Diane Soran
October 14, 1983

GLICKMAN SUB-COMMITTEE

HST-Glickman-Sub-Committee-Hearing

Witness List

| | |
|---|---|
| OMB<br>(Office of management and Budget) | Joe Wright, Deputy Director |
| GAO<br>(Government Accounting Office) | Warren Reed, Director, Information Management & Technology |
| NBS<br>(National Bureau of Standards) | Dr. Lyons, Deputy Director |
| NSA<br>(National Security agency) | Melvin Klein, Director, DOD., Computer Security Center |
| FBI | Mr. Clarke, Deputy Assistant Director<br>Criminal Investigation Division |
| TREAS<br>(Dept. of Treasury) | Richard Shriver, Assistant Secretary<br>Electronic Systems and Information Technology |

Congressional Hearing 10/17/83

Diane Soran
October 14, 1983

GLICKMAN SUB-COMMITTEE

HST-Glickman-Sub-Committee-Hearing

Witness List

| | |
|---|---|
| OMB<br>(Office of management and Budget) | Joe Wright, Deputy Director |
| GAO<br>(Government Accounting Office) | Warren Reed, Director, Information Management & Technology |
| NBS<br>(National Bureau of Standards) | Dr. Lyons, Deputy Director |
| NSA<br>(National Security agency) | Melvin Klein, Director, DOD., Computer Security Center |
| FBI | Mr. Clarke, Deputy Assistant Director<br>Criminal Investigation Division |
| TREAS<br>(Dept. of Treasury) | Richard Shriver, Assistant Secretary<br>Electronic Systems and Information Technology |



Congressional Hearing 10/17/83

J. Dotty

Diