizes many law abiding citizens. Unneeded legislation banning the sale of scanning receivers that can receive the cellular bands does nothing to stop the fraud and abuse that plagues the Cellular industry. The problem is the data channels used to recognize a valid phone are transmitted "in the clear" which allows cellular pirates to snatch valid cellular telephone identification credentials to create cloned phones. Simple data scrambling would hinder the cellular pirate industry while strong encryption would eliminate the problem of stealing the information from the air entirely.

On the subject of listening to the conversations, tone masking or time element scrambling, or a host of digital scrambling methods, could be easily employed which would hinder the enthusiast, while again, encrypting the speech channel would eliminate the problem of the ordinary citizen, the criminal, and the federal government from monitoring private cellular communications. Hopefully technology resulting from the NSA's Operation CONDOR to provide secure communications to Government, Military, and Law Enforcement officials will eventually trickle down into the commercial markets.

Some recent changes to the Cellular Telephone Protection Act make having in your possession a receiver capable of receiving the cellular band, a cellular phone, and

software to change the identity of a cellular phone illegal. Thereby criminalizing individuals that legitimately would like to reprogram their own telephone with the identity of another phone they currently own. It is the equivalent of wiring an additional telephone into your home. Instead of making it difficult for criminals to extract the information anonymously over the air, possession of legitimate equipment and software is made a crime.

The L0pht also recommends the relaxation of crypto export laws to empower United States software security industry. On the issue of research into key recovery systems, we feel that this research is very important an should continue, HOWEVER, the resultant technology should allow data warehouses, companies and private citizens to access their protected information in the event of key loss. The Escrowed key would remain in the possession of the owner of the information, not a third party. This cannot continue to happen.

Incentives

Many computer and communications manufacturers wash their hands of any liability if their product fails. No where is this more prevalent than with software manufacturers. Since software is not legally owned, but license to the end user, software manufacturers are able to craft up an extremely restrictive license agreement which give the end user no rights. If the software completely fails usually you have no recourse except a refund. This is very different than most products where the manufacturers are liable for the damages their products cause.

Software should be held to a higher standard than it is now. Users should demand better licenses. If companies were liable for product failure then they would have incentive to design security into their products earlier, to test the security features better, and to educate their users.

We appreciate the opportunity to share our viewpoints in this forum and hope they were in some way beneficial and helpful.

Responses to Questions from L0pht Heavy Industries

Senators Thompson, Glenn, Collins, Lieberman, other members of the committee:

In response to the questions asked and the issues raised during our testimony May 19, we have drafted suggestions and a plan of action we believe would help government, businesses and citizens alike.

The Committee asked, "What, as lawmakers, can we do through legislation to identify these problems?" Our answers are difficult ones: in some cases not easy to implement, in other cases difficult to convince the businesses and the general public that these plans are worthwhile.

As an example of how the public will find these suggestions difficult to accept, you need only look to the media and their interpretation of our testimony to you. The media is prejudiced against people who wear the hacker badge of honor. This is slowly turning, as people such as ourselves come forward to share our knowledge on computer system vulnerabilities. For others in our shoes, the prejudice makes it difficult to come forward because they are viewed not as "computer experts" but as "hackers boasting their prowess". The so-called "experts" are greeted with respect even though their relationship with the media is often profit motivated, while hackers are looked down upon because of their unorthodox style of learning and exploring computer systems with no personal profit motive.

This problem, simply stated, exists because the public gets their information from the media. Only the sensational phrases of our testimony were mentioned by the media and they did not understand the critical nature of the Senate hearing. In order to correctly educate both the Government and the public, one needs an unbiased source of information. If such an agency is "for profit" or externally funded by major organizations, you can be quite certain of a twisted or biased view on the facts.

We call on the media to report on the vast majority of hackers that are not involved in criminal activities, and treat them with the respect that their expertise deserves. The media will find that there is a wealth of information out in the hacker community. It can serve as an opposing view to those of the marketing organizations of major corporations and the views of non-hacker computer experts.

Suggestions

Our first suggestion targets the liability, or lack thereof, of the software manufacturers / developers / publishers. Currently there are no means to pursue legal action even in the case of a most grievous failing to ensure security in software. Standard software licensing relieves the manufacturer of any and all responsibility for their own product's fitness. If Microsoft, to use the most well-known software company as an example, could be targeted by lawsuit for failing to protect their own customers' best interests of computer security, we have no doubt that they would within a short period of time fortify their software products against security flaws. Perhaps more importantly, they would be pressed to make notice in a timely manner to their customers of issues affecting the security and stability of the customers' computer systems. A legal responsibility to inform the software customer of a vulnerability would be a tremendous step forward towards educating the user, eliminating the biggest source of security holes other than the software itself.

This protection should exist under the UCC. Software licensees should not be forced to waive basic commerce rights by breaking the shrink-wrap on a store bought software package. Currently when software fails or is defective, retailers will not accept the software back for a refund, even though according to the software license agreement this is the consumers' only recourse. We have a system under which one can't even get money back for a product that fails to perform as the software manufacturer advertises.

Another problem is the lack of diversity in the operating system software market. Adversaries will always target their research toward finding vulnerabilities in the most popular operating system. If everyone used the same computer operating system, and a serious defect was found by an adversary of the US, a majority of businesses and government computers could be disrupted by exploiting just one defect. A survey of the top twelve Intel-processor-based PC manufacturers found that all twelve would not install any other operating system than Microsoft Windows.

As we stated in our initial written testimony, independent, non-biased testing organizations are crucial. In the current state of marketing hype, there is no method for testing and evaluating software by truly disinterested parties. We suggest a scenario in which any and all software for use on public networks is submitted for testing by an organization similar to both Underwriter's Laboratories and Consumer Reports. Even if a "small" change is made to a software product or package, it should be resubmitted for full evaluation. Unlike a car crash-safety test that need not be repeated if the design of the radio is changed, software must undergo thorough evaluation if any change is made, no matter how insignificant the developer may claim the change to be. Any change to software source code can open up a major security vulnerability or software bug. Unlike the current ICSA (International Computer Security Association, formerly CERT) process, software must NOT inherit approval in the version 2 incarnation simply because version 1 did pass the tests. Further, software "source code" must be made available to this independent testing agency. To test software without the source code being made available is akin to crash testing an automobile without being able to look under the hood before the test and unable to look inside the wreckage after the test. Without source code, the underlying poor design and possible design flaws would not be known. We do acknowledge the need for confidentiality within such a future testing organization; keeping the source code out of the public eye is essential for a publisher's business. That notwithstanding, there should be legislation similar to that for the auto industry that ensures and requires proper testing in both controlled and real-world conditions.

The objective of an "air gap" method of isolation should be enforced in control networks and systems of utility companies. In the same way that the military maintains a physical gap between private, classified networks and public, Internet networks, utility companies should establish hard breaks between private control channels and publicly accessible paths. There should be no system, no matter how seemingly innocuous, that should bridge between. Further, utility companies should undergo the same type of review process as the Federal Aviation Administration applies to air traffic control. Water, telephone and electricity service should be under as much scrutiny as airlines, automobiles and railroads; there is an equal potential for disaster amongst them all. Internet service providers should also share the requirement for isolated control systems, and should have "hardened" physical facilities, much like the phone company switching centers are strengthened to protect from malicious physical attacks. Internet providers now are commonly located in low security office buildings.

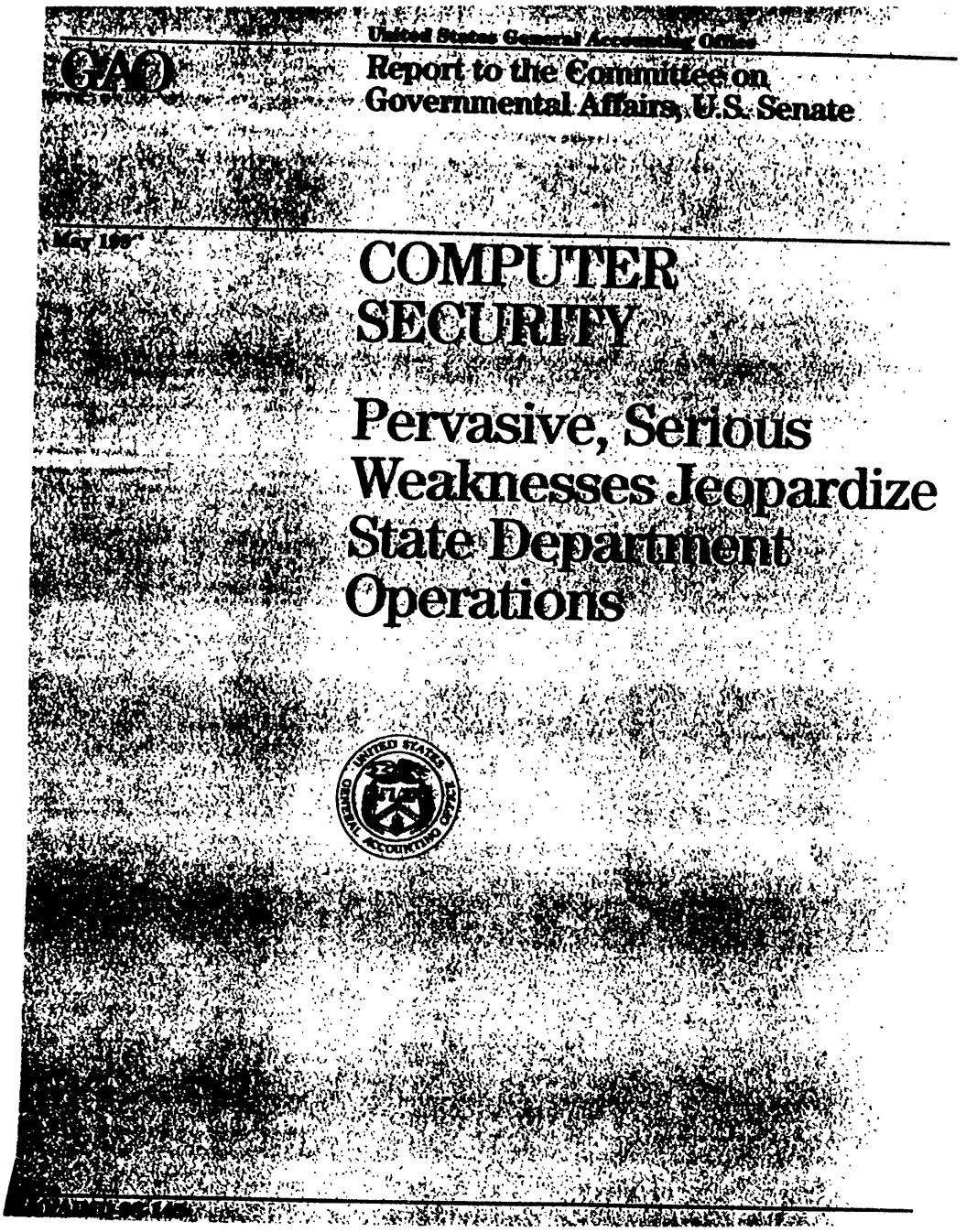
While perhaps in 1998 there is not an immediate risk of fatalities if there is a failure of the public Internet or private data networks, there is currently the risk of economic chaos with so much of our economy relying on electronic activity. If Internet providers and other data carriers were also forced to maintain separate control circuits for their networks, the opportunities for malicious damage would be lessened.

Finally, encryption and authentication mechanisms must be made not only legal for any use, but must be required. Simply put, one of the greatest challenges now in data systems is proving one's identity in an irrefutable manner. The "phantom controller" that interfered with airline traffic would not have been successful if airlines used rudimentary cryptographic authentication. Tracing the source of an attack on Internet systems could be done quickly and easily if there were similar authentication. The next version of the Internet Protocol, known as IPv6, will contain an option for such authentication. We suggest that IPv6 be made a mandatory upgrade for all public networks and systems, just as seat belts and air bags are now required in automobiles. A counterpart to the use of stronger authentication in network protocols is filtering that must be done by Internet providers and data carriers. In the same way that the Postal Service could reject a letter that was traveling through a California post office despite a return address and destination address both being on the East Coast, Internet providers could easily implement filters that discard obviously improper, suspicious data transmissions. This type of filtering would stop many denial-of-service attacks, which usually employ "spoofing", a well-known method of hiding attacks. Coupled with authentication of the source, these two changes would vastly improve the security and reliability of both the public Internet and private networks.

We suggest that the dialog we have entered into with your committee be only the beginning of a further relationship between the government and the hacker community. We have been very fortunate to contribute our experience and expertise in a constructive manner; we're certain there are other hacker groups and individuals that would follow suit.

Thank you again for the opportunity to speak before you.

L0pht Heavy Industries
Brian Oblivion
Weld Pond
Mudge
Space Rogue
John Tan
Kingpin
Stefan von Neumann



GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-279842

May 18, 1998

The Honorable Fred Thompson
Chairman
The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

As a result of rapid growth in computer technology, the Department of State, like other governmental and private sector entities, has become extremely dependent on automated information systems. Much of the data stored and processed on these systems is critical to operations involving foreign affairs, economic and commercial matters, and scientific and technological issues.

Given the sensitive[1] nature of this information and its importance to our national welfare, you asked us to determine how susceptible the State Department's unclassified automated information systems are to unauthorized access, identify what the State Department is doing to address information security issues, and determine what additional actions may be needed. We issued a classified report to you detailing the results of our review in March 1998. This is an unclassified version of that report. It summarizes the problems State faces in securing its information systems, the steps State has underway to address problems, and our recommendations for additional actions.

Results in Brief

State's information systems and the information contained within them are vulnerable to access, change, disclosure, disruption or even denial of service by unauthorized individuals. We conducted penetration tests to determine how susceptible State's systems are to unauthorized access and found that we were able to access sensitive information. In addition, we could have performed system administration actions that would have allowed us to download, delete, and modify these data, add new data, shut down servers,[2] and monitor network traffic. Moreover, our penetration of

[1]According to the Computer Security Act of 1987 (Public Law 100-235), sensitive information is "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled" under the Privacy Act of 1974, as amended. The Privacy Act requires federal agencies to keep personal information about individuals confidential.

[2]Servers are network computers that perform selected processing operations for computer users on a network.

State's computer resources went largely undetected, further underscoring the department's serious vulnerability.

The results of our tests show that individuals or organizations seeking to damage State operations, commit terrorism, or obtain financial gain could possibly exploit the department's information security weaknesses. For example, by accessing State's systems, an individual could obtain sensitive information on State's administrative processes and key business processes including diplomatic negotiations and agreements.

Although State has some projects underway to improve security of its information systems and help protect sensitive information, it does not have a security program that allows State officials to comprehensively manage the risks associated with the department's operations. First, State lacks a central focal point for overseeing and coordinating security activities. Second, State does not routinely perform risk assessments to protect its sensitive information based on its sensitivity, criticality, and value. Third, the department's primary information security policy document is incomplete. Fourth, State is not adequately ensuring that computer users are fully aware of the risks and responsibilities of protecting sensitive information. Fifth, the department lacks key controls for monitoring and evaluating the effectiveness of its security programs and it has not established a robust incident response capability.

Clearly, State needs to greatly accelerate its efforts and address these serious information security weaknesses. However, to date, its top managers have not demonstrated that they are committed to doing so. For example, despite reporting mainframe computer security as a significant weakness confronting the agency to the Congress and the President since 1987, managers have not yet developed a comprehensive security plan or ensured that adequate resources are devoted to strengthening controls and ensuring that they remain effective on a continuing basis.

Internet security was the only area in which we found that State's controls were currently adequate. However, plans to expand its Internet usage will create new security risks. State conducted an analysis of the risks involved with using Internet more extensively, but has not yet decided how to address the security risks of additional external connectivity or the concerns this review raised. If State increases its Internet use before instituting a comprehensive security program and addresses the additional vulnerabilities unique to the Internet, it will unnecessarily increase the risks of unauthorized access to its systems and information.

Background

State relies on a variety of decentralized information systems and networks to help it carry out its responsibilities and support business functions, such as personnel, financial management, medical, visas, passports, and diplomatic agreements and communications. The data stored in these systems is sensitive enough to be attractive targets for individuals and organizations seeking monetary gain or desiring to learn about or damage State operations. For example, much of this information deals with State employees and includes American and Foreign Service National personnel records, employee and retiree pay data, and private health records. Background investigation information about employees being considered for security clearances is also processed on State's unclassified network as is sensitive financial and procurement information.

The potential consequences of misuse of this information are of major concern. For example, unauthorized deletion or alteration of data could enable dangerous individuals to enter the United States. In addition, personnel information concerning approximately 35,000 State employees could be useful to foreign governments wishing to build personality profiles on selected employees. Further, manipulation of financial data could result in over- or underpayments to vendors, banks, and individuals, and inaccurate information being provided to agency managers and the Congress.

Objectives, Scope, and Methodology

Our objectives were to (1) determine how susceptible the State Department's automated information systems are to unauthorized access, (2) identify what the State Department is doing to address information security issues, and (3) determine what additional actions may be needed. To determine how susceptible State's systems are to unauthorized access, we tested the department's technical and physical controls for ensuring that data, systems, and facilities were protected from unauthorized access. We tested the operation of these controls to determine whether they existed and were operating effectively. We contracted with a major public accounting firm to assist in our evaluation and testing of these controls. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported. During our testing, we performed controlled penetration attacks at dial-in access points, the department's Internet gateways, and public information servers. We also performed penetration activities to access security controls on State's

major internal networks. In addition, we performed social engineering[3] activities to assess user awareness, and attempted to gain physical access to two State facilities.

We attempted to access State's sensitive data and programs under conditions negotiated with State Department officials known as "rules of engagement." These rules were developed to assist us in obtaining access to State's facilities and information resources and to prevent damage to any systems or sensitive information. Under the rules, all testing was required to take place within the department's headquarters building between 8:00 a.m. and 10:00 p.m. and was physically monitored by State employees and contractor personnel. In addition, State monitors were authorized to stop our testing when we obtained access to sensitive information or systems. We were also required to inform State personnel about the types of tests we planned to conduct prior to the testing. As agreed with State, we limited the scope of our testing to unclassified systems.

To identify what State is doing to address the issue of unauthorized access to its information systems, we discussed with department officials their efforts to protect these systems and reviewed supporting documentation. For example, we obtained information on the department's initiatives to improve the security of its mainframe computers and establish a centrally managed information system security officer program at headquarters. We also discussed with department officials preliminary plans to expand the use of the Internet and reviewed supporting documentation. We reviewed numerous evaluations of information security at domestic State locations and foreign posts performed by the department's Bureau of Diplomatic Security. We reviewed recent reports submitted by State to the President and the Congress under provisions of the 1982 Federal Managers' Financial Integrity Act,[4] which outlined known information management and technology weaknesses and plans for corrective actions. We reviewed the department's policy guidance on information security as contained in the Foreign Affairs Manual, Volume 1 and Volume 12, Chapter 600, and its Fiscal Year 1997-2001 Strategic and Performance Management Plan for Information Resources Management. We visited a computer security

[3]Social engineering is a technique commonly used by attackers to bypass an organization's existing physical and logical security controls to gain unauthorized access to systems, networks, and resources by relying on information provided by naive, poorly trained, and well intended organizational personnel.

[4]The Financial Managers' Financial Integrity Act requires that the head of each executive agency provide an annual statement to the President and the Congress stating whether the systems of internal accounting and administrative control fully comply with standards issued by the Comptroller General.

assessment center in Fairfax, Virginia, which the department uses primarily for certifying and accrediting software to be used on State information systems.

To evaluate State's security program management and formulate recommendations for improvement, we compared State's practices to guidelines in two National Institute of Standards and Technology (NIST) publications, the "Generally Accepted Principles and Practices for Securing Information Technology Systems" and "An Introduction to Computer Security: The NIST Handbook," as well as other guides and textbooks. In addition, we reviewed a Department of State Inspector General report on unclassified mainframe systems security. We also relied on our work to identify the best information security management practices of non-federal organizations which is presented in our Executive Guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-21 Exposure Draft, November 1997). The guide identifies key elements of an effective information security program and practices which eight leading nonfederal organizations have adopted and details the management techniques these leading organizations use to build information security controls and awareness into their operations.

We performed our audit work primarily at State Department headquarters offices from July 1996 through August 1997 in accordance with generally accepted government auditing standards.

Information Systems Are Vulnerable to Unauthorized Access

Our penetration tests revealed that State's sensitive but unclassified information systems can be easily accessed by unauthorized users who in turn can read, delete, modify, or steal sensitive information on State's operations. First, while simulating outside attackers without knowledge of State's systems, we were able to successfully gain unauthorized access to State's networks through dial-in connections to modems.[5] Having obtained this access, we could have modified or deleted important data, shut down services, downloaded data, and monitored network traffic such as e-mail and data files.

We also tested internal network security controls and found them to be inadequate. For example, we were able to gain privileged (administrator) access to host systems on several different operating platforms (such as UNIX and Windows NT). This access enabled us to view international

[5]A modem is a device that enables a computer to transmit and receive information over a standard telephone line by converting digital signals into analog signals and vice versa.

financial data, travel arrangements, detailed network diagrams, a listing of valid users on local area networks, e-mail, and performance appraisals, among other sensitive data.

Our tests also found that security awareness among State employees is problematic. We were able to gain access to State's networks by guessing user passwords, bypassing physical security at one facility, and searching unattended areas for user account information and active terminal sessions. For example, in several instances we were able to enter a State facility without required identification. In an unlocked work area for one office, we found unattended personal computers logged onto a local area network. We also found a user identification and password taped to one of the computers. Using these terminals, we were able to download a file that contained a password list. In another unlocked area, we were able to access the local area network server and obtain supervisor-level access to a workstation. With this access, we could have added or deleted users, implemented unauthorized programs, and eliminated audit trails.

Our tests of dial-in-security, internal network security, and physical security demonstrated that information critical to State's operations as well as to the operations of other federal agencies operating overseas can be easily accessed and compromised. For example, we gained access to information that detailed the physical layout of State's automated information infrastructure. These data would make it much easier for an outsider who had no knowledge of State's operations or infrastructure to penetrate the department's computer resources. In addition, we obtained information on administrative and sensitive business operations which may be attractive targets to adversaries or hackers. At the conclusion of our testing, we provided senior State managers with the test results and suggestions for correcting the specific weaknesses identified.

State Lacks a Comprehensive Information Security Program

Our tests were successful primarily because State's computer security program is not comprehensive enough to effectively manage the risks to which its systems and networks are exposed. For example, the department does not have the information it needs to effectively manage its risks—it does not fully appreciate the sensitivity of its information, the vulnerabilities of its systems, or the costs of countermeasures. In addition, security is not managed by a strong focal point within the agency that can oversee and coordinate security activities. State also does not have the types of controls needed to ensure the security of its sensitive information, including current and complete security policies and enterprisewide

incident reporting and response capability. Moreover, top managers at State have not demonstrated that they are committed to strengthening security over the systems that they rely on for nearly every aspect of State's operations.

Elements of a Comprehensive Security Program

Our study of information security management[6] at leading organizations identified the following five key activities that are necessary in order to effectively manage security risks.

- A strong framework with a central management focal point and ongoing processes to coordinate efforts to manage information security risks.
- Risk assessment procedures that are used by business managers to determine whether risks should be tolerated or mitigated and to select appropriate controls.
- Comprehensive and current written policies that are effectively implemented and then updated to address new risks or clarify areas of misunderstanding.
- Steps to increase the awareness of users concerning the security risks to information and systems and their responsibilities in safeguarding these assets.
- Ability to monitor and evaluate the effectiveness of policy and other controls.

Furthermore, each of these activities should be linked in a cycle to help ensure that business risks are continually monitored, policies and procedures are regularly updated, and controls are in effect.

Perhaps the single most important factor in prompting the establishment of an effective information security program is commitment from top management. Ultimately, it is top managers who ensure that the agency embraces all elements of good security and who drive the risk management cycle of activity. However, State's top managers are not demonstrating the commitment necessary to practice good security and State's information security program does not fully incorporate any of the activities described above. Specifically, there is (1) no central management focal point, (2) no routine process for assessing risks, (3) no comprehensive and current set of written policies, (4) inadequate security awareness among State personnel, and (5) no effective monitoring and evaluation of policies and controls. In addition, State lacks a

[6]Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-21, Exposure Draft, November 1997).

comprehensive information security plan that would help ensure that these elements are in place.

Top Management Commitment at State Is Insufficient

While senior management at State has shown some interest in information security through actions including drafting memoranda, forming working groups to improve information security, and approving limited funding for selected security activities, this interest has not been sufficient to overcome longstanding and institutionalized security weaknesses. For example, while top management at State is aware of longstanding problems associated with its information management and information security and has reported a number of these high-risk and material weaknesses to the President and the Congress under provisions of the 1982 Federal Managers' Financial Integrity Act, these weaknesses remain unresolved. For example, mainframe computer security was identified as a material weakness 10 years ago but has not yet been corrected.

In reporting on unclassified mainframe systems security in its January 1996 Security Oversight Report, the department's Inspector General noted:

"The lack of senior management's involvement in addressing authority, responsibility, accountability and policy is the critical issue perpetuating the Department's lax approach to mainframe security . . . . In addition, the lack of clear management responsibility has resulted in incomplete and unreliable security administration . . . ."

Many mid-level State officials told us that the information security problems we and others identified during our review were already known throughout the department. Collectively, they believed that senior State management was not convinced of the seriousness of the problems and were unable or unwilling to commit the requisite attention and resources to resolve them. They noted that budget requests for security measures, such as information systems security officers, were approved but later rescinded. Many officials said that while the assignment of a chief information officer (CIO) was a critical step in elevating the importance of information management and security throughout the department, the CIO does not have the authority needed to ensure that improvements are made throughout State's decentralized activities. They also said that budgets for important controls, such as Bureau of Diplomatic Security information security evaluations at worldwide posts, are severely constrained and that the same security deficiencies are found and ignored year after year. Other officials reported that State personnel do not carry out their security

responsibilities satisfactorily because security is assigned as a low-priority collateral duty.

State Lacks a Clearly Defined Central Focal Point

The Department of State is a decentralized organization with bureaus operating semi-autonomously in their areas of responsibility. As a result, information resources management is scattered throughout the department. There is no single office responsible for overseeing the architecture, operations, configuration, or security of its networks and systems. The chief information officer, the Bureau of Diplomatic Security, and the information management office all perform information security functions. Many offices and functional bureaus also manage, develop, and procure their own networks and systems. In addition, according to Bureau of Diplomatic Security officials, some of the approximately 250 posts operated by State around the world have established their own network connections, further complicating security and configuration management.

This decentralized approach to information security is problematic. Scarce talent and resources are spread throughout the department, making communication and coordination difficult. Because the responsibilities for information security are divided among three offices, no one office is fully accountable, duties and responsibilities have been fragmented, and the department's principal security and information technology managers have often disagreed over strategy and tactics for improving the information security of the department. Perhaps most importantly, the department cannot determine if its systems are being attacked or if its information is being tampered with. State's Internet Risk Analysis states the following:

"Since there is no enterprise-wide authority for ensuring the confidentiality, integrity and availability of information as it traverses the unclassified network, it is extremely difficult to detect when information is lost, misdirected, intercepted or spoofed. Therefore, a post that is not expecting to receive information will not miss critical information that never arrives. More importantly, if a post does receive information it was not expecting, there is no office to confirm that the transmission was legitimate and not disinformation sent by a network intruder or disgruntled employee."

State Does Not Routinely Assess Risks

In assessing risks, managers should consider the (1) value and sensitivity of the information to be protected, (2) vulnerabilities of their computers and networks, (3) threats, including hackers, thieves, disgruntled employees, competitors, and in State's case, foreign adversaries and spies,

(4) countermeasures available to combat the problem, and
(5) cost-effectiveness of the countermeasures. In addition to providing the basis for selecting appropriate controls, results obtained from risk assessments should also be used to help develop and update an organizations's security plan and policies.

We met with representatives from the Office of Information Management and Bureau of Diplomatic Security who told us that they are unaware of any significant risk management activity related to information security within the department. These officials stated that they have not been requested to provide technical assistance to program managers at State. One significant exception to this is the comprehensive risk analysis performed by the Bureau of Diplomatic Security, which evaluated the risks associated with Internet connectivity.

Computer security evaluations performed at posts located around the world by Bureau of Diplomatic Security staff further demonstrate that State officials are not addressing and correcting risks appropriately. The evaluations revealed numerous problems at foreign posts such as use of inappropriate passwords and user identifications, failure to designate an information systems security officer, poor or nonexistent systems security training, and lack of contingency plans. Diplomatic security staff also told us that they have found that some posts have installed modem connections and Internet connections without approval, further complicating the department's ability to manage and secure its networks. Annual analyses of these evaluations show a pattern in which system security requirements are continually overlooked or ignored. Diplomatic security staff noted that the majority of the security deficiencies that they found are correctable with modest capital outlay and more attentive system administration.

State's Information Security Policies Are Incomplete

State's information security policies are primarily contained in its Foreign Affairs Manual. State also provides policy guidance in other formats, including instructions, cablegrams, letters, and memoranda. These policies are deficient in several respects. First, they fail to acknowledge some important security responsibilities within the department. For example, while the security manual details responsibilities of system managers and information systems security officers, it does not address the information security responsibilities of the Department's chief information officer (CIO). The CIO's authority and ability to operate effectively would be enhanced with departmental policy recognition of the legislatively

prescribed security responsibilities.[7] State's Foreign Affairs Manual was updated in February 1997 to describe the CIO position, but it does not discuss any information security responsibilities.

Second, the Foreign Affairs Manual does not require and consequently provides no mandate for, or guidance on, the use of risk assessments. As previously discussed, the department does not routinely assess and manage its information security risks. There is no specific State policy requiring threat and vulnerability assessments, despite their known value.

Third, State's policy manual does not sufficiently address users' responsibilities. For example, the manual does not emphasize that users should be accountable for securing their automated data, much as they are held responsible for securing classified paper documents. And it does not adequately emphasize the importance of information and computer resources as critical assets that must be protected. A significant finding in the department's Internet risk analysis is that users and even systems administrators "do not feel that their unclassified data is sensitive and therefore spend little to no effort in protecting the data from external disclosure." Clearly stated policy and effective implementation could contribute greatly to increased awareness.

State Is Not Adequately Promoting Awareness

Often, computer attacks and security breakdowns are the result of failures on the part of computer users to take appropriate security measures. For this reason, it is vital that employees who use a computer system in their day-to-day operations be aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality and integrity. In accepting responsibility for security, users need to follow organizational policies and procedures, and acknowledge the consequences of security violations. They should also devise effective passwords, change them frequently, and protect them from disclosure. Further, it is important that users not leave their computers, workstations, or terminals unattended, and log out when finished using their computers. In addition, users should help maintain physical security over their assigned areas and computer resources.

[7]Under the Paperwork Reduction Act of 1996 (Public Law 104-13, Chapter 35 of Title 44, United States Code) and the Clinger-Cohen Act of 1996 (Public Law 104-106, the National Defense Authorization Act for Fiscal Year 1996), chief information officers are responsible for ensuring agency compliance with privacy and security requirements. Specifically, they are to provide advice and assistance to senior agency officials to ensure that the information security policies, procedures, and practices of their agency are adequate.

Many computer users at State had weak passwords that were easily guessed, indicating that they were unaware of or insensitive to the need for secure passwords. During our testing of State's systems, we were able to guess passwords on a number of machines on various networks using both manual guessing and automated password cracking programs. One way to prevent password guessing is to ensure that users use complex passwords such as those composed of alphanumeric, upper- and lower-case characters. However, there was no evidence that State was training its users to employ these techniques. We also found little evidence that State was training its users to prevent unauthorized access to information. For example, we called a user under the pretense that we were systems maintenance personnel and were able to convince her to disclose her password.

We also bypassed physical security at a State facility and searched unattended areas for user account information and active terminal sessions. For example, in several instances we were able to enter a facility without the required State identification by using turnstiles designed for handicapped use. Once inside the facility, we entered unlocked work areas and found unattended personal computers logged onto a local area network. From one of these computers, we downloaded a file that contained a password list. We also noticed that a password and user identification code were taped to the desk in a workstation.

State Does Not Regularly Evaluate Its Controls

Some key controls are not in place at State to ensure that it can defend its sensitive information and systems. For example, State has very little departmentwide capacity to respond to security incidents and individual bureaus currently handle incidents on an ad hoc basis. Problems experienced are not shared across the department because the incidents are not reported or tracked centrally and very little documentation is prepared. Furthermore, State does not regularly test its systems and network access controls through penetration testing. Finally, State has limited ability to visit all its worldwide locations to perform security evaluations.

Our study of information security management at leading organizations found that an organization must monitor and evaluate its policies and other controls on a regular basis to periodically reassess whether it is achieving its intended results. Testing the existence and effectiveness of controls and other risk reduction efforts can help determine if they are operating effectively. Over time, policies and controls may become

inadequate because of changes in threats, changes in operations, or deterioration in the degree of compliance.

Because breaches in information security, computer viruses, and other related problems are becoming more common, an aggressive incident response capability is an important control and a key element of a good security program. Organizations need this capability to respond quickly and effectively to security incidents, help contain and repair any damage caused and prevent future damage. In recognition of the value of an incident response capability, federal agencies are now required by the Office of Management and Budget to establish formal mechanisms to respond to security incidents.[8] Many organizations are now setting up emergency response teams and coordinating with other groups, including the Federal Computer Incident Response Capability and Carnegie Mellon's Computer Emergency Response Team. Knowing that organizations have a formidable response capability has proved to be a deterrent to hackers and other unauthorized users.

State acknowledges that it needs the capability to detect and react to computer incidents and information security threats in a timely and efficient manner. At the time of our review, Department personnel were drafting incident response procedures. Bureau of Diplomatic Security officials told us that they are beginning to develop an incident response capability at the laboratory that they use to evaluate and accredit systems and software. Information management officials also told us that efforts were underway to obtain some services from the Federal Computer Incident Response Capability[9] that would help them detect and react to unauthorized access to their systems.

As discussed earlier, Bureau of Diplomatic Security performs evaluations of field locations to identify and make recommendations for correcting security weaknesses. However, Bureau of Diplomatic Security officials told us that budget constraints limit their ability to perform these evaluations and visit all locations on a systematic and timely basis. State officials also told us that they need to periodically assess the

[8]The February 1996 revision to Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Systems, requires agencies to establish formal incident response mechanisms and awareness training of these mechanisms for employees.

[9]The Federal Computer Incident Response Capability is a collaboration among the National Institute of Standards and Technology, the Defense Advanced Research Project Agency's Computer Emergency Response Team Coordination Center, and the Department of Energy's Computer Incident Advisory Capability. This service has been designed to provide federal civilian agencies with cost-reimbursable, direct technical assistance and incident handling support.

vulnerabilities of and threats to their systems. They also acknowledged the need for and importance of developing a reporting mechanism that can be used across the department to share information on vulnerabilities and incidents.

An additional control mechanism that could help State ensure that controls are in place and working as intended, and that incident response capability is strong, is the annual financial statement audit. This audit is required to be conducted annually by the Chief Financial Officers Act of 1990.[10] A part of this audit could involve a detailed examination of an agency's general and application computer controls.[11] We have been working with the department's inspector general to ensure that State's financial audit includes a comprehensive assessment of these controls. When this audit is complete, management will be able to better gauge its progress in establishing and implementing sound information security controls.

State Lacks a Comprehensive Information Security Plan

Federal agencies are required by the Computer Security Act to develop and implement security plans to protect any systems containing sensitive data. The February 1996 revision to Appendix III of OMB Circular A-130 requires that a summary of the security plans be incorporated into an agency's strategic information resources management plan. State has no information security plan. Instead, the department's IRM Strategic and Performance Management Plan includes several pages of text on information security and its implementation. This discussion highlights the development of computer security and privacy plans for each system containing sensitive information, as required by the Computer Security Act. However, when we requested copies of these individual plans, we were told that they could not be located and that even if they were found, they would be virtually useless because they were drafted in the late 1980s, never updated, and are now obsolete.

The strategic plan also references other efforts underway within the department, including assessments of various software applications to identify vulnerabilities and evaluations of antivirus software products. However, this discussion is insufficient. It merely lists a set of ad hoc and

[10]The Chief Financial Officers Act of 1990 (Public Law 101-576), as amended in 1994, requires State and 23 other federal agencies to prepare financial statements that can pass the test of an independent audit and provide decisionmakers with reliable financial information.

[11]Our Federal Information System Controls Audit Manual provides guidance for evaluating general and application controls over the integrity, confidentiality, and availability of data maintained in computer-based information systems.

largely unrelated programs and projects to improve information security. It does not relate these programs to any risk-based analysis of threats to and vulnerabilities of the department's networks or systems. Furthermore, this discussion mentions the existence of but does not endorse or discuss planned efforts to implement any key recommendations identified in the Internet Risk Analysis.

A companion document to the strategic plan, the department's February 1997 Tactical Information Resources Management Plan, indicates the lack of emphasis that information security receives. According to this plan, the department should closely monitor and centrally manage all information resource management initiatives that "are critical to the Department missions; will cost more than $1 million through their life cycle; have schedules exceeding one year; and cut across organizational lines." However, the plan acknowledges that "at this time the Department has no Security projects that meet the criteria" above. In addition, the plan ignores the need for centralized management for information technology projects and, instead, requires individual offices to fund and manage their own security requirements.

Greater Internet Connectivity Poses Additional Risks

Internet security was the only area in which we found that State's controls were currently adequate. We attempted to gain access to internal State networks by going through and around State's Internet gateways or exploiting information servers from the outside via the Internet, but we were not able to gain access to State's systems. State's protection in this area is adequate, in part, because the department has limited its use and access to the Internet. However, State officials have been requesting greater Internet access and the department is considering various options for providing it.

Expansion of Internet services would provide more pathways and additional tools for an intruder to attempt to enter unclassified computer resources and therefore increase the risk to State systems. Recognizing this, State conducted an analysis of the risks involved with increasing Internet use. However, the department has not yet decided to what extent it will accept and/or address these new risks. Until it does so and implements a comprehensive security program that ensures that top managers are committed to enforcing security controls and users are fully aware of their computer security responsibilities, State will not be in a good position to expand its Internet use.

Conclusions

Networked information systems offer tremendous potential for streamlining and improving the efficiency of State Department operations. However, they also greatly increase the risks that sensitive information supporting critical State functions can be attacked. Our testing demonstrated that State does not have adequate controls to protect its computer resources and data from external attacks and unauthorized activities of trusted users who are routinely allowed access to computer resources for otherwise legitimate purposes. These weaknesses pose serious risk to State information and operations and must be mitigated.

We recognize that no organization can anticipate all potential vulnerabilities, and even if it could, it may not be cost-effective to implement every measure available to ensure protection. However, State has yet to take some basic steps to upgrade its information systems security and improve its position against unauthorized access. These steps include ensuring that top managers are fully aware of the need to protect State's computer resources, establishing a strong central management focal point to remedy the diluted and fragmented security management structure, and addressing the risks of additional external connectivity before expanding its Internet usage. Until State embraces these important aspects of good computer security, its operations, as well as those of other federal agencies that depend on State, will remain vulnerable to unauthorized access to computer systems and data.

Recommendations

We reaffirm the recommendations we made in our March 1998 classified report. These recommendations called on State to take the following actions.

- Establish a central information security unit and assign it responsibility for facilitating, coordinating, and overseeing the department's information security activities. In doing so,
  - assign the Chief Information Officer the responsibility and full authority for ensuring that the information security policies, procedures, and practices of the agency are adequate;
  - clarify the computer security responsibilities of the Bureau of Diplomatic Security, the Office of Information Management, and individual bureaus and diplomatic posts; and
  - consider whether some duties that have been assumed by these offices can be assigned to, or at a minimum coordinated with, the central information security unit.

- Develop policy and procedures that require senior State managers to regularly determine the (1) value and sensitivity of the information to be protected, (2) vulnerabilities of their computers and networks, (3) threats, including hackers, thieves, disgruntled employees, foreign adversaries, and spies, (4) countermeasures available to combat the problem, and (5) cost-effectiveness of the countermeasures.
- Revise the Foreign Affairs Manual so that it clearly describes the legislatively-mandated security responsibilities of the Chief Information Officer, the security responsibilities of senior managers and all computer users, and the need for and use of risk assessments.
- Develop and maintain an up-to-date security plan and ensure that revisions to the plan incorporate the results obtained from risk assessments.
- Establish and implement key controls to help the department protect its information systems and information, including
  - periodic penetration testing to identify vulnerabilities in State's information resources;
  - assessments of the department's ability to (1) react to intrusion and attacks on its information systems, (2) respond quickly and effectively to security incidents, (3) help contain and repair any damage caused, and (4) prevent future damage, and
  - central reporting and tracking of information security incidents to ensure that knowledge of these problems can be shared across the department and with other federal agencies.
- Ensure that the results of the annual financial statement audits required by the Chief Financial Officers Act of 1990 are used to track the department's progress in establishing, implementing, and adhering to sound information security controls.
- Require department managers to work with the central unit to expeditiously review the specific vulnerabilities and suggested actions we provided to State officials at the conclusion of our testing. After the department has reviewed these weaknesses and determined the extent to which it is willing to accept or mitigate security risks, assign the central unit responsibility for tracking the implementation and/or disposition of these actions.
- Direct the Assistant Secretary for Diplomatic Security to follow-up on the planned implementation of cost-effective enhanced physical security measures.
- Defer the expansion of Internet usage until (1) known vulnerabilities are addressed using risk-based techniques and (2) actions are taken to provide appropriate security measures commensurate with the planned level of Internet expansion.

Agency Comments and Our Evaluation

The Department of State provided written comments on a draft of our classified report and concurred with eight of our nine recommendations. In summary, State said that its Chief Information Officer is beginning to address the lack of a central focus for information systems security through the establishment of a Security Infrastructure Working Group; agreed to formalize and document risk management decisions; agreed to revise provisions of the Foreign Affairs Manual related to information security and undertake an evaluation of one of its most significant networks based on our review; and said it is implementing a plan to correct the technical weaknesses identified during our testing. State also took steps to minimize unauthorized physical access to a State facility.

State did not concur with our recommendation to defer the expansion of Internet usage. In explaining its nonconcurrence, State asserted that

- expanded use of Internet resources is a priority;
- the Chief Information Officer, Office of Information Management, and Bureau of Diplomatic Security are coordinating on architecture and security functionality that should mitigate any significant security vulnerabilities through the use of a separate enclave;
- segmenting the network, implementing controlled interfaces, restricting services, restricting the processing or transmission of sensitive unclassified information, and proactive network monitoring and incident handling should mitigate these risks; and
- a formal risk analysis of expanding the Internet throughout the department has been conducted and known risk factors are being considered in the Internet expansion.

Some of these assertions are invalid; the rest do not fully address our recommendation. First, designating expanded Internet usage as a priority does not mean that State should proceed before it fully implements appropriate security controls. If State expands Internet connectivity without effectively mitigating the significant additional risks that entails, it will increase its already serious vulnerabilities to individuals or organizations seeking to damage State's operations, commit terrorism, or obtain financial gain.

Second, State does not explain how "coordination on architecture and security functionality" between the Chief Information Officer, Office of Information Management, and Bureau of Diplomatic Security will reduce Internet risks, including computer attacks from those wishing to steal information or disable the department's systems. As noted in this report,

the organizations cited by State share various information security responsibilities, but have different missions and interests. This assertion does not address our recommendation that State establish an organization unit with responsibility for and authority over all information security activities, including protecting the department from computer attacks via Internet.

Third, State identified a number of controls with it believes will reduce Internet security risks, including establishing a (logically) separate network (enclave) dedicated to Internet usage, and proactively monitoring the network and handling incidents. If effectively implemented and maintained, these measures can help reduce security risks. However, State did not specify how it planned to implement these controls, what resources it has allocated to these efforts, or if they would be completed before State expands its Internet usage. Our point is that State must actually implement and maintain security measures to mitigate these risks prior to increasing Internet usage.

Finally, we discussed State's risk analysis of expanded Internet usage in our report. This analysis identifies numerous risks associated with expansion and options for addressing them. It is not sufficient that "known risk factors are being considered in the Internet expansion"; as previously noted, State must mitigate these risks prior to increasing Internet usage.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from its date. At that time, we will send copies of this report to the Chairman and Ranking Minority Members of the House Government Reform and Oversight Committee, Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, the House Committee on Appropriations, Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, and the Secretary of State. Copies will be available to others upon request.

If you have questions about this report, please contact me at (202) 512-6240. Major contributors are listed in appendix I.

Jack L. Brock, Jr.
Director, Governmentwide
and Defense Information Systems

Appendix I

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Keith A. Rhodes, Technical Director John B. Stephenson, Assistant Director Kirk J. Daubenspeck, Evaluator-in-Charge Patrick R. Dugan, Auditor Cristina T. Chaplain, Communications Analyst

United States General Accounting Office

GAO

Report to the Committee on Governmental Affairs, U.S. Senate

May 1998

AIR TRAFFIC CONTROL

Weak Computer Security Practices Jeopardize Flight Safety

GAO/AIMD-98-155

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-276735

May 18, 1998

The Honorable Fred Thompson
Chairman
The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

Security at our nation's airports has received great attention in recent years due to several commercial aircraft explosions; however, securing our nation's airports alone does not ensure safe air travel. It is also critical to secure the Federal Aviation Administration's (FAA) air traffic control (ATC) computer systems that provide information to air traffic controllers and aircraft flight crews to ensure safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruption of air traffic or even loss of life due to collisions. Since malicious attacks on computer systems are an increasing threat, it is essential that FAA ensure the integrity and availability of ATC information and protect it from unauthorized users.

Given the paramount importance of computer security of ATC systems, you asked us to determine (1) whether FAA is effectively managing physical security at ATC facilities and systems security for its current operational systems, (2) whether FAA is effectively managing systems security for future ATC modernization systems, and (3) the effectiveness of FAA's management structure and implementation of policy for computer security. We issued a "Limited Official Use" report to you detailing the results of our review on April 29, 1998. This unclassified version of that report summarizes the weaknesses we found in FAA's ATC computer security program and our recommendations for corrective actions.

Results in Brief

FAA is ineffective in all critical areas included in our computer security review—facilities physical security, operational systems information security, future systems modernization security, and management structure and policy implementation.

In the physical security area, known weaknesses exist at many ATC facilities. For example, a March 1997 inspection of a facility that controls aircraft disclosed 13 physical security weaknesses, including unauthorized personnel being granted unescorted access to restricted areas. FAA is

unaware of weaknesses that may exist at other locations. For example, FAA has not assessed the physical security controls at 187 facilities since 1993 and therefore does not know how vulnerable they are.

Second, FAA is similarly ineffective in managing systems security for its operational systems and is in violation of its own policy. An October 1996 information systems security assessment concluded that FAA had performed the necessary analysis to determine system threats, vulnerabilities, and safeguards for only 3 of 90 operational ATC computer systems, or less than 4 percent. FAA officials told us that this assessment is an accurate depiction of the current state of operational systems security. Further, according to the team that maintains FAA's telecommunications networks, only one of the nine operational ATC telecommunications networks has been analyzed. Without knowing the specific vulnerabilities of its ATC systems, FAA cannot adequately protect them.

Third, FAA is also not effectively managing systems security for future ATC modernization systems. It does not consistently include well formulated security requirements in specifications for all new ATC modernization systems, as required by FAA policy. Further, it does not have a well-defined security architecture, a concept of operations, or security standards all of which are needed to define and ensure adequate security throughout the ATC network.

Finally, FAA's management structure and implementation of policy for ATC computer security is not effective. Security responsibilities are distributed among three organizations, all of which have been remiss in their ATC security duties. The Office of Civil Aviation Security is responsible for developing and enforcing security policy, the Office of Air Traffic Services is responsible for implementing security policy for operational ATC systems, and the Office of Research and Acquisitions is responsible for implementing policy for ATC systems that are being developed. The Office of Civil Aviation Security has not adequately enforced FAA policies that require the assessment of physical security controls at all ATC facilities and vulnerabilities, threats, and safeguards for all operational ATC computer systems. In addition, the Office of Air Traffic Services has not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards. Finally, the Office of Research and Acquisitions has not implemented the FAA policy that requires it to formulate requirements for security in specifications for all new ATC modernization systems.

Background

FAA's ATC network is an enormous, complex collection of interrelated systems, including navigation, surveillance, weather, and automated information processing and display systems that reside at, or are associated with, hundreds of ATC facilities. These systems and facilities are interconnected by complex communications networks that separately transmit both voice and digital data. As stated in our 1997 report on high-risk issues,[1] while the use of interconnected systems promises significant benefits in improved government operations, it also increases vulnerability to anonymous intruders who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations. Since this interconnectivity is expected to grow as systems are modernized to meet the projected increases in air traffic and to replace aging equipment, the ATC network will become even more vulnerable to such network-related threats.

The threat to information systems is also growing because of the increasing availability of strategies and tools for launching planned attacks. For example, in May 1996 we reported that tests at the Department of Defense showed that Defense systems may have experienced as many as 250,000 attacks during 1995, about 65 percent of these succeeded in gaining access, and only about 4 percent were detected.[2]

Since intruders can use a variety of techniques to attack computer systems, it is essential that FAA's approach to computer security be comprehensive and include (1) physical security of the facilities that house ATC systems (e.g., locks, guards, fences, and surveillance equipment), (2) information security of the ATC systems (e.g., safeguards incorporated into computer hardware and software), and (3) telecommunications security of the networks linking ATC systems and facilities (e.g., secure gateways, firewalls, and communication port protection devices).

For years, the need for federal agencies to protect sensitive and critical, but unclassified, federal data has been recognized in various laws, including the Privacy Act of 1974, the Computer Security Act of 1987, and the Paperwork Reduction Act of 1995, and was recently reemphasized in the Clinger-Cohen Act of 1996. The adequacy of controls over computerized data is also addressed indirectly by the Federal Managers'

[1]High-Risk Series: Information Management and Technology (GAO/HR-97-09, Feb. 1997).

[2]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

Financial Integrity Act (FMFIA) of 1982 and the Chief Financial Officers Act of 1990. For example, FMFIA requires agency managers to evaluate their internal control systems annually and report to the President and the Congress any material weaknesses that could lead to fraud, waste, and abuse in government operations. In addition, a considerable body of federal guidance on information security has been developed by both the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Objectives, Scope, and Methodology

The objectives of our review were to determine (1) whether FAA is effectively managing physical security at ATC facilities and systems security for its current operational systems, (2) whether FAA is effectively managing systems security for future ATC modernization systems, and (3) the effectiveness of FAA's management structure and implementation of policy for computer security.

To determine whether FAA is effectively managing physical security at ATC facilities, we

- reviewed FAA Order 1600.6C, Physical Security Management Program, to determine ATC facility security inspection and accreditation requirements;
- reviewed data from FAA's Facility Inspection Reporting System (FIRS) to determine the accreditation status of category I and II towers, terminal radar approach control (TRACON) facilities, and air route traffic control towers (en route centers) and their last inspection date;[3]
- verified the accuracy of the FIRS accreditation data with each of the nine regional FIRS program managers by requesting accreditation reports for each facility that FIRS reported as being accredited;
- for those facilities that were not accredited, requested dates of their initial comprehensive physical security inspection[4] and follow-up inspections from each of the nine regional FIRS program managers to determine why ATC facilities were not accredited;
- verified the initial and follow-up inspection dates by requesting and reviewing documentation for each inspection conducted from April 16, 1993, to July 31, 1997, and then provided our analyses to Office of Civil

[3]Category I facilities are those that are critical to national security and the National Airspace System (NAS). Category II facilities are other FAA-staffed facilities. We did not review security measures at airports.

[4]FAA calls this initial physical security inspection an initial physical security survey, and it includes an evaluation of the local threat, physical security controls, security documentation, and required corrective actions.

Aviation Security Operations officials, who in turn verified it with each region;

- reviewed the Department of Justice's June 28, 1995, report, Vulnerability Assessment of Federal Facilities, to identify new physical security requirements for federal facilities;
- reviewed physical security assessments for three locations to determine FAA's ATC compliance with Department of Justice blast standards and to identify additional physical security weaknesses at key ATC facilities;
- reviewed the Facility Security Risk Management Mission Need Statement for Staffed Facilities, Number 316, June 23, 1997, to determine physical security deficiencies and FAA's plans to improve physical security; and
- interviewed officials from the Offices of Civil Aviation Security, Operations and Policy and Planning, and Airways Facility Services to determine physical security requirements, to determine whether FAA is in compliance with 1600.6C, to identify reasons for noncompliance, and to identify who develops, implements, and enforces ATC physical security policy.

To determine whether FAA is effectively managing systems security for its current operational systems, we

- reviewed federal computer security requirements specified in the Computer Security Act of 1987 (Public Law 100-235); Paperwork Reduction Act of 1995 (Public Law 104-13), as amended; OMB Circular A-130, appendix III, "Security of Federal Automated Information Resources;" the 1996 Clinger-Cohen Act; and An Introduction to Computer Security: The NIST Handbook to identify federal security requirements;
- reviewed FAA Order 1600.54B, FAA Automated Information Systems Security Handbook, and FAA Order 1600.66, Telecommunications and Information Systems Security Policy, to determine ATC system risk assessment, certification, and accreditation requirements;
- reviewed Volpe National Transportation Systems Center NAS AIS Security Review, October 1, 1996, to determine how many ATC operational systems were assessed, certified, and accredited as of October 1, 1996;
- requested and reviewed accreditation reports, security certification reports, risk assessments, contingency plans, and disaster recovery plans for six operational ATC systems;[5]
- reviewed the White House Commission on Aviation Safety and Security's final report to the President, February 12, 1997, to determine recommendations to improve ATC computer security;

[5]The six operational ATC systems we selected were not intended to be a representative sample. However, each is critical to controlling aircraft, and collectively they represent systems from different environments in which aircraft are controlled.

- reviewed the Federal Aviation Administration Air to Ground Communications Vulnerabilities Assessment, June 1993, to determine ATC communication systems vulnerabilities;
- reviewed the Report to Congress, Air Traffic Control Data and Communications Vulnerabilities and Security, Report of the Federal Aviation Administration Pursuant to House-Senate Report Accompanying the Department of Transportation and Related Agencies Appropriations Act, 102-639, June 1, 1993, to determine what ATC security vulnerabilities FAA disclosed to the Congress in 1993;
- interviewed the telecommunications integrated product team to determine what operational communication systems have been assessed, certified, and accredited and reviewed the team's 1994 and 1997 strategic plans to determine communication system risks and planned security improvement initiatives;
- interviewed the Director of Spectrum Policy and Management to determine the extent to which intruders are accessing ATC frequencies;
- interviewed FAA's Designated Approving Authority (DAA) to determine FAA's policy for accrediting ATC systems; and
- interviewed the Office of Civil Aviation Security Operations officials and Airways Facilities Services officials to determine who develops, implements, and enforces ATC operational systems security policy and to determine whether an incident reporting and handling capability exists.

To determine whether FAA is effectively managing systems security for future ATC modernization systems, we

- requested and reviewed risk assessments and acquisition specifications for six ATC systems that are being developed to determine if security requirements based on detailed assessments existed;[6]
- interviewed three integrated product teams (IPT) to determine what security policy/guidance each follows in developing ATC systems;
- reviewed the NAS Information Security Mission Need Statement, April 22, 1997, to determine information security deficiencies, future system vulnerabilities, and FAA's plans to improve information security;
- interviewed the NAS Information Security (NIS) group to determine its plans to improve ATC information security and reviewed its NAS Information Security Action Plan; and
- reviewed the President's Commission of Critical Infrastructure Protection's (PCCIP) final report, Critical Foundations, Protecting America's Infrastructures, October 1997, and its supplemental report,

[6]The six ATC systems currently being developed that we selected were not intended to be a representative sample. However, each will be critical to controlling aircraft in the future, and collectively they represent systems from different environments in which aircraft are controlled

Vulnerability Assessment of the FAA National Airspace Systems (NAS) Architecture, October 1997, to determine future ATC systems security vulnerabilities.

To determine the effectiveness of FAA's management structure and implementation of policy for computer security, we

- reviewed FAA Order 1600.6C, Physical Security Management Program (dated April 1993), Order 1600.54B, FAA Automated Information Systems Security Handbook (dated February 1989), and Order 1600.66, Telecommunications and Information Systems Security Policy (dated July 1994), to determine what organizations are assigned responsibility for developing, implementing, and enforcing ATC computer security policy[7] and
- interviewed officials from the Offices of Civil Aviation Security, Air Traffic Services, and Research and Acquisitions to determine what organizations are responsible for developing, implementing, and enforcing ATC computer security policy.

In addition, we interviewed the Associate Administrators for Civil Aviation Security and for Research and Acquisitions and the Director of Airway Facilities under the Associate Administrator for Air Traffic Services to determine why ATC computer security policies have not been adequately implemented and enforced.

We performed our work at FAA headquarters in Washington, D.C., from April 1997 through January 1998 in accordance with generally accepted government auditing standards.

ATC Physical Security Management and Controls Are Ineffective

ATC systems used to control aircraft reside at, or are associated with, a variety of ATC facilities including towers, TRACONs, and en route centers. FAA policy, dated April 1993, required that these facilities be inspected by April 1995 and that annual or triennial follow-up inspections be conducted depending on the type of facility to determine the status of physical security at each facility. These inspections determine whether the facility meets the physical security standards established in FAA policy and are the basis for accrediting ATC facilities (i.e., concluding that they are secure).

[7]We did not conduct a complete assessment of Orders 1600.6C, 1600.54B, or 1600.66 since two of these orders were undergoing major revisions at the time of our review.

FAA is not effectively managing physical security at ATC facilities. Known physical security weaknesses exist at many ATC facilities. For example, an inspection of a facility that controls aircraft disclosed 26 physical security findings including (1) fire protection systems that failed to meet minimum detection and suppression standards and (2) service contract employees that were given unrestricted access to sensitive areas without having appropriate background investigations. FAA recently confirmed its physical security weaknesses when it performed detailed assessments of several key ATC facilities following the Oklahoma City bombing to determine physical security risks and the associated security measures and costs required to reduce these risks to an acceptable level.[8] For example, an assessment of a facility that controls aircraft concluded that access control procedures are weak to nonexistent and that the center is extremely vulnerable to criminal and terrorist attack.

In addition, FAA is unaware of physical security weaknesses that may exist at other FAA facilities. For example, FAA has not assessed the physical security controls at 187 facilities since 1993 and therefore does not know how vulnerable they are. Until FAA inspects its remaining facilities, it does not know if they are secure and if the appropriate controls are in place to prevent loss or damage to FAA property, injury to FAA employees, or compromise of FAA's capability to perform critical air safety functions.

ATC Operational System Security Is Ineffective and Systems Are Vulnerable

FAA policy requires that all ATC systems be certified and accredited.[9] A risk assessment, which identifies and evaluates vulnerabilities, is a key requirement for certification and accreditation. We recently reported that leading information security organizations use risk assessments to identify and manage security risks confronting their organizations.[10]

FAA has not assessed, certified, or accredited most operational ATC systems. A review conducted for FAA's Office of Civil Aviation Security in October 1996 concluded that FAA had not conducted risk assessments on 83 of 90, or over 90 percent, of all operational ATC systems. FAA officials told us that this assessment is an accurate depiction of the agency's

[8]A key part of these assessments was to conduct a blast analysis of FAA facilities.

[9]System certification is the technical evaluation that is conducted to verify that FAA systems comply with FAA security requirements, identify security deficiencies, specify remedies, and justify exceptions. Certification results are one factor management considers in deciding whether to accredit systems. Accreditation is the formal declaration from management that the appropriate security safeguards have been properly implemented and that residual risk is acceptable.

[10]Executive Guide: Information Security Management — Learning From Leading Organizations (Exposure Draft) (GAO/AIMD-98-21, Nov. 1997).

knowledge regarding operational systems security. As a result, FAA does not know how vulnerable these operational ATC systems are and consequently has no basis for determining what protective measures are required. Further, the review concluded that of the 7 systems assessed, only 3 resulted in certifications because 4 systems did not have the proper certification documentation.[11] Accordingly, less than 4 percent of the 90 operational systems are certified. In addition, FAA has not assessed most ATC telecommunication systems. For example, FAA's officials responsible for maintaining the nine FAA-owned and leased communication networks told us that only one has been assessed. Such poor security management exists despite the fact that FAA's 1994 Telecommunications Strategic Plan stated that "vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety." FAA's 1997 Telecommunications Strategic Plan continues to identify security of telecommunication systems as an area in need of improvement.

Office of Civil Aviation Security officials told us that they were not aware of a single ATC system that was accredited. We found similar results when we reviewed six operational systems to determine if they were assessed, certified, or accredited. Risk assessments had been conducted and certification reports written for only two of the systems, while none of the systems had been accredited. The Associate Administrator for Civil Aviation Security, who is responsible for accrediting systems, told us that FAA has decided to spend its limited funds not on securing currently operating systems, but rather on developing new systems and that FAA management is reluctant to acknowledge information security threats.

FAA claims that because current ATC systems often utilize custom-built, 20-year-old equipment with special purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited. While these configurations may not be commonly understood by external hackers, one cannot conclude that old or obscure systems are, a priori, secure. In addition, the certification reports that FAA has done reveal operational systems vulnerabilities. Furthermore, archaic and proprietary features of the ATC system provide no protection from attack by disgruntled current and former employees who understand them.

[11]The documentation did not exist or was not signed by appropriate authorities.

FAA Is Not Effectively Managing Security for New ATC Systems

Essential computer security measures can be provided most effectively and cost efficiently if they are addressed during systems design. Retrofitting security features into an operational system is far more expensive and often less effective. Sound overall security guidance, including a security architecture, security concept of operations, and security standards, is needed to ensure that well formulated security requirements are included in specifications for all new ATC systems.

FAA has no security architecture, security concept of operations, or security standards. As a result, implementation of security requirements across ATC development efforts is sporadic and ad hoc. Of the six current ATC system development efforts that we reviewed, four had security requirements, but only two of the four developed their security requirements based on a risk assessment. Without security requirements based on sound risk assessments, FAA lacks assurance that future ATC systems will be protected from attack. Further, with no security requirements specified during systems design, any attempts to retrofit security features later will be increasingly costly and technically challenging. An FAA June 1993 report to the Congress on information security states that because FAA lacks a security architecture to guide the development of ATC security measures, technical security requirements will be retrofitted or not implemented at all because the retrofit "could be so costly or technically complex that it would not be feasible."[12]

In April 1996, the Associate Administrator for Research and Acquisitions established the National Airspace Systems (NAS) Information Security (NIS) group to develop, along with other security initiatives, the requisite security architecture, security concept of operations, and security standards. The NIS group has developed a mission need statement that asserts that "information security is the FAA mission area with the greatest need for policy, procedural, and technical improvement. Immediate action is called for, to develop and integrate information security into ATC systems throughout their life cycles." FAA has estimated that it will cost about $183 million to improve ATC information security. The NIS group has developed an action plan that describes each of its proposed improvement activities. However, over 2 years later it has not developed detailed plans or schedules to accomplish these tasks.

As FAA modernizes and increases system interconnectivity, ATC systems will become more vulnerable, placing even more importance on FAA's

[12]Report to Congress, Air Traffic Control Data and Communications Vulnerabilities and Security, Report of the Federal Aviation Administration Pursuant to House-Senate Report Accompanying the Department of Transportation and Related Agencies Appropriations Act, 102-639, June 1, 1993.

ability to develop adequate security measures. These future vulnerabilities are well documented in FAA's information security mission need statement and also in reports completed by the President's Commission on Critical Infrastructure Protection.[13] The President's Commission summary report concluded that the future ATC architecture appears to have vulnerabilities and recommended that FAA act immediately to develop, establish, fund, and implement a comprehensive systems security program to protect the modernized ATC system from information-based and other disruptions, intrusions, and attacks. It further recommended that this program be guided by the detailed recommendations made in the NAS vulnerability assessment.

FAA's Management Structure Is Not Effectively Implementing and Enforcing Computer Security Policy

FAA's management structure and implementation of policy for computer security has been ineffective: the Office of Civil Aviation Security has not adequately enforced the security policies it has formulated; the Office of Air Traffic Services has not adequately implemented security policy for operational ATC systems; and the Office of Research and Acquisitions has not adequately implemented policy for new ATC systems development. For example, the Office of Civil Aviation Security has not enforced FAA policies that require the assessment of physical security controls at all ATC facilities and vulnerabilities, threats, and safeguards for all operational ATC computer systems; the Office of Air Traffic Services has not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards; and the Office of Research and Acquisitions has not implemented the FAA policy that requires it to include, in specifications for all new ATC modernization systems, requirements for security based on risk assessments.

FAA established a central security focal point, the NIS group, to develop additional security guidance (i.e., a security architecture, a security concept of operations, and security standards), to conduct risk assessments of selected ATC systems, to create a mechanism to respond to security incidents, and to provide security engineering support to ATC system development teams. The NIS group includes members from the Offices of Civil Aviation Security, Air Traffic Services, and Research and Acquisitions.

[13]The President's Commission on Critical Infrastructure Protection (PCCIP) was established in July 1996, in Executive Order 13010, to assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. As a supplement to the transportation assessment, the PCCIP conducted a vulnerability assessment of the NAS architecture.

Establishing a central security focal point is a practice employed by leading security organizations. In order to be effective, the security focal point must have the authority to enforce the organization's security policies or have access to senior executives that are organizationally positioned to take action and effect change across organizational divisions. One approach for ensuring that a central group has such access at FAA would be to place it under a Chief Information Officer (CIO) who reports directly to the FAA Administrator. This approach is consistent with the Clinger-Cohen Act,[14] which requires that major federal departments and agencies establish CIOs who report to the department/agency head and are responsible for implementing effective information management.

FAA does not have a CIO reporting to the Administrator. Although the NIS group has access to certain key Associate Administrators (e.g., the Associate Administrator for Civil Aviation Security and the Associate Administrator for Research and Acquisitions), it does not have access to the management level that can effect change across organizational divisions (e.g., FAA's Administrator or Deputy Administrator). Thus, there is no assurance that the NIS group's guidance, once issued, will be adequately implemented and enforced, that results of its risk assessments will be acted upon, and that all security breaches will be reported and adequately responded to. Until existing ATC computer security policy is effectively implemented and enforced, operational and developmental ATC systems will continue to be vulnerable to compromise of sensitive information and interruption of critical services.

In addition, OMB Circular A-130, Appendix III, requires that systems, such as ATC systems, be accredited by the management official who is responsible for the functions supported by the systems and whose mission is adversely affected by any security weaknesses that remain (i.e., the official who owns the operational systems). At FAA, this management official is the Associate Administrator for Air Traffic Services. However, FAA's ATC systems authorizing official is the Associate Administrator for Civil Aviation Security, who does not own the operational ATC systems.

Conclusions

Since physical security is the agency's first line of defense against criminal and terrorist attack, failure to strengthen physical security controls at ATC towers, TRACONs, and en route centers places property and the safety of the flying public at risk. Information system security safeguards, either those now in place or those planned for future ATC systems, cannot be fully

[14]The 1996 Clinger-Cohen Act, Public Law No. 104-106, section 5125, 110 Stat. 684 (1996).

effective as long as FAA continues to function with significant physical security vulnerabilities. Also, because FAA has not assessed physical security controls at all facilities since 1993, it does not know how vulnerable they are.

Similarly, FAA does not know how vulnerable its operational ATC systems are and cannot adequately protect them until it performs the appropriate system risk assessments and certifies and accredits ATC systems. In addition, FAA is not effectively incorporating security controls into new ATC systems. FAA has taken preliminary steps to develop security guidance by forming the NIS group and estimating the cost to fill this void. However, until this group develops the guidance and the ATC development teams apply it, new ATC system development will not effectively address security issues.

Until FAA's three organizations responsible for ATC system security carry out their computer security responsibilities adequately, sensitive information is at risk of being compromised and flight services interrupted. Moreover, central security groups assigned to assist these organizations can only be successful if they have the authority to enforce their actions or a direct line to top management to ensure that needed changes can be implemented across organizational divisions. At FAA this central security group has neither. Finally, FAA's designated ATC system accrediting authority is inconsistent with federal guidance and sound management practices since this designee is not responsible for the daily operations of ATC systems.

Recommendations

Given the importance of physical security at the FAA facilities that house ATC systems, we recommend that the Secretary of Transportation direct the FAA Administrator to complete the following tasks:

- Develop and execute a plan to inspect the 187 ATC facilities that have not been inspected in over 4 years and correct any weaknesses identified so that these ATC facilities can be granted physical security accreditation as expeditiously as possible, but no later than April 30, 1999.
- Correct identified physical security weaknesses at inspected facilities so that these ATC facilities can be granted physical security accreditation as expeditiously as possible, but no later than April 30, 1999.
- Ensure that the required annual or triennial follow-up inspections are conducted, deficiencies are promptly corrected, and accreditation is kept current for all ATC facilities, as required by FAA policy.

Given the importance of operational ATC systems security, we recommend that the Secretary of Transportation direct the FAA Administrator to complete the following tasks:

- Assess, certify, and accredit all ATC systems, as required by FAA policy, as expeditiously as possible, but no later than April 30, 1999.
- Ensure that all systems are assessed, certified, and accredited at least every 3 years, as required by federal policy.

To improve security for future ATC modernization systems, we recommend that the Secretary of Transportation direct the FAA Administrator to ensure that

- specifications for all new ATC systems include security requirements based on detailed security assessments by requiring that security requirements be included as a criterion when FAA analyzes new systems for funding under its acquisition management system and
- the NIS group establishes detailed plans and schedules to develop a security architecture, a security concept of operations, and security standards and that these plans are implemented.

We further recommend that the Secretary report FAA physical security controls at its ATC facilities, operational ATC system security, and the lack of information security guidance (e.g., a security architecture, a security concept of operations, and security standards) as material internal control weaknesses in the department's fiscal year 1998 FMFIA report and in subsequent annual FMFIA reports until these problems are substantially corrected.

Finally, we recommend that the Secretary of Transportation direct the FAA Administrator to establish an effective management structure for developing, implementing, and enforcing ATC computer security policy. Given the importance and the magnitude of the information technology initiative at FAA, we are expanding on our earlier recommendation that a CIO management structure similar to the department-level CIOs as prescribed in the Clinger-Cohen Act be established for FAA[15] by recommending that FAA's CIO be responsible for computer security. We further recommend that the NIS group report to the CIO and that the CIO direct the NIS group to implement its plans. In addition, we recommend

[15]Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, Feb. 3, 1997) and Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, Mar. 21, 1997)

that the CIO designate a senior manager in Air Traffic Services to be the ATC operational accrediting authority.

We made two additional recommendations pertaining to operational ATC systems security in our "Limited Official Use" report.

Agency Comments and Our Evaluation

The Department of Transportation provided written comments on a draft of our "Limited Official Use" report. In summary, the department recognized that facility, systems, and data security are critical elements in FAA's management of the nation's ATC systems and that adequate physical security controls are important to ensure the safety of employees and ATC systems. The department agreed that required FAA inspections should be completed and said that immediate action had been directed to inspect and, where appropriate, accredit the 187 facilities identified in the draft report, that inspections had already been completed for about 100 of these facilities, and that completion of the remaining inspections was expected by June 1998.

However, the department did not state what, if any, specific action it would take on the remaining 14 recommendations. Further, while the department did not dispute any of the facts presented, it offered alternative interpretations of some of them. For example, the department did not agree that FAA's management of computer security has been inappropriate or that ATC systems are vulnerable to the point of jeopardizing flight safety. In addition, the department stated that the report does not present a complete picture regarding decisions guiding FAA resource allocation in that it does not recognize the basis for FAA decisions to allocate resources to other concerns facing FAA, rather than to correcting computer security vulnerabilities. We do not agree with these alternative interpretations.

As discussed in the report, FAA's management of facility, systems, and data security is ineffective for the following reasons:

- Known physical security weakness persist at many ATC facilities, and FAA is unaware of weaknesses that may exist at another 187 facilities.
- FAA has not analyzed the threats and vulnerabilities, or developed safeguards to protect 87 of its 90 operational ATC computer systems and 8 of its 9 operational ATC telecommunications networks.
- FAA does not have a well-defined security architecture, a security concept of operations, or security standards, and does not consistently include

well formulated security requirements in specifications for new ATC systems.

- None of the three organizations responsible for ATC security have discharged their respective security responsibilities effectively: the Office of Civil Aviation Security has not adequately enforced FAA policies that require the assessment of (1) physical security controls at all ATC facilities and (2) vulnerabilities, threats, and safeguards of all operational ATC computer systems; the Office of Air Traffic Services has not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards; and the Office of Research and Acquisitions has not implemented FAA policy that requires it to formulate requirements for security in specifications for all new ATC modernization systems.

FAA has recognized for several years that its vulnerabilities could jeopardize, and have already jeopardized, flight safety. In its 1994 Telecommunications Plan, FAA states that vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety. Vulnerabilities that have jeopardized flight safety are discussed in our "Limited Official Use" report.

Finally, making judicious decisions regarding resource allocation requires a thorough understanding of relative levels of risk, as well as reliable estimates of costs. As we have reported, FAA has not fully assessed its security vulnerabilities and threats and does not understand its security risks. Further, since it has not formulated countermeasures, it cannot reliably estimate the cost to mitigate the risks. As a result, FAA has no analytical basis for its decisions not to allocate resources to security. In recent years, FAA has invested billions of dollars in failed efforts to modernize its ATC systems while critical security vulnerabilities went uncorrected.

The department's comments and our detailed evaluation of them are presented in our "Limited Official Use" report.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from its date. At that time, we will send copies to the Secretary of Transportation; the Director, Office of Management and Budget; the Administrator, Federal Aviation Administration; and interested congressional committees. Copies will be available to others upon request. If you have any questions about

this report, please call me at (202) 512-6253. I can also be reached by e-mail at *willemssenj.aimd@gao.gov*. Major contributors to this report are listed in appendix I.

Joel C. Willemssen
Director, Civil Agencies Information Systems

Appendix I

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Dr. Rona B. Stillman, Chief Scientist for Computers and Telecommunications Keith A. Rhodes, Technical Director Randolph C. Hite, Senior Assistant Director Colleen M. Phillips, Assistant Director Hai V. Tran, Technical Assistant Director Nabajyoti Barkakati, Technical Assistant Director David A. Powner, Evaluator-in-Charge Barbarol J. James, ADP/Telecommunications Analyst

United States General Accounting Office

GAO

Accounting and Information Management Division

May 1998

Executive Guide

Information Security Management

Learning From Leading Organizations

GAO/AIMD-98-68

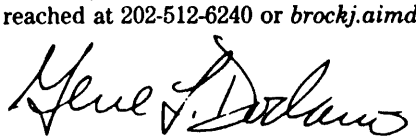
Preface

Increased computer interconnectivity and the popularity of the Internet are offering organizations of all types unprecedented opportunities to improve operations by reducing paper processing, cutting costs, and sharing information. However, the success of many of these efforts depends, in part, on an organization's ability to protect the integrity, confidentiality, and availability of the data and systems it relies on.

Deficiencies in federal information security are a growing concern. In a February 1997 series of reports to the Congress, GAO designated information security as a governmentwide high-risk area. In October 1997, the President's Commission on Critical Infrastructure Protection described the potentially devastating implications of poor information security from a broader perspective in its report entitled Critical Foundations: Protecting America's Infrastructures. Since then, audit reports have continued to identify widespread information security weaknesses that place critical federal operations and assets at risk.

Although many factors contribute to these weaknesses, audits by GAO and Inspectors General have found that an underlying cause is poor security program management. To help identify solutions to this problem, Senators Fred Thompson and John Glenn, Chairman and Ranking Minority Member, respectively, of the Senate Committee on Governmental Affairs, requested that we study organizations with superior security programs to identify management practices that could benefit federal agencies. This guide outlines the results of that study. It is intended to assist federal officials in strengthening their security programs, and we are pleased that it has been endorsed by the federal Chief Information Officers Council.

This guide is one of a series of GAO publications, listed in appendix I, that are intended to define actions federal officials can take to better manage their information resources. It was prepared under the direction of Jack L. Brock, Director, Governmentwide and Defense Information Systems, who can be reached at 202-512-6240 or *brockj.aimd@gao.gov*.



Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

A Message From the Federal Chief Information Officers Council

Washington
April 7, 1998

A high priority of the CIO Council is to ensure the implementation of security practices within the Federal government that gain public confidence and protect government services, privacy, and sensitive and national security information. This Executive Guide, "Information Security Management, Learning From Leading Organizations," clearly illustrates how leading organizations are successfully addressing the challenges of fulfilling that goal. These organizations establish a central management focal point, promote awareness, link policies to business risks, and develop practical risk assessment procedures that link security to business needs. This latter point–the need to link security to business requirements–is particularly important, and is illustrated in a statement of a security manager quoted in the guide: "Because every control has some cost associated with it, every control needs a business reason to be put in place."

The CIO Council is pleased to endorse the principles and best practices embodied in this guide. Its findings underscore the policies articulated in Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources." We expect that it will be a valuable resource for all agency CIOs and program managers who execute those policies, and will complement the other activities of the Council to improve Federal information systems security.

We look forward to working with the General Accounting Office in the future as we implement these best practices to further enhance agency security practices and programs.

G. Edward DeSeve
Acting Deputy Director for Management
U.S. Office of Management and Budget
and Chair, CIO Council

James J. Flyzik
Chief Information Officer
U.S. Department of the Treasury
and Vice Chair, CIO Council

Contents

Abbreviations

CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
GAO	General Accounting Office
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

Federal Information Security Is A Growing Concern

Electronic information and automated systems are essential to virtually all major federal operations. If agencies cannot protect the availability, integrity, and, in some cases, the confidentiality, of this information, their ability to carry out their missions will be severely impaired. However, despite the enormous dependence on electronic information and systems, audits continue to disclose serious information security weaknesses. As a result, billions of dollars in federal assets are at risk of loss, vast amounts of sensitive data are at risk of inappropriate disclosure, and critical computer-based operations are vulnerable to serious disruptions.

This guide is designed to promote senior executives' awareness of information security issues and to provide information they can use to establish a management framework for more effective information security programs. Most senior federal executives, like many of their private sector counterparts, are just beginning to recognize the significance of these risks and to fully appreciate the importance of protecting their information resources. The opening segments describe the problem of weak information security at federal agencies, identify existing federal guidance, and describe the issue of information security management in the context of other information technology management issues. The remainder of the guide describes 16 practices, organized under five management principles, that GAO identified during a study of nonfederal organizations with reputations for having good information security programs. Each of these practices contains specific examples of the techniques used by these organizations to increase their security program's effectiveness.

Potential Risks Are Significant

Although they have relied on computers for years, federal agencies, like businesses and other organizations throughout the world, are experiencing an explosion in the use of electronic data and networked computer systems. As a result, agencies have become enormously dependent on these systems and data to support their operations.

The Department of Defense, alone, has a vast information infrastructure that includes 2.1 million computers and over 10,000 networks that are used to

exchange electronic messages, obtain data from remote computer sites, and maintain critical records. Civilian agencies also are increasingly reliant on automated, often interconnected, systems, including the Internet, to support their operations. For example,

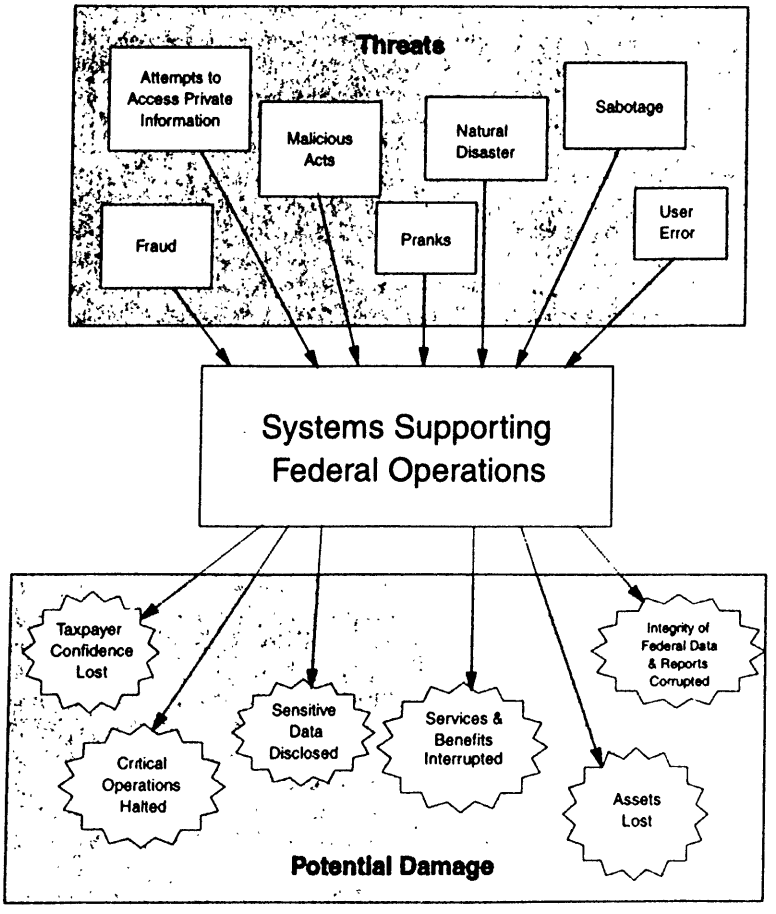
- law enforcement officials throughout the United States and Canada rely on the Federal Bureau of Investigation's National Crime Information Center computerized database for access to sensitive criminal justice records on individual offenders;
- the Internal Revenue Service relies on computers to process and store hundreds of millions of confidential taxpayer records;
- the Customs Service relies on automated systems to support its processing and inspection of hundreds of billions of dollars worth of imported goods; and
- many federal agencies, such as the Social Security Administration, the Department of Agriculture, and the Department of Health and Human Services, rely on automated systems to manage and distribute hundreds of billions of dollars worth of payments to individuals and businesses, such as medicare, social security, and food stamp benefits.

Although these advances promise to streamline federal operations and improve the delivery of federal services, they also expose these activities to greater risks. This is because automated systems and records are fast replacing manual procedures and paper documents, which in many cases are no longer available as "backup" if automated systems should fail.

This risk is exacerbated because, when systems are interconnected to form networks or are accessible through public telecommunication systems, they are much more vulnerable to anonymous intrusions from remote locations. Also, much of the information maintained by federal agencies, although unclassified, is extremely sensitive, and many automated operations are attractive targets for individuals or organizations with malicious intentions, such as committing fraud for personal gain or sabotaging federal operations. Several agencies have experienced intrusions into their systems, and there are indications, such as tests at the Department of Defense, that the number of attacks is growing and that many attacks are not detected.

Additional risks stem from agency efforts to examine and adjust their computer systems to ensure that they properly recognize the Year 2000. These Year 2000 conversion efforts are often conducted under severe time constraints that, without adequate management attention, could result in a weakening of controls over the integrity of data and programs and over the confidentiality of sensitive data.

Information Security Risks



Weaknesses Abound, but Management Attention Has Been Lacking

> *"Just as in the private sector, many federal agencies are reluctant to make the investments required in this area [of computer security] because of limited budgets, lack of direction and prioritization from senior officials, and general ignorance of the threat."*
>
> – Statement of Gary R. Bachula, Acting Under Secretary for Technology, Department of Commerce, before House Science Subcommittee on Technology, June 19, 1997

Unfortunately, federal agencies are not adequately protecting their systems and data. In September 1996, we reported that audit reports and agency self-assessments issued during the previous 2 years showed that weak information security was a widespread problem.[1] Specifically, weaknesses such as poor controls over access to data and inadequate disaster recovery plans increased the risk of losses, inappropriate disclosures, and disruptions in service associated with the enormous amounts of electronically maintained information essential for delivering federal services and assessing the success of federal programs. Due to these previously reported weaknesses and findings resulting from our ongoing work, in February 1997, we designated information security as a new governmentwide high-risk issue.[2]

In our September 1996 report, we stated that an underlying cause of federal information security weaknesses was that agencies had not implemented information security programs that (1) established appropriate policies and controls and (2) routinely monitored their effectiveness. Despite repeated reports of serious problems, senior agency officials had not provided the management attention needed to ensure that their information security programs were effective.

Also, in that report, we made a number of recommendations intended to improve the Office of Management and Budget's (OMB) oversight of agency information security practices and strengthen its leadership role in this area. Specifically, we recommended that OMB promote the federal Chief Information Officers Council's adoption of information security as one of its top priorities and encourage the council to develop a strategic plan for increasing awareness of the importance of information security, especially among senior agency executives, and improving information security program management

---

[1] Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996).

[2] High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

governmentwide. Initiatives that we suggested for the CIO Council to consider incorporating in its strategic plan included

- developing information on the existing security risks associated with nonclassified systems currently in use,
- developing information on the risks associated with evolving practices, such as Internet use,
- identifying best practices regarding information security programs so that they can be adopted by federal agencies,
- establishing a program for reviewing the adequacy of individual agency information security programs using interagency teams of reviewers,
- ensuring adequate review coverage of agency information security practices by considering the scope of various types of audits and reviews performed and acting to address any identified gaps in coverage,
- developing or identifying training and certification programs that could be shared among agencies, and
- identifying proven security tools and techniques.

Since September 1996, the CIO Council, under OMB's leadership, has taken some significant actions, which include designating information security as one of six priority areas and establishing a Security Committee. The Security Committee, in turn, has developed a preliminary plan for addressing various aspects of the problem, established links with other federal entities involved in security issues, held a security awareness day for federal officials, and begun exploring ways to improve federal incident response capabilities.

Although there is more that OMB and the CIO Council can do, information security is primarily the responsibility of individual agencies. This is because agency managers are in the best position to assess the risks associated with their programs and to develop and implement appropriate policies and controls to mitigate these risks. Accordingly, in our reports over the last several years, we have made dozens of specific recommendations to individual agencies. Although many of these recommendations have been implemented, similar weaknesses continue to surface because agencies have not implemented a management framework for overseeing information security on an agencywide and ongoing basis. A list of our previous reports and testimonies on information security is provided at the end of this guide.

Requirements Are Outlined in Laws and Guidance

The need for federal agencies to protect sensitive and critical, but unclassified, federal data has been recognized for years in various laws, including the Privacy Act of 1974, the Paperwork Reduction Act of 1995, and the Computer

Security Act of 1987. Further, since enactment of the original Paperwork Reduction Act in 1980, OMB has been responsible for developing information security guidance and overseeing agency practices, and the Computer Security Act assigns the National Institute of Standards and Technology (NIST) primary responsibility for developing technical standards and providing related guidance. OMB, NIST, and agency responsibilities regarding information security were recently reemphasized in the Clinger-Cohen Act of 1996, formerly named the Information Technology Management Reform Act of 1996.
The adequacy of controls over computerized data is also addressed indirectly by the Federal Managers' Financial Integrity Act of 1982 and the Chief Financial Officers Act of 1990. The Federal Managers' Financial Integrity Act requires agency managers to annually evaluate their internal control systems and report to the President and the Congress any material weaknesses that could lead to fraud, waste, and abuse in government operations. The Chief Financial Officers Act requires agencies to develop and maintain financial management systems that provide complete, reliable, consistent, and timely information.

In addition, a considerable body of federal guidance on information security has been developed. OMB has provided guidance since 1985 in its Circular A-130, Appendix III, Security of Federal Automated Information Resources, which was updated in February 1996. Further, NIST has issued numerous Federal Information Processing Standards, as well as a comprehensive description of basic concepts and techniques entitled An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, December 1995, and Generally Accepted Principles and Practices for Securing Information Technology Systems,[3] published in September 1996.

Additional federal requirements have been established for the protection of information that has been classified for national security purposes. However, these requirements are not discussed here because this guide pertains to the protection of sensitive but unclassified data, which constitute the bulk of data supporting most federal operations.

Exploring Practices of Leading Organizations

To supplement our ongoing audit work at federal agencies and gain a broader understanding of how information security programs can be successfully implemented, we studied the management practices of eight nonfederal

[3]Appendix II lists the principles identified in NIST's Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.

organizations recognized as having strong information security programs. The specific objective of our review was to determine how such organizations have designed and implemented their programs in order to identify practices that could be applied at federal agencies.

We focused primarily on the management framework that these organizations had established rather than on the specific controls that they had chosen, because previous audit work had identified security management as an underlying problem at federal agencies. Although powerful technical controls, such as those involving encryption, are becoming increasingly available to facilitate information security, effective implementation requires that these techniques be thoughtfully selected and that their use be monitored and managed on an ongoing basis. In addition, there are many aspects of information security, such as risk assessment, policy development, and disaster recovery planning, that require coordinated management attention.

To identify leading organizations, we reviewed professional literature and research information and solicited suggestions from experts in professional organizations, nationally known public accounting firms, and federal agencies. In selecting organizations to include in our study, we relied primarily on recommendations from the Computer Security Institute and public accounting firms because they were in a position to evaluate and compare information security programs at numerous organizations. In addition, we attempted to select organizations from a variety of business sectors to gain a broad perspective on the information security practices being employed. After initial conversations with a number of organizations, we narrowed our focus to eight organizations that had implemented fairly comprehensive organizationwide information security programs. All were prominent nationally known organizations. They included a financial services corporation, a regional electric utility, a state university, a retailer, a state agency, a nonbank financial institution, a computer vendor, and an equipment manufacturer. The number of computer users at these organizations ranged from 3,500 to 100,000, and four had significant international operations. Because most of the organizations considered discussions of their security programs to be sensitive and they wanted to avoid undue public attention on this aspect of their operations, we agreed not to identify the organizations by name.

We obtained information primarily through interviews with senior security managers and document analysis conducted during and after visits to the organizations we studied. In a few cases, we toured the organizations' facilities and observed practices in operation. We supplemented these findings, to a very limited extent, with information obtained from others. For example, at the state agency, we also met with a statewide security program official and with state auditors. In addition, we asked the Computer Security Institute to

query its members about their efforts to measure the effectiveness of their security programs in order to gain a broader perspective of practices in this area.

To determine the applicability of the leading organization's practices to federal agencies, we discussed our findings with numerous federal officials, including officials in OMB's Information Policy and Technology Branch, the Computer Security Division of NIST's Information Technology Laboratory, CIO Council members, the chairman of the Chief Financial Officers Council's systems subcommittee, information security officers from 15 federal agencies, and members of the President's Commission on Critical Infrastructure Protection. Further, we discussed our findings with our Executive Council on Information Management and Technology, a group of executives with extensive experience in information technology management who advise us on major information management issues affecting federal agencies.

Throughout the guide, we make several observations on federal information security practices in order to contrast them with the practices of the non-federal organizations we studied. These observations are based on the body of work we have developed over the last several years and on our recent discussions with federal information security officers and other federal officials who are knowledgeable about federal information security practices.

Although we attempted to be as thorough as possible within the scope of our study, we recognize that more work in this area remains to be done, including a more in-depth study of individual practices. We also recognize that the practices require customized application at individual organizations depending on factors such as existing organizational strengths and weaknesses.

Security as an Element of a Broader Information Management Strategy

Although this guide focuses on information security program management, this is only one aspect of an organization's overall information management strategy. As such, an organization's success in managing security-related efforts is likely to hinge on its overall ability to manage its use of information technology. Unfortunately, federal performance in this broader area has been largely inadequate. Over the past 6 years, federal agencies have spent a reported $145 billion on information technology with generally disappointing mission-related results.

Recognizing the need for improved information management, the Congress has enacted legislation that is prompting landmark reforms in this area. In

particular, the Paperwork Reduction Act of 1995 emphasized the need for agencies to acquire and apply information resources to effectively support the accomplishment of agency missions and the delivery of services to the public. The Clinger-Cohen Act of 1996 repeated this theme and provided more detailed requirements. These laws emphasize involving senior executives in information management decisions, appointing senior-level chief information officers, and using performance measures to assess the contribution of technology in achieving mission results. Although their primary focus is much broader, both of these laws specify security as one of the aspects of information management that must be addressed. This environment of reform is conducive to agencies rethinking their security programs, as part of broader information management changes, and considering the implementation of the practices that have been adopted by nonfederal organizations.

Other Issues Affecting Federal Information Security

Security program management and the related implementation of controls over access to data, systems, and software programs, as well as service continuity planning, are central factors affecting an organization's ability to protect its information resources and the program operations that these resources support. However, there are numerous policy, technical, legal, and human resource issues that are not fully within the control of officials at individual agencies. These issues are currently being debated and, in many cases, addressed by private-sector and federal efforts. They include, but are not limited to, matters concerning (1) the use of encryption to protect the confidentiality of information and other cryptographic capabilities, including digital signatures and integrity checks, (2) personal privacy, (3) the adequacy of laws protecting intellectual property and permitting investigations into computer-related crimes, and (4) the availability of adequate technical expertise and security software tools.

These topics are beyond the scope of this guide and, thus, are not discussed herein. However, it is important to recognize that strengthening information security requires a multifaceted approach and sometimes involves issues that are beyond the control of individual businesses and agencies. Although the management practices described in this guide are fundamental to improving an organization's information security posture, they should be considered in the context of this broader spectrum of issues.

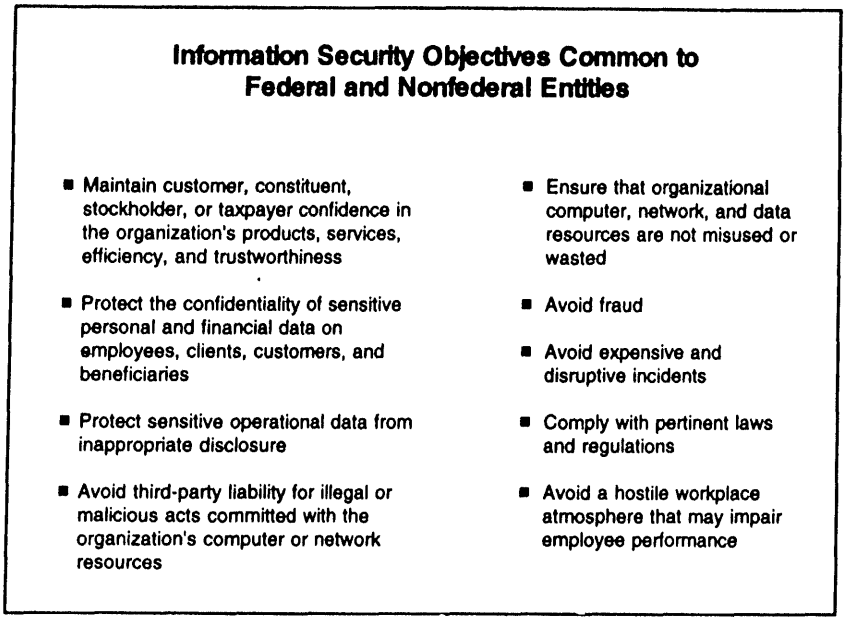
Leading Organizations Apply Fundamental Risk Management Principles

The organizations we studied were striving to manage the same types of risks that face federal agencies. To do so, they had responded to these risks by reorienting their security programs from relatively low-profile operations focused primarily on mainframe security to visible, integral components of their organizations' business operations. Because of the similarities in the challenges they face, we believe that federal entities can learn from these organizations to develop their own more effective security programs.

Federal and Nonfederal Entities Face Similar Risks and Rely on Similar Technologies

Like federal agencies, the organizations we studied must protect the integrity, confidentiality, and availability of the information resources they rely on. Although most of the organizations were private enterprises motivated by the desire to earn profits, their information security concerns focused on providing high-quality reliable service to their customers and business partners, avoiding fraud and disclosures of sensitive information, promoting efficient operations, and complying with applicable laws and regulations. These are the same types of concerns facing federal agencies.

Also, like federal agencies, the organizations relied, to varying degrees, on a mix of mainframe and client-server systems and made heavy use of interconnected networks. In addition, all were either using or exploring the possibilities of using the Internet to support their business operations.


Information Security Objectives Common to Federal and Nonfederal Entities
Maintain customer, constituent, stockholder, or taxpayer confidence in the organization's products, services, efficiency, and trustworthiness
Protect the confidentiality of sensitive personal and financial data on employees, clients, customers, and beneficiaries
Protect sensitive operational data from inappropriate disclosure
Avoid third-party liability for illegal or malicious acts committed with the organization's computer or network resources
Ensure that organizational computer, network, and data resources are not misused or wasted
Avoid fraud
Avoid expensive and disruptive incidents
Comply with pertinent laws and regulations
Avoid a hostile workplace atmosphere that may impair employee performance

Risk Management Principles Provide A Framework for an Effective Information Security Program

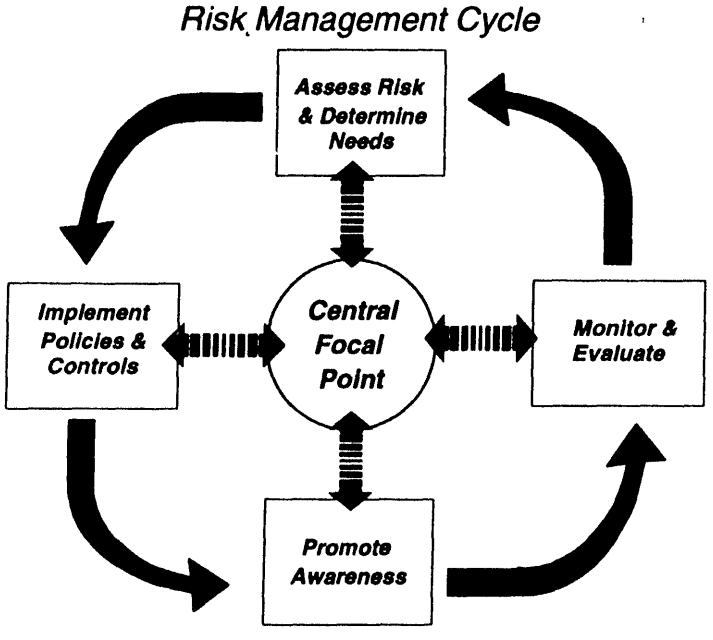
Although the nature of their operations differed, the organizations all had embraced five risk management principles, which are listed in the box below. These principles guided the organizations' efforts to manage the risk associated with the increasingly automated and interconnected environment in which they functioned.

Risk Management Principles Implemented by Leading Organizations

- **Assess risk and determine needs**
- **Establish a central management focal point**
- **Implement appropriate policies and related controls**
- **Promote awareness**
- **Monitor and evaluate policy and control effectiveness**

An important factor in effectively implementing these principles was linking them in a cycle of activity that helped ensure that information security policies addressed current risks on an ongoing basis. The single most important factor in prompting the establishment of an effective security program was a general recognition and understanding among the organization's most senior executives of the enormous risks to business operations associated with relying on automated and highly interconnected systems. However, risk assessments of individual business applications provided the basis for establishing policies and selecting related controls. Steps were then taken to increase the awareness of users concerning these risks and related policies. The effectiveness of controls and awareness activities was then monitored through various analyses, evaluations, and audits, and the results provided input to subsequent risk assessments, which determined if existing policies and controls needed to be modified. All of these activities were coordinated through a central security management office or group the staff of which served as consultants and

facilitators to individual business units and senior management. This risk management cycle is illustrated in the diagram below.

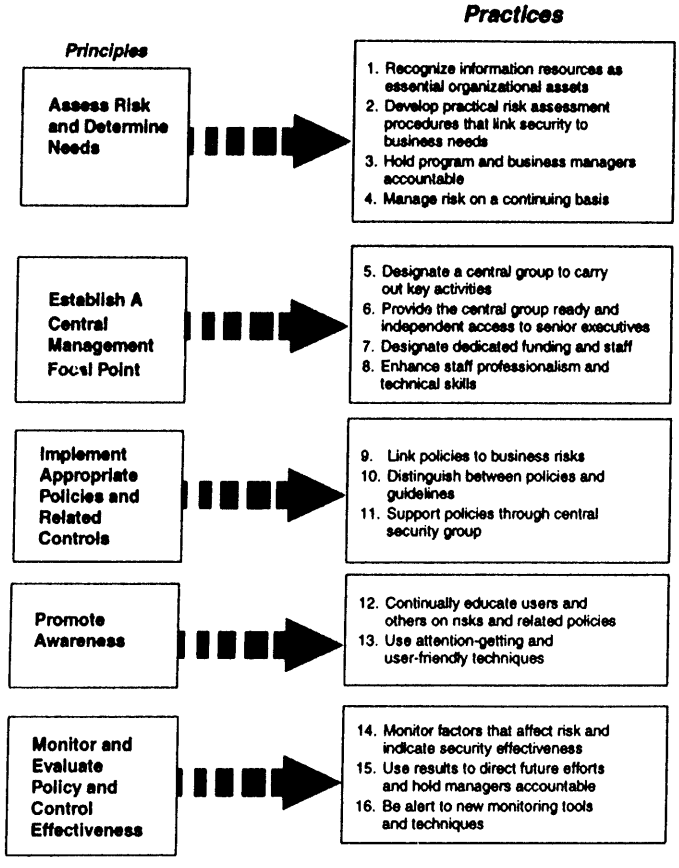


This continuing cycle of monitoring business risks, maintaining policies and controls, and monitoring operations parallels the process associated with managing the controls associated with any type of program. In addition, these principles should be familiar to federal agency officials since they have been emphasized in much of the recent guidance pertaining to federal information security. Most notably, they incorporate many of the concepts included in NIST's September 1996 publication, Generally Accepted Principles and Practices for Securing Information Technology Systems, and in OMB's February 1996 revision of Circular A-130, Appendix III, Security of Federal Automated Information Resources.

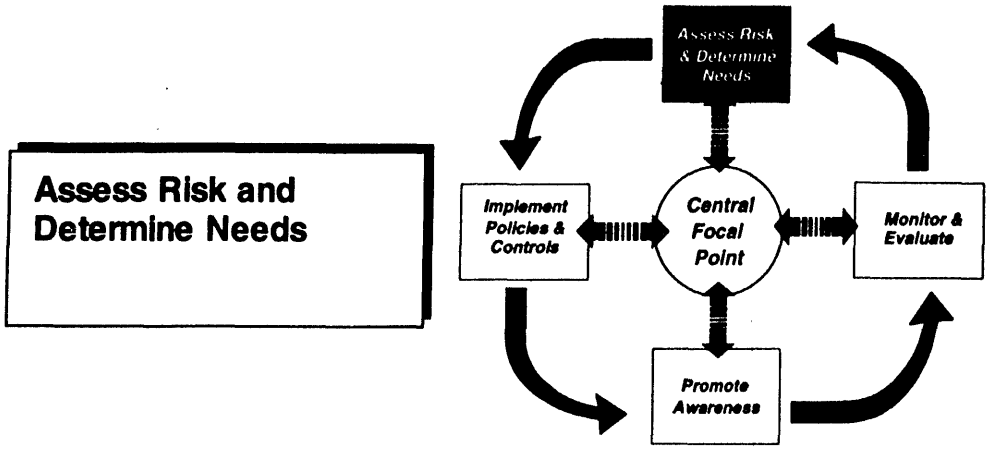
Principles Were Implemented Though Similar Practices

The organizations had developed similar sets of practices to implement the five risk management principles, although the techniques they employed varied depending on each organization's size and culture. Some programs were less mature than others and had not fully implemented all of the practices. However, security managers at each organization agreed that the 16 practices outlined in the following illustration, which relate to the five risk management principles, were key to the effectiveness of their programs.

Sixteen Practices Employed by Leading Organizations To Implement the Risk Management Cycle



The following pages provide a more detailed discussion of these practices and illustrative examples of the techniques used to implement them by the organizations we studied. The discussion follows the order of the practices as outlined above. Individual agency priorities for adopting the practices will vary depending on their existing security programs.



"We are not in the business of protecting information. We only protect information insofar as it supports the business needs and requirements of our company."
– Senior security manager at a major electric utility

All of the organizations said that risk considerations and related cost-benefit trade-offs were a primary focus of their security programs. Security was not viewed as an end in itself, but as a set of policies and related controls designed to support business operations, much like other types of internal controls.[4]

Controls were identified and implemented to address specific business risks. As one organization's security manager said, "Because every control has some cost associated with it, every control needs a business reason to be put in place." Regardless of whether they were analyzing existing or proposed operations, security managers told us that identifying and assessing information security risks in terms of the impact on business operations was an essential step in determining what controls were needed and what level of resources could be expended on controls. In this regard, understanding the business risks associated with information security was the starting point of the risk management cycle.

---

[4]In GAO's recently revised Standards for Internal Control in the Federal Government, Exposure Draft (GAO/AIMD-98-21.3.1, December 1997), controls over computerized information and information processing are discussed in the context of the larger body of an agency's internal control activities.

Practice 1: Recognize Information Resources as Essential Organizational Assets That Must Be Protected

"Information technology is an integral and critical ingredient for the successful functioning of major U.S. companies."
– Deloitte & Touche LLP Survey of American Business Leaders, November 1996

The organizations we studied recognized that information and information systems were critical assets essential to supporting their operations that must be protected. As a result, they viewed information protection as an integral part of their business operations and of their strategic planning.

Senior Executive Support Is Crucial

In particular, senior executive recognition of information security risks and interest in taking steps to understand and manage these risks were the most important factors in prompting development of more formal information security programs. Such high-level interest helped ensure that information security was taken seriously at lower organizational levels and that security specialists had the resources needed to implement an effective program.

This contrasts with the view expressed to us by numerous federal managers and security experts that many top federal officials have not recognized the indispensable nature of electronic data and automated systems to their program operations. As a result, security-related activities intended to protect these resources do not receive the resources and attention that they merit.

In some cases, senior management's interest had been generated by an incident that starkly illustrated the organization's information security vulnerabilities, even though no damage may have actually occurred. In other cases, incidents at other organizations had served as a "wake-up call." Two organizations noted that significant interest on the part of the board of directors was an important factor in their organizations' attention to information security. However, security managers at many of the organizations told us that their chief executive officers or other very senior executives had an ongoing interest in information technology and security, which translated into an organizationwide emphasis on these areas.

Although the emphasis on security generally emanated from top officials, security specialists at lower levels nurtured this emphasis by keeping them

abreast of emerging security issues, educating managers at all levels, and by emphasizing the related business risks to their own organizations.

Security Seen As An Enabler

In addition, most of the organizations were aggressively exploring ways to improve operational efficiency and service to customers through new or expanded applications of information technology, which usually prompted new security considerations. Officials at one organization viewed their ability to exploit information technology as giving them a significant competitive advantage. In this regard, several organizations told us that security was increasingly being viewed as an enabler–a necessary step in mitigating the risks associated with new applications involving Internet use and broadened access to the organization's computerized data. As a result, security was seen as an important component in improving business operations by creating opportunities to use information technology in ways that would not otherwise be feasible.

Practice 2: Develop Practical Risk Assessment Procedures That Link Security to Business Needs

The organizations we studied had tried or were exploring various risk assessment methodologies, ranging from very informal discussions of risk to fairly complex methods involving the use of specialized software tools. However, the organizations that were the most satisfied with their risk assessment procedures were those that had defined a relatively simple process that could be adapted to various organizational units and involved a mix of individuals with knowledge of business operations and technical aspects of the organization's systems and security controls.

The manufacturing company had developed an automated checklist that asked business managers and relevant staff in individual units a series of questions that prompted them to consider the impact of security controls, or a lack thereof, on their unit's operations. The results of the analysis were reported in a letter to senior management that stated the business unit's compliance with the security policy, planned actions to become compliant, or willingness to accept the risk. The results were also reported to the internal auditors, who used them as a basis for reviewing the business unit's success in implementing the controls that the unit's managers had determined were needed. Through the reporting procedure, the business managers took responsibility for either tolerating or mitigating security risks associated with their operations.

Such procedures provided a relatively quick and consistent means of exploring risk with business managers, selecting cost-effective controls, and documenting conclusions and business managers' acceptance of final determinations regarding what controls were needed and what risks could be tolerated. With similar objectives in mind, the utility company had developed a streamlined risk assessment process that brought together business managers and technical experts to discuss risk factors and mitigating controls. (This process is described in detail as a case example on page 28.)

Other organizations had developed less formal and comprehensive techniques for ensuring that risks were considered prior to changes in operations.

- The retailer had established standard procedures for requesting and granting new network connections. Under these procedures, documentation about the business need for the proposed connection and the risks associated with the proposed connection had to be submitted in writing prior to consideration by the central security group. Then, a meeting between the technical group, which implemented new connections, the requester, and the central security group was held to further explore the issue. The documentation and meeting helped

ensure that the requester's business needs were clearly understood and the best solution was adopted without compromising the network's security.

- The financial services corporation had implemented procedures for documenting business managers' decisions to deviate from organizationwide policies and standards. In order to deviate from a "mandatory policy," the business unit prepared a letter explaining the reason for the deviation and recognizing the related risk. Both the business unit executive and the central security group manager signed the letter to acknowledge their agreement to the necessity of the policy deviation. Deviations from less rigid "standards" were handled similarly, although the letter could be signed by the business unit executive, alone, and did not require the central security group's approval, though it was generally received. In all cases, the central security group discussed the information security implications of the deviation with the appropriate executive and signed-off only when it was satisfied that the executives fully understood the risk associated with the deviation. However, the ultimate decision on whether a deviation from policies or standards was appropriate was usually left to the business unit.

Organizations Saw Benefits Despite Lack of Precision

"Actual losses are not necessarily good indications of risk."
– Security manager at a prominent financial institution

Although all of the organizations placed emphasis on understanding risks, none attempted to precisely quantify them, noting that few quantified data are available on the likelihood of an incident occurring or on the amount of damage that is likely to result from a particular type of incident. Such data are not available because many losses are never discovered and others are never reported, even within the organizations where they occurred. In addition, there are limited data on the full costs of damage caused by security weaknesses and on the operational costs of specific control techniques. Further, due to fast-paced changes in technology and factors such as the tools available to would-be intruders, the value of applying data collected in past years to the current environment is questionable. As a result, it is difficult, if not impossible, to precisely compare the cost of controls with the risk of loss in order to determine which controls are the most cost-effective. Ultimately, business managers and security specialists must rely on the best information available and their best judgment in determining what controls are needed.

Despite their inability to precisely compare the costs of controls with reductions in risk, the organizations said that risk assessments still served their primary purpose of ensuring that the risk implications of new and existing applications were explored. In particular, the security managers believed that adequate information was available to identify the most significant risks. For example, in addition to their own organization's experience, they noted that information on threats, specific software vulnerabilities, and potential damage was widely available in technical literature, security bulletins from organizations such as the Carnegie-Mellon Computer Emergency Response Team (CERT), surveys done by professional associations and audit firms, and discussion groups. Although much of this information was anecdotal, the security managers thought that it was sufficient to give them a good understanding of the threats of concern to their organizations and of the potential for damage.

In addition, the lack of quantified results did not diminish the value of risk assessments as a tool for educating business managers. By increasing the understanding of risks, risk assessments (1) improved business managers' ability to make decisions on controls needed, in the absence of quantified risk assessment results, and (2) engendered support for policies and controls adopted, thus helping to ensure that policies and controls would operate as intended.

Practice 3: Hold Program and Business Managers Accountable

"Holding business managers accountable and changing the security staff's role from enforcement to service has been a major paradigm shift for the entire company."

– Security manager at a major equipment manufacturer

The organizations we studied were unanimous in their conviction that business managers must bear the primary responsibility for determining the level of protection needed for information resources that support business operations. In this regard, most held the view that business managers should be held accountable for managing the information security risks associated with their operations, much as they would for any other type of business risk. However, security specialists played a strong educational and advisory role and had the ability to elevate discussions to higher management levels when they believed that risks were not being adequately addressed.

Business managers, usually referred to as program managers in federal agencies, are generally in the best position to determine which of their information resources are the most sensitive and what the business impact of a loss of integrity, confidentiality, or availability would be. Business or program managers are also in the best position to determine how security controls may impair their operations. For this reason, involving them in selecting controls can help ensure that controls are practical and will be implemented.

Accordingly, security specialists had assumed the role of educators, advisors, and facilitators who helped ensure that business managers were aware of risks and of control techniques that had been or could be implemented to mitigate the risks. For several of the organizations, these roles represented a dramatic reversal from past years, when security personnel were viewed as rigid, sometimes overly protective enforcers who often did not adequately consider the effect of security controls on business operations.

Some of the organizations had instituted mechanisms for documenting and reporting business managers' risk determinations. These generally required some type of sign-off on memoranda that either (1) reported deviations from predetermined control requirements, as was the case at the financial services corporation and the manufacturing company discussed previously or (2) provided the results of risk assessments, as was the case of the utility company described in the following case example. According to the security managers, such sign-off requirements helped ensure that business managers carefully considered their decisions before finalizing them.

Case Example: A Practical Method for Involving Business Managers in Risk Assessment

A major electric utility company has developed an efficient and disciplined process for ensuring that information security-related risks to business operations are considered and documented. The process involves analyzing one system or segment of business operation at a time and convening a team of individuals that includes business managers who are familiar with business information needs and technical staff who have a detailed understanding of potential system vulnerabilities and related controls. The sessions, which follow a standard agenda, are facilitated by a member of the central security group who helps ensure that business managers and technical staff communicate effectively and adhere to the agenda.

During the session, the group brainstorms to identify potential threats, vulnerabilities, and resultant negative impacts on data integrity, confidentiality, and availability. Then, they analyze the effects of such impacts on business operations and broadly categorize the risks as major or minor. The group does not usually attempt to obtain or develop specific numbers for threat likelihood or annual loss estimates unless the data for determining such factors are readily available. Instead, they rely on their general knowledge of threats and vulnerabilities obtained from national incident response centers, professional associations and literature, and their own experience. They believe that additional efforts to develop precisely quantified risks are not cost-effective because (1) such estimates take an inordinate amount of time and effort to identify and verify or develop, (2) the risk documentation becomes too voluminous to be of practical use, and (3) specific loss estimates are generally not needed to determine if a control is needed.

After identifying and categorizing risks, the group identifies controls that could be implemented to reduce the risk, focusing on the most cost-effective controls. As a starting point, they use a list of about 25 common controls designed to address various types of risk. Ultimately, the decision as to what controls are needed lies with the business managers, who take into account the nature of the information assets and their importance to business operations and the cost of controls.

The team's conclusions as to what risks exist and what controls are needed are documented along with a related action plan for control implementation. This document is then signed by the senior business manager and technical expert participating and copies are made available to all participant groups and to the internal auditors, who may later audit the effectiveness of the agreed upon controls.

Each risk analysis session takes approximately 4 hours and includes 7 to 15 people, though sessions with as many as 50 and as few as 4 people have occurred. Additional time is usually needed to develop the action plan. The information security group conducts between 8 and 12 sessions a month. According to the utility's central information security group, this process increases security awareness among business managers, develops support for needed controls, and helps integrate information security considerations into the organization's business operations.

Practice 4: Manage Risk on a Continuing Basis

> *"Information security is definitely a journey, not a destination--there are always new challenges to meet."*
>
> – Chief information security officer at a major financial services corporation

The organizations emphasized the importance of continuous attention to security to ensure that controls were appropriate and effective. They stressed that constant vigilance was needed to ensure that controls remained appropriate–addressing current risks and not unnecessarily hindering operations–and that individuals who used and maintained information systems complied with organizational policies.

Such attention is important for all types of internal controls, but it is especially important for security over computerized information, because, as mentioned previously, the factors that affect computer security are constantly changing in today's dynamic environment. Such changing factors include threats, systems technologies and configurations, known vulnerabilities in existing software, the level of reliance on automated systems and electronic data, and the sensitivity of such operations and data.

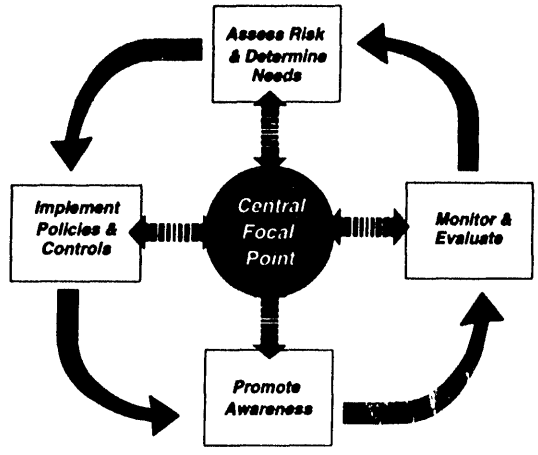
Existing Federal Guidance Provides a Framework for Implementing Risk Management Practices

OMB's 1996 revision of Circular A-130, Appendix III, recognizes that federal agencies have had difficulty in performing effective risk assessments–expending resources on complex assessments of specific risks with limited tangible benefits in terms of improved security. For this reason, the revised circular eliminates a long-standing federal requirement for formal risk assessments. Instead, it promotes a risk-based approach and suggests that, rather than trying to precisely measure risk, agencies focus on generally assessing and managing risks. This approach is similar to that used by the organizations we studied.

Similarly, the concept of holding program managers accountable underlies the existing federal process for accrediting systems for use. Accreditation is detailed in NIST's Federal Information Processing Standards Publication 102, Guideline for Computer Security Certification and Accreditation, which was published in 1983. According to NIST, accreditation is "the formal authorization by the management official for system operation and an explicit acceptance of risk." OMB's 1996 update to Circular A-130, Appendix III, provides similar guidance, specifying that a management official should authorize in writing the use of each system before beginning or significantly changing use of the system. "By authorizing processing in a system, a manager accepts the risks associated with it."

Getting Started--Assessing Risk and Determining Needs	
Senior Program Officials	Gain an understanding of the criticality and sensitivity of the information and systems that support key agency programs. Recognize that information security risks to program operations are potentially significant and support efforts to further explore and understand these risks as they relate to your agency's operations. Review discussions made by subordinate managers regarding the levels of information protection needed and take responsibility for making final determinations. Monitor implementation of the risk assessment process to ensure that it is providing benefits and does not evolve into a "paperwork exercise."
CIOs	Define risk assessment processes that involve senior program officials and require them to make final determinations regarding the level of information protection needed. Ensure that security specialists and other technical experts are available to educate and advise program officials regarding potential vulnerabilities and related controls.
Senior Security Officers	Promote and facilitate the risk assessment process by (1) developing practical risk assessment procedures and tools, (2) arranging for risk assessment sessions, (3) ensuring the involvement of key program and technical personnel, and (4) providing mechanisms for documenting final decisions. In promoting the adoption of policies and other controls, focus on the specific business reasons for the controls rather than on generic requirements.

Establish a Central Management Focal Point



"A central focal point is essential to spotting trends, identifying problem areas, and seeing that policies and administrative actions are handled in a consistent manner."
– Senior information security officer for a major university

"Information security has become too important to handle on an ad hoc basis."
– Security specialist at a major retailing company

Managing the increased risks associated with a highly interconnected computing environment demands increased central coordination to ensure that weaknesses in one organizational unit's systems do not place the entire organization's information assets at undue risk. Each of the organizations we studied had adopted this view and, within the last few years, primarily since 1993, had established a central security management group or reoriented an existing central security group to facilitate and oversee the organization's information security activities. As such, the central group served as the focal point for coordinating activities associated with the four segments of the risk management cycle.

As discussed in the previous section on risk analysis, the central security groups served primarily as advisers or consultants to the business units, and, thus, they generally did not have the ability to independently dictate information security practices. However, most possessed considerable "clout" across their organizations due largely to the support they received from their organization's senior management. In this regard, their views were

sought and respected by the organizations' business managers. The following case example describes how one organization strengthened its central security group and reoriented its focus.

Case Example: Transforming an Organization's Central Security Focal Point

In 1995, realizing that security was an essential element of its efforts to innovatively use information technology, a major manufacturer significantly reorganized and strengthened its central information security function. Prior to the reorganization, a central security group of about four individuals concentrated on mainframe security administration and had little interaction with the rest of the company. Since then, the central group has grown to include 12 individuals who manage the security of the company's (1) main network, (2) decentralized computer operations, and (3) Internet use. In addition, the group participates in the company's strategic planning efforts and in the early stages of software development projects to ensure that security implications of these efforts are addressed. In this regard, it serves as a communications conduit between management and the information systems staff who design, build, and implement new applications.

Members of the central group possess a variety of technical skills and have specific information security responsibilities, such as developing policy, maintaining the firewall that protects the organization's network from unauthorized intrusions, or supporting security staff assigned to individual business units. According to the group's manager, because of the shift in the central group's responsibilities, "the members of the group had to change their mind-set from a staff organization to a service organization. They had to be willing to work with business managers to enable rather than to control business operations."

Practice 5: Designate a Central Group to Carry Out Key Activities

Overall, the central security groups served as (1) catalysts for ensuring that information security risks were considered in both planned and ongoing operations, (2) central resources for advice and expertise to units throughout their organizations, and (3) a conduit for keeping top management informed about security-related issues and activities affecting the organization. In addition, these central groups were able to achieve some efficiencies and increase consistency in the implementation of the organization's security program by performing tasks centrally that might otherwise be performed by multiple individual business units.

Specific activities performed by central groups differed somewhat, primarily because they relied to a varying extent on security managers and administrators in subordinate units and on other organizationally separate groups, such as disaster recovery or emergency response teams. Examples of the most common activities carried out by central groups are described below.

- Developing and adjusting organizationwide policies and guidance, thus reducing redundant policy-related activities across the organization's units. For example, the manufacturer's central security group recently revamped the company's entire information security manual and dedicated one staff member to maintaining it.

- Educating employees and other users about current information security risks and helping to ensure consistent understanding and administration of policies through help-line telephone numbers, presentations to business units, and written information communicated electronically or through paper memos.

- Initiating discussions on information security risks with business managers and conducting defined risk assessment procedures.

- Meeting periodically with senior managers to discuss the security implications of new information technology uses being considered.

- Researching potential threats, vulnerabilities, and control techniques and communicating this information to others in the organization. Many of the organizations supplemented knowledge gained from their own experiences by frequently perusing professional publications, alerts, and other information available in print and through the Internet. Several mentioned the importance of networking with outside organizations, such as the International Information Integrity Institute, the European Security Forum, and the Forum of Incident Response and Security

Teams, to broaden their knowledge. One senior security officer noted, "Sharing information and solutions is important. Many organizations are becoming more willing to talk with outsiders about security because they realize that, despite differing missions and cultures, they all use similar technology and face many of the same threats."

- Monitoring various aspects of the organization's security-related activities by testing controls, accounting for the number and types of security incidents, and evaluating compliance with policies. The central groups often characterized these evaluative activities as services to the business units.

- Establishing a computer incident response capability, and, in some cases, serving as members of the emergency response team.

- Assessing risks and identifying needed policies and controls for general support systems, such as organizationwide networks or central data processing centers, that supported multiple business units. For example, some central groups controlled all new connections to the organization's main network, ensuring that the connecting network met minimum security requirements. Similarly, one organization's central group was instrumental in acquiring a strong user authentication system to help ensure that network use could be reliably traced to the individual users. Further, most central groups oversaw Internet use.

- Creating standard data classifications and related definitions to facilitate protection of data shared among two or more business units.

- Reviewing and testing the security features in both commercially developed software that was being considered for use and internally developed software prior to its being moved into production. For example, the manufacturing company's central group reviewed all new Internet related applications and had the authority to stop such applications from going into production if minimum security standards were not met. Similarly, the central information protection group at the utility was required to approve all new applications to indicate that risks had been adequately considered.

- Providing self-assessment tools to business units so that they could monitor their own security posture. For example, the financial services corporation provided business units with software tools and checklists so that they would assume responsibility for identifying and correcting weaknesses rather than depending on auditors to identify problems.

Practice 6: Provide the Central Group Ready and Independent Access to Senior Executives

Senior information security managers emphasized the importance of being able to discuss security issues with senior executives. Several noted that, to be effective, these senior executives had to be in a position to act and effect change across organizational divisions. The ability to independently voice security concerns to senior executives was viewed as important because such concerns could often be at odds with business managers' and system developers' desires to implement new computer applications quickly and avoid controls that would impede efficiency, user friendliness, and convenience. This ability to elevate significant security concerns to higher management levels helped ensure that risks were thoroughly understood and that decisions as to whether such risks should be tolerated were carefully considered before final decisions were made.

The organizational positions of the central groups varied. Most were located two levels below the Chief Information Officer (CIO). However, the groups reporting directly to the CIO or to an even more senior official viewed this as an advantage because it provided them greater independence. Several others said that, despite their lower organizational position, they felt free to contact their CIOs and other senior executives when important security issues arose, and they were relatively unrestrained by the need to "go through the chain of command." Some noted that senior managers frequently called them to discuss security issues. For example, at the nonbank financial institution, the senior security manager was organizationally placed two levels below the CIO, but she met independently with the CIO once every quarter. Also, during the first three months of 1997, she had met twice with the organization's chief executive officer, at his request, to discuss the security implications of new applications.

In contrast, several federal information security officials told us that they felt that their organizations were placed too low in the organizational structure to be effective and that they had little or no opportunity to discuss information security issues with their CIOs and other senior agency officials.

Rather than depend on the personal interest of individual senior managers, two of the organizations we studied had established senior-level committees to ensure that information technology issues, including information security, received appropriate attention. For example, the university's central group had created a committee of respected university technical and policy experts to discuss and build consensus about the importance of certain information security issues reported to senior management, thus lending weight and credibility to concerns raised by the central security office.

Practice 7: Designate Dedicated Funding and Staff

Unlike many federal agencies, the central groups we studied had defined budgets, which gave them the ability to plan and set goals for their organization's information security program. At a minimum, these budgets covered central staff salaries and training and security hardware and software. At one organization, business units could supplement the central group's resources in order to increase the central group's participation in high priority projects. While all of the central groups had staffs ranging from 3 to 17 people permanently assigned to the group, comparing the size of these groups is of limited value because of wide variations in the (1) sizes of the organizations we studied, (2) inherent riskiness of their operations, and (3) the additional support the groups received from other organizational components and from numerous subordinate security managers and administrators.

In particular, no two groups were alike regarding the extent of support they received from other organizational units. For example, the computer vendor relied on a security manager in each of the organization's four regional business units, while the utility's nine-member central group relied on 48 part-time information security coordinators at various levels within the company. Some central groups relied heavily on technical assistance located in another organizational unit, while others had significant technical expertise among their own staff, and, thus, were much more involved in directly implementing and testing controls.

Despite these differences, two key characteristics were common to each of the organizations: (1) information security responsibilities had been clearly defined for the groups involved and (2) dedicated staff resources had been provided to carry out these responsibilities. The following table summarizes the details on the size and structure of the organizations' information security staffs.

Placement and Staffing of Eight Central Information Security Management Groups

Organization	Approximate number of system users	Placement of central group	Number of dedicated central staff	Other staff resources relied on (some numbers are approximate)
Financial services corporation	70,000	Two levels below CEO	17	• 35 security officers in business units
Electric utility	5,000	One level below CIO	9	• 48 security coordinators at three levels throughout the organization • Virus response team • Administrators
State university	100,000	One level below CIO	3	• 170 LAN administrators • Technical committee • Policy committee • Incident handling team
Retailer	65,000	Two levels below CIO	12	• 2,000 distributed security administrators • Internal audit staff • Technical services group • Loss prevention staff
State agency	8,000	Two levels below CIO	8	• 25 district managers • Security administrators in 31 units • Individuals with specialized expertise in the information systems group
Nonbank financial institution	3,500	Two levels below CIO	7	• Central security administration group
Computer vendor	15,000	Three levels below CIO	4	• 27 regional security specialists
Equipment manufacturer	35,000	Several levels below CIO	12	• 70 site security administrators

Practice 8: Enhance Staff Professionalism and Technical Skills

The organizations had taken steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. In addition, they recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. Further, most of the organizations were striving to increase the professional stature of their staff in order to gain respect from others in their organizations and attract competent individuals to security-related positions.

Update Skills and Knowledge of Security Managers and Specialists

The training emphasis for staff in the central security management groups, many of whom came to their groups with significant technical expertise, was on keeping staff skills and knowledge current. This was accomplished primarily through attendance at technical conferences and specialized courses on topics such as the security features of new software, as well as networking with other security professionals and reviewing the latest technical literature and bulletins. To maximize the value of expenditures on external training and events, one central group required staff members who attended these events to brief others in the central group on what they had learned.

In an effort to significantly upgrade the expertise of information security officers in its various business units, the central group at the financial services corporation had recently arranged for an outside firm to provide 5 weeks of training for these individuals. The training, which is planned to take place in 1-week increments throughout the year, is expected to entail a broad range of security-related topics, including general information security, encryption, access control, and how to build a better working relationship with the corporation's technical information systems group.

Citing an emerging trend, the senior information security managers had also started to create information security career paths and stress professional certification for security specialists. In particular, many organizations were encouraging their staff to become Certified Information Systems Security Professionals (CISSP).[5] One security manager noted that security specialists

[5]The CISSP certification was established by the International Information Systems Security Certification Consortium. The consortium was established as a joint effort of several information security-related organizations, including the Information Systems Security Association and the Computer Security Institute, to develop a certification program for information security professionals.

also needed excellent communication skills if they were to effectively fulfill their roles as consultants and facilitators for business managers who were less technically expert regarding computers and telecommunications.

Educate System Administrators

Increasing the expertise of system administrators presented different challenges. System administrators are important because they generally perform day-to-day security functions, such as creating new system user accounts, issuing new passwords, and implementing new software. These tasks must be completed properly and promptly or controls, such as passwords and related access restrictions, will not provide the level of protection intended. In addition, system administrators are the first line of defense against security intrusions and are generally in the best position to notice unusual activity that may indicate an intrusion or other security incident. However, at the organizations we studied, as at federal agencies, security is often a collateral duty, rather than a full-time job, and the individuals assigned frequently have limited technical expertise. As a result, the effectiveness of individual system administrators in maintaining security controls and spotting incidents is likely to vary.

To enhance the technical skills of their security administrators and help ensure that all of them had the minimal skills needed, most of the groups had established special training sessions for them. For example,

- the manufacturer required new security administrators to spend 2 to 5 days in training with the central security group, depending on their technical skills, before they were granted authority to perform specific functions on the network, such as controlling the users' access rights;
- the central security group at the university held annual technical conferences for the university's systems administrators and engaged professional training organizations to offer on-campus training at very reduced rates; and
- the state agency held a biannual conference for systems administrators that included sessions related to their information security responsibilities.

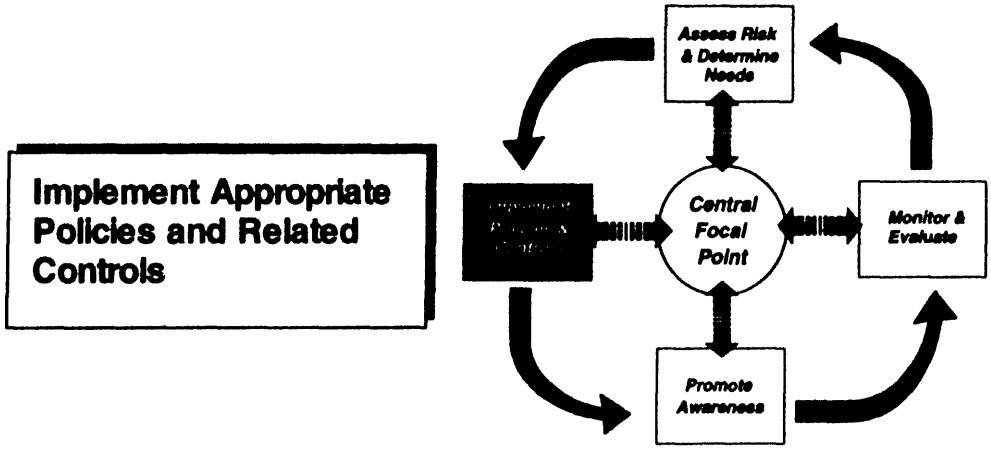
Attract and Keep Individuals with Technical Skills

Most of the groups cited maintaining or increasing the technical expertise among their security staff as a major challenge, largely due to the high demand

for information technology experts in the job market. In response, several said they offered higher salaries and special benefits to attract and keep expert staff. For example, the financial services corporation provided competitive pay based on surveys of industry pay levels, attempted to maintain a challenging work environment, and provided flexible work schedules and telecommuting opportunities that allowed most of the staff to work at home 1 day a week. In addition, provisions were made for staff to do the type of work they preferred, such as software testing versus giving presentations.

Organizations relied on both internally and externally developed and presented training courses, sometimes engaging contractors or others to assist. For example, the state information security office above the state agency worked with an information security professional organization to provide a relatively low-cost statewide training conference. The state organization provided meeting rooms and administrative support while the professional organization used its professional contacts to obtain knowledgeable speakers.

Getting Started--Establishing a Central Focal Point	
Senior Program Officials	Involve agency security specialists in the early planning stages of projects involving computer and/or network support. Be accessible to agency security experts and open to considering the information security implications of any operations.
CIOs	Establish a central group to serve as a center of knowledge and expertise on information security and to coordinate agencywide security-related activities. Provide the central group adequate funding for staff resources, training, and security software tools. Be accessible to agency security specialists. Involve agency security experts in the early planning stages of system development or enhancement projects. Support efforts to attract and retain individuals with needed technical skills.
Senior Security Officers	Develop training plans for increasing the expertise of security specialists and security administrators. Explore mechanisms for leveraging resources by drawing on the expertise of others within or outside of the agency. Develop methods for attracting and retaining individuals with needed technical skills.



The organizations viewed information security policies as the foundation of their information security programs and the basis for adopting specific procedures and technical controls. As with any area of operations, written policies are the primary mechanism by which management communicates its views and requirements to its employees, clients, and business partners. For information security, as with other types of internal controls, these views and requirements generally flow directly from risk considerations, as illustrated in the management cycle depicted above.

As discussed earlier, our discussions with the eight organizations focused on their methods for developing and supporting policies and guidelines. We did not discuss the specific controls they had implemented due to the proprietary and often highly technical nature of this information.

Practice 9: Link Policies to Business Risks

The organizations stressed the importance of up-to-date policies that made sense to users and others who were expected to understand them. Many senior security managers told us that prior to the recent strengthening of their security programs, their organization's information security policies had been neglected and out-of-date, thus failing to address significant risks associated with their current interconnected computing environment. As a result, developing a comprehensive set of policies was one of their first steps in establishing an effective corporatewide security program. In addition, they emphasized the importance of adjusting policies continually to respond to newly identified risks or areas of misunderstanding. For example,

- At the financial services corporation, the central security group routinely analyzed the causes of security weaknesses identified by management and by auditors in order to identify policy and related control deficiencies.
- The university had recently developed more explicit policies on system administrator responsibilities in recognition of the critical role of system administration in a distributed environment.
- The manufacturing company had recently drafted policies on security incident response after an incident had exposed shortfalls in the company's guidance in this area.

A relatively new risk area receiving particular attention in organizational policies was user behavior. Many policies are implemented and, to some extent, enforced by technical controls, such as logical access controls that prevent individuals from reading or altering data in an unauthorized manner. However, many information security risks cannot be adequately mitigated with technical controls because they are a function of user behavior. In a networked environment, these risks are magnified because a problem on one computer can affect an entire network of computers within minutes and because users are likely to have easier access to larger amounts of data and the ability to communicate quickly with thousands of others. For example, users may accidentally disclose sensitive information to a large audience through electronic mail or introduce damaging viruses that are subsequently transmitted to the organizations entire network of computers. In addition, some users may feel no compunction against browsing sensitive organizational computer files or inappropriate Internet sites if there is no clear guidance on what types of user behavior are acceptable.

To address these risks, many of which did not exist prior to extensive use of networks, electronic mail, and the Internet, the organizations had begun

placing more emphasis on user behavior in their policies and guidelines. For example, the university's policies went beyond the traditional warnings against password disclosure by including prohibitions against a variety of possible user actions. These included misrepresenting their identity in electronic communications and conducting and promoting personal commercial enterprises on the network. The senior security officer at this organization noted that, when rules such as this are aimed at users, it is especially important that they be stated in clearly understandable, relatively nontechnical language. The security officers at the computer vendor said that because the company's information security policies emphasized user behavior, they were included in the organization's employee code of conduct.

Practice 10: Distinguish Between Policies and Guidelines

"Detailed guidelines are an important supplement to the official policies because they educate users and serve as an awareness tool."
– Security manager at a prominent financial institution

A common technique for making organizational information security policies more useful was to divide them into two broad segments: concise high-level policies and more detailed information referred to as guidelines or standards. Policies generally outlined fundamental requirements that top management considered to be imperative, while guidelines provided more detailed rules for implementing the broader policies. Guidelines, while encouraged, were not considered to be mandatory for all business units.

Distinguishing between organizational policies and guidelines provided several benefits. It allowed senior management to emphasize the most important elements of information security policy, provided some flexibility to unit managers, made policies easier for employees to understand, and, in some cases, reduced the amount of formal review needed to finalize updated policies.

Guidelines Can Serve As An Educational Tool

Several security managers said that short policies that emphasized the most important aspects of the organizations security concerns were more likely to be read and understood than voluminous and detailed policies. However, they noted that more detailed guidelines often provided answers to employees' questions and served as a tool for educating subordinate security managers and others who wanted a more thorough understanding of good security practices.

For example, the utility company had distilled the fundamental components of its information protection policies into less than one page of text. This narrative (1) stated that *"Information is a corporate asset . . . . Information must be protected according to its sensitivity, criticality and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed,"* (2) outlined the responsibilities of information owners, custodians, and users, (3) defined the organization's three data classification categories, and (4) stated that each business unit should develop an information protection program to implement these policies. The policy

statement then referred the reader to a 73-page reference guide that provided definitions, recommended guidelines and procedures, explanatory discussions, and self-assessment questionnaires designed to assist business units in understanding the need for the policies and how they could be implemented.

Guidelines Provide for Flexibility

Although the latitude granted to business units varied, providing both policies and guidelines allowed business units to tailor the guidelines to their own individual unit's information protection needs. It also reinforced the business managers' sense of ownership of their information assets.

For example, the large financial services corporation had divided its information security rules into "policies" and "standards." Policies were mandatory, high-level requirements that, with rare exception, had to be followed. An example of a policy was that units were required to use commercially developed software rather than developing unique software in-house. An example of a standard at the same institution was a prescribed minimum password length. At this organization, deviations from policies had to be documented in a letter signed by both the executive of the business group requesting the deviation and the central information security group's manager. However, deviations from standards required only approval from the group's executive. Such deviations were required to be documented in a letter and, though not required, were usually approved by the central security group. All deviations had to be renewed annually.

Practice 11: Support Policies Through the Central Security Group

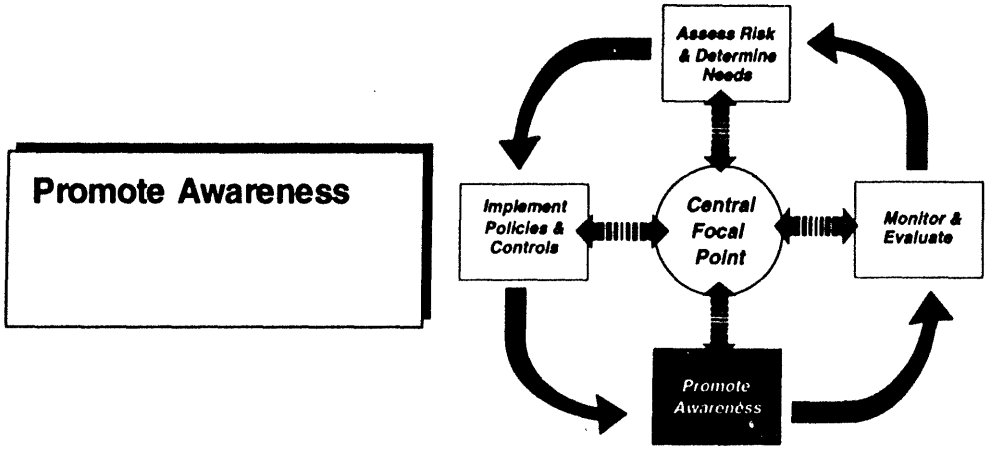
Generally, the central security management groups were responsible for developing written corporatewide policies in partnership with business managers, internal auditors, and attorneys. In addition, the central groups provided related explanations, guidance, and support to business units. Several security managers noted that business managers are much more likely to support centrally developed policies if they clearly address organizational needs and are practical to implement. For this reason, these organizations had developed mechanisms for involving other organizational components in policy documentation.

Most often this involvement was in the form of reviews of policy drafts. However, the university had established an information security policy committee that included top university officials, legal counsel, and representatives from student affairs, faculty affairs, and internal audit to assist in the development and review of policies.

The central security management groups played an important role in ensuring that policies were consistently implemented by serving as focal points for user questions. By serving as a readily available resource for organization employees, they helped clear up misunderstandings and provided guidance on topics that were not specifically addressed in written guidance.

Most organizations had also made their policies available through their computer networks so that users could readily access the most up-to-date version whenever they needed to refer to them. In addition, many organizations required users to sign a statement that they had read and understood the organization's information security policies. Generally, such statements were required from new users at the time access to information resources was first provided and from all users periodically, usually once a year. One security manager thought that requiring such signed statements served as a useful technique for impressing on the users the importance of understanding organizational policies. In addition, if the user was later involved in a security violation, the statement served as evidence that he or she had been informed of organizational policies. Additional techniques for communicating information security policies are discussed in the next section on promoting awareness.

Getting Started--Implementing Appropriate Policies and Related Controls	
Senior Program Officials	Review existing policies and assist in developing new policies to ensure that they address current business risks and related information protection needs.
CIOs	Assign responsibility to the central security group for coordinating the development of written policies that address current risks. Institute procedures for periodically updating policies.
Senior Security Officers	Document policies clearly so that they can be readily understood by managers and users. Review existing policies to identify the need to distinguish between official policies and guidelines.



"Users are much more likely to support and comply with policies if they clearly understand the purpose for the policies and their responsibilities in regard to the policies."

– Information security manager for a state agency

User awareness is essential to successfully implementing information security policies and ensuring that related controls are working properly. Computer users, and others with access to information resources, cannot be expected to comply with policies that they are not aware of or do not understand. Similarly, if they are not aware of the risks associated with their organization's information resources, they may not understand the need for and support compliance with policies designed to reduce risk. For this reason, the organizations considered promoting awareness as an essential element of the risk management cycle.

Practice 12: Continually Educate Users and Others on Risks and Related Policies

The central groups had implemented ongoing awareness strategies to educate all individuals who might affect the organization's information security. These individuals were primarily computer users, who might be employees; contractors; clients; or commercial partners, such as suppliers. One organization took an even broader view, targeting awareness efforts also at custodians and security guards, after a night security guard accidentally destroyed some important data while playing games on a computer after hours.

The groups focused their efforts on increasing everyone's understanding of the risks associated with the organization's information and the related policies and controls in place to mitigate those risks. Although these efforts were generally aimed at encouraging policy compliance, the senior security official at the retailing company emphasized the importance of improving users' understanding of risks. She said that her central security group had recognized that policies, no matter how detailed, could never address every scenario that might lead to a security incident. As a result, her overarching philosophy regarding awareness efforts was that users who thoroughly understood the risks were better equipped to use good judgment when faced with a potential security breach. For example, such employees were less likely to be tricked into disclosing sensitive information or passwords.

This last point highlights one of the most important reasons for sensitizing computer users and other employees to the importance of information security. Users disclosing sensitive information or passwords in response to seemingly innocent requests from strangers either over the phone or in person can provide intruders easy access to an organization's information and systems. Such techniques, often referred to as "social engineering," exploit users' tendencies to be cooperative and helpful, instead of guarded, careful, and suspicious, when information is requested. Without adequate awareness about the risks involved in disclosing sensitive information, users may volunteer information which can allow an intruder to circumvent otherwise well-designed access controls.

Practice 13: Use Attention-Getting and User-Friendly Techniques

To get their message across, the central security groups used a variety of training and promotional techniques to make organizational policies readily accessible, educate users on these policies, and keep security concerns in the forefront of users' minds. Techniques used included

- intranet websites that communicated and explained information security-related policies, standards, procedures, alerts, and special notes;
- awareness videos with enthusiastic endorsements from top management for the security program to supplement basic guidance, such as the importance of backing up files and protecting passwords;
- interactive presentations by security staff to various user groups to market the services provided by the central information security group and answer user questions; and
- security awareness day and products with security-related slogans.

The organizations avoided having once-a-year, one-size-fits-all security briefings like those seen at many federal agencies. The security managers said that it was important to relate security concerns to the specific risks faced by users in individual business groups and ensure that security was an everyday consideration.

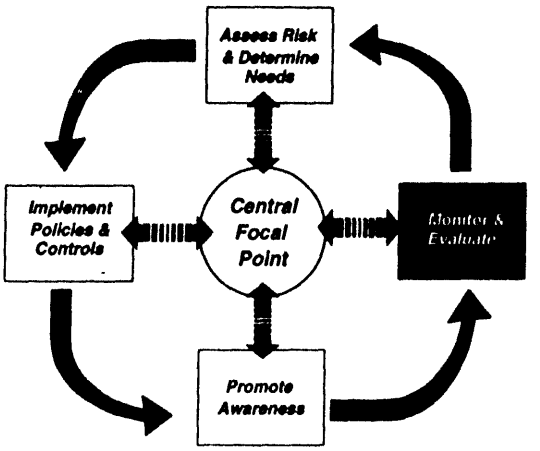
Case Example - Coordinating Policy Development and Awareness Activities

After experiencing a significant virus infection in 1989, a retailing company assigned one of its managers to step up efforts to promote employee awareness of information security risks and related organizational policies. Since then, this individual's responsibilities for information security policy development and awareness, which had previously been handled on a part-time basis, have evolved into a full-time "awareness manager position" in the organization's central security group. The company's response to a minor incident involving the unintentional release of company financial data illustrates the compatibility of these roles. To reduce the chances of a similar incident, the awareness manager concurrently (1) coordinated the development of a policy describing organizational data classification standards and (2) developed a brochure and guidelines to publicize the new standards and educate employees on their implementation. By coordinating policy development and awareness activities in this manner, she helps ensure that new risks and policies are communicated promptly and that employees are periodically reminded of existing policies through means such as monthly bulletins, an intranet web site, and presentations to new employees.

Getting Started--Promoting Awareness

Senior Program Officials	Demonstrate support by participating in efforts to promote information security awareness.
CIOs	Provide adequate funding and support to adequately promote awareness throughout the agency.
Senior Security Officers	Implement ongoing awareness strategies to educate all individuals who might affect the organization's information security.

Monitor and Evaluate Policy and Control Effectiveness



As with any type of business activity, information security should be monitored and periodically reassessed to ensure that policies continue to be appropriate and that controls are accomplishing their intended purpose. Over time, policies and procedures may become inadequate because of changes in threats, changes in operations, or deterioration in the degree of compliance. Periodic assessments or reports on activities can be a valuable means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security program.

The organizations we studied had recognized that monitoring control effectiveness and compliance with policies is a key step in the cycle of managing information security. Accordingly, they monitored numerous factors associated with their security programs, and they used the results to identify needed improvements. They used various techniques to do this, and several mentioned their efforts to identify, evaluate, and implement new, more effective tools as they become available. Such tools include software that can be used to automatically monitor control effectiveness and information systems activity. In addition, several of the security managers expressed interest in improving their ability to more precisely measure the costs and benefits of security-related activities so that their organizations could better determine which controls and activities were the most cost effective.

Practice 14: Monitor Factors that Affect Risk and Indicate Security Effectiveness

The organizations focused their monitoring efforts primarily on (1) determining if controls were in place and operating as intended to reduce risk and (2) evaluating the effectiveness of the security program in communicating policies, raising awareness levels, and reducing incidents. As discussed below, these efforts included testing controls, monitoring compliance with policies, analyzing security incidents, and accounting for procedural accomplishments and other indicators that efforts to promote awareness were effective.

Testing the Effectiveness of Controls

Directly testing control effectiveness was cited most often as an effective way to determine if the risk reduction techniques that had been agreed to were, in fact, operating effectively. In keeping with their role as advisors and facilitators, most of the security managers said that they relied significantly on auditors to test controls. In these cases, the central security management groups kept track of audit findings related to information security and the organization's progress in implementing corrective actions.

However, several of the central security groups also performed their own tests. For example, the central security group at the university periodically ran a computer program designed to detect network vulnerabilities at various individual academic departments and reported weaknesses to department heads. A subsequent review was performed a few months later to determine if weaknesses had been reduced. The central security manager told us that she considered the tests, which could be performed inexpensively by her staff, a cost-effective way to evaluate this important aspect of security and provide a service to the academic departments, which were ultimately responsible for the security of their departments' information and operations.

Several organizations periodically tested system and network access controls by allowing designated individuals to try to "break into" their systems using the latest hacking techniques. This type of testing is often referred to as penetration testing. The individuals performing the tests, which at various organizations were internal auditors, contractors, student interns, or central security staff, were encouraged to research and use hacking instructions and tools available on the Internet or from other sources in order to simulate attacks from real hackers. By allowing such tests, the organizations could readily identify previously unknown vulnerabilities and either eliminate them or make adjustments in computer and network use to lessen the risks.

One organization had performed annual tests of its disaster recovery plan to identify and correct plan weaknesses. A recent test was particularly effective because it involved a comprehensive simulation of a real disaster. The test involved staging a surprise "bomb scare" to get employees, who were unaware that the threat was a pretense, to evacuate the building. After the employees had evacuated, they were told that they were participating in a test, that they were to assume that a bomb had actually destroyed their workplace, and to proceed with emergency recovery plans. The test, which was organized by the agency's contingency planning group, proved extremely successful in identifying plan weaknesses and in dramatically sensitizing employees to the value of anticipating and being prepared for such events.

Monitoring Compliance With Policies and Guidelines

All of the organizations monitored compliance with organizational policies to some extent. Much of this monitoring was achieved through informal feedback to the central security group from system administrators and others in other organizational units. However, a few organizations had developed more structured mechanisms for such monitoring. For example, the utility company developed quarterly reports on compliance with organizational policies, such as the number of organizational units that had tailored their own information protection policies as required by corporate-level policy. Also, several organizations said that they had employed self-assessment tools, such as the Computer Security Institute's "Computer Security Compliance Test," to compare their organization's programs to preestablished criteria.

Accounting For and Analyzing Security Incidents

Keeping summary records of actual security incidents is one way that an organization can measure the frequency of various types of violations as well as the damage suffered from these incidents. Such records can provide valuable input for risk assessments and budgetary decisions.

Although all of the organizations kept at least informal records on incidents, those that had formalized the process found such information to be a valuable resource. For example, at the nonbank financial institution, the central security manager kept records on viruses detected and eradicated, including estimates of the cost of potential damage to computer files that was averted by the use of virus detection software. This information was then used to justify annual budget requests when additional virus detection software was needed. However, as discussed in the following case example, the university had

developed the most comprehensive procedures for accounting for and analyzing security incidents.

Case Example: Developing an Incident Database

A university's central security group had developed a database that served as a valuable management tool in monitoring problems, reassessing risks, and determining how to best use limited resources to address the most significant information security problems. The database accounted for the number of information security incidents that had been reported, the types of incidents, and actions taken to resolve each incident, including disciplinary actions. At the time of our visit, in February 1997, incidents were categorized into 13 types, which generally pertained to the negative effects of the violations. Examples included denial of service, unauthorized access, data compromise, system damage, copyright infringement, and unauthorized commercial activity.

By keeping such records, the central group could develop monthly reports that showed increases and decreases in incident frequency, trends, and the status of resolution efforts. This, in turn, provided the central security group a means of (1) identifying emerging problems, (2) assessing the effectiveness of current policies and awareness efforts, (3) determining the need for stepped up education or new controls to address problem areas, and (4) monitoring the status of investigative and disciplinary actions to help ensure that no individual violation was inadvertently forgotten and that violations were handled consistently.

The means of maintaining the database and the details that it contained had changed as the number of reported incidents at the university had grown–from 3 or 4 a month in 1993 to between 50 and 60 a month in early 1997–and as the database's value as a management tool became more apparent. Records originally maintained in a paper logbook had been transferred to a personal computer, and information on follow-up actions had recently been expanded.

The university's senior security officer noted that the database could be augmented to provide an even broader range of security management information. For example, while the university did not develop data on the actual cost of incidents, such as the cost of recovering from virus infections, the database could be used to compile such information, which would be useful in measuring the cost of security lapses and in determining how much to spend on controls to reduce such lapses.

Monitoring the Effectiveness of the Central Security Management Group

Several of the central security groups had developed measures of their own activities, outputs, and expertise as an indication of their effectiveness. Examples of these items included

- the number of calls from users, indicating knowledge of and respect for security specialists;
- the number of security-related briefings and training sessions presented;
- the number of risk assessments performed;
- the number of security managers and systems administrators who were Certified Information System Security Professionals; and
- the number of courses and conferences held or attended.

Emerging Interest in More Precisely Measuring Cost and Benefits

Several of the security managers expressed an interest in developing better measurement capabilities so that they could more precisely measure the ultimate benefits and drawbacks of security-related policies and controls–that is, the positive and negative affects of information security on business operations. However, they said that such measurements would be difficult because it is costly to do the research and recordkeeping necessary to develop information on (1) the full cost of controls–both the initial cost and operational inefficiencies associated with the controls–and (2) the full cost of incidents or problems resulting from inadequate controls. Further, as discussed previously regarding risk assessment, actual reductions in risk cannot be precisely quantified because sufficient data on risk factors are not available.

In an effort to more thoroughly explore this topic, we expanded our discussions beyond the eight organizations that were the primary subjects of our study by requesting the Computer Security Institute to informally poll its most active members on this subject. We also discussed assessment techniques with experts at NIST. Although we identified no organizations that had made significant progress in applying such measures, we found that more precisely measuring the positive and negative effects of security on business operations is an area of developing interest among many information security experts. For this reason, improved data and measurement techniques may be available in the future.

Practice 15: Use Results to Direct Future Efforts and Hold Managers Accountable

Although monitoring, in itself, may encourage compliance with information security policies, the full benefits of monitoring are not achieved unless results are used to improve the security program. Analyzing the results of monitoring efforts provides security specialists and business managers a means of (1) reassessing previously identified risks, (2) identifying new problem areas, (3) reassessing the appropriateness of existing controls and security-related activities, (4) identifying the need for new controls, and (5) redirecting subsequent monitoring efforts. For example, the central security group at the utility redirected its training programs in response to information security weaknesses reported by its internal auditors. Similarly, security specialists at the manufacturing company recently visited one of the company's overseas units to assist in resolving security weaknesses identified by internal auditors. The previously-cited example of using records on virus incidents to determine the need for virus-detection software also illustrates this point.

Results can also be used to hold managers accountable for their information security responsibilities. Several organizations had developed quarterly reporting mechanisms to summarize the status of security-related efforts. However, the financial services corporation provided the best example of how periodic reports of results can be used to hold managers accountable for understanding, as well as reducing, the information security risks to their business units. A description of this process is provided in the following case example.

Case Example: Measuring Control Effectiveness and Management Awareness

At a major financial services corporation, managers are expected to know what their security problems are and to have plans in place to resolve them. To help ensure that managers fulfill this responsibility, they are provided self-assessment tools that they can use to evaluate the information security aspects of their operations. When weaknesses are discovered, the business managers are expected to either improve compliance with existing policies or consult with the corporation's security experts regarding the feasibility of implementing new policies or control techniques.

Ratings based on audit findings serve as an independent measure of control effectiveness and management awareness. At the start of every audit, the auditors ask the pertinent business managers what weaknesses exist in their operations and what corrective actions they have deemed necessary and have planned. After audit work is complete, the auditors compare their findings with management's original assertions to see if management was generally aware of all of the weaknesses prior to the audit. The auditors then develop two ratings on a scale of 1 to 5: One rating to indicate the effectiveness of information security controls and a second rating to indicate the level of management awareness. If the auditors discover serious, but previously unrecognized weaknesses, the management awareness rating will be lowered. However, if the auditor finds no additional weaknesses, management will receive a good awareness rating, even if controls need to be strengthened.

These ratings are forwarded to the CEO and to the board of directors, where they can be used as performance measures. According to the bank's central security manager, the bank chairman's goal is for all business units to have favorable ratings (4 or 5) in both categories. Such a rating system provides not only a measure of performance and awareness, but it also places primary responsibility for information security with the managers whose operations depend on it. Further, it recognizes the importance of identifying weaknesses and the risk they present, even when they cannot be completely eliminated.

Practice 16: Be Alert to New Monitoring Tools and Techniques

The security specialists said that they were constantly looking for new tools to test the security of their computerized operations. Two security managers noted that their organizations had implemented new, more sophisticated, software tools for monitoring network vulnerabilities. However, several security managers said that the development of automated monitoring tools is lagging behind the introduction of new computer and network technologies and that this has impaired their efforts to detect incidents, especially unauthorized intrusions. Similarly, as discussed previously, managers are looking for practical techniques for more precisely measuring the value of security controls and obtaining better data on risk factors. In such an environment, it is essential that (1) security specialists keep abreast of developing techniques and tools and the latest information about system vulnerabilities and (2) senior executives ensure they have the resources to do this.

Several security managers told us that, in addition to reading current professional literature, their involvement with professional organizations was a valuable means of learning about the latest monitoring tools and research efforts. Examples of such organizations included the Computer Security Institute, Information Systems Security Association, the Forum of Incident Response and Security Teams, and less formal discussion groups of security professionals associated with individual industry segments. Several security managers said that by participating in our study, they hoped to gain insights on how to improve their information security programs.

Getting Started--Monitoring and Evaluating Policy and Control Effectiveness	
Senior Program Officials	Determine what aspects of information security are important to mission-related operations and identify key indicators to monitor the effectiveness of related controls.
CIOs	Include security-related performance measures when developing information technology performance measures.
Senior Security Officers	Establish a reporting system to account for the number and type of incidents and related costs.
	Establish a program for testing and evaluating key areas and indicators of security effectiveness.
	Develop a mechanism for reporting evaluation results to key business managers and others who can act to address problems.
	Become an active participant in professional associations and industry discussion groups in order to keep abreast of the latest monitoring tools and techniques.

Conclusion

"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress."

Vice President Albert Gore, Jr., in the Administration's July 1997 report, A Framework For Global Electronic Commerce

To achieve the benefits offered by the new era of computer interconnectivity, the federal government, like other organizational entities and individuals, must find ways to address the associated security implications. Individual security controls and monitoring tools will change as technology advances, and new risks are likely to emerge. For this reason, it is essential that organizations such as federal agencies establish management frameworks for dealing with these changes on an ongoing basis.

Developing an information security program that adheres to the basic principles outlined in this guide is the first and most basic step that an agency can take to build an effective security program. In this regard, agencies must continually (1) explore and assess information security risks to business operations, (2) determine what policies, standards, and controls are worth implementing to reduce these risks, (3) promote awareness and understanding among program managers, computer users, and systems development staff, and (4) assess compliance and control effectiveness. As with other types of internal controls, this is a cycle of activity, not an exercise with a defined beginning and end.

By instituting such a management framework, agencies can strengthen their current security posture, facilitate future system and process improvement efforts, and more confidently take advantage of technology advances.

Appendix I

GAO Guides on Information Technology Management

Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments (GAO/AIMD-98-89, March 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (Exposure Draft, GAO/AIMD-10.1.19, February 1998)

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)

Business Process Reengineering Assessment Guide (GAO/AIMD-10.1.15, April 1997, Version 3)

Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making (GAO/AIMD-10.1.13, February 1997, Version 1)

Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994)

Appendix II

NIST's Generally Accepted Principles and Practices for Securing Information Technology Systems

To provide a common understanding of what is needed and expected in information technology security programs, NIST developed and published Generally Accepted Principles and Practices for Securing Information Technology Systems (Special Pub 800-14) in September 1996.[6] Its eight principles are listed below.

1. Computer Security Supports the Mission of the Organization
2. Computer Security Is an Integral Element of Sound Management
3. Computer Security Should Be Cost-Effective
4. Systems Owners Have Security Responsibilities Outside Their Own Organizations
5. Computer Security Responsibilities and Accountability Should Be Made Explicit
6. Computer Security Requires a Comprehensive and Integrated Approach
7. Computer Security Should Be Periodically Reassessed
8. Computer Security Is Constrained by Societal Factors

[6]At the time of publication, this document, along with other publications pertaining to information security, was available on NIST's Computer Security Resource Clearinghouse internet page at http://csrc.nist.gov/publications.html. The listed documents are also available through either the Government Printing Office or the National Technical Information Service, for more information call (202) 783-3238 or (703) 487-4650, respectively.

Appendix III

Major Contributors to This Executive Guide

Accounting and Information Management Division Washington, D.C.	Jean Boltz, Assistant Director, (202) 512-5247 Michael W. Gilmore, Information Systems Analyst Ernest A. Döring, Senior Evaluator

GAO Reports and Testimonies on Information Security Issued Since September 1993

U.S. Government Financial Statements: Results of GAO's Fiscal Year 1997 Audit (GAO/T-AIMD-98-128, April 1, 1998)

Financial Audit: 1997 Consolidated Financial Statements of the United States Government (GAO/AIMD-98-127, March 31, 1998)

Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997)

Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997)

Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements (GAO/AIMD-97-89, August 29, 1997)

Social Security Administration: Internet Access to Personal Earnings and Benefits Information (GAO/T-AIMD/HEHS-97-123, May 6, 1997)

IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified (GAO/T-AIMD-97-82, April 15, 1997)

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/T-AIMD-97-76, April 10, 1997)

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997)

High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997)

Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996)

Financial Audit: Examination of IRS' Fiscal Year 1995 Financial Statements (GAO/AIMD-96-101, July 11, 1996)

Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996)

Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996)

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996)

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996)

Security Weaknesses at IRS' Cyberfile Data Center (GAO/AIMD-96-85R, May 9, 1996)

Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome To Achieve Success (GAO/T-AIMD-96-75, March 26, 1996)

Financial Management: Challenges Facing DOD in Meeting the Goals of the Chief Financial Officers Act (GAO/T-AIMD-96-1, November 14, 1995)

Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/ AIMD-95-141, August 4, 1995)

Federal Family Education Loan Information System: Weak Computer Controls Increase Risk of Unauthorized Access to Sensitive Data (GAO/AIMD-95-117, June 12, 1995)

Department of Energy: Procedures Lacking to Protect Computerized Data (GAO/AIMD-95-118, June 5, 1995)

Financial Management: Control Weaknesses Increase Risk of Improper Navy Civilian Payroll Payments (GAO/AIMD-95-73, May 8, 1995)

Information Superhighway: An Overview of Technology Challenges (GAO/AIMD-95-23, January 23, 1995)

Information Superhighway: Issues Affecting Development (GAO/RCED-94-285, September 30, 1994)

IRS Automation: Controlling Electronic Filing Fraud and Improper Access to Taxpayer Data (GAO/T-AIMD/GGD-94-183, July 19, 1994)

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1993 and 1992 (GAO/AIMD-94-131, June 30, 1994)

Financial Audit: Examination of Customs' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-119, June 15, 1994)

Financial Audit: Examination of IRS' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-120, June 15, 1994)

HUD Information Resources: Strategic Focus and Improved Management Controls Needed (GAO/AIMD-94-34, April 14, 1994)

Financial Audit: Federal Deposit Insurance Corporation's Internal Controls as of December 31, 1992 (GAO/AIMD-94-35, February 4, 1994)

Financial Management: Strong Leadership Needed to Improve Army's Financial Accountability (GAO/AIMD-94-12, December 22, 1993)

Communications Privacy: Federal Policy and Actions (GAO/OSI-94-2, November 4, 1993)

IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, September 22, 1993)

Document Security: Justice Can Improve Its Controls Over Classified and Sensitive Documents (GAO/GGD-93-134, September 7, 1993)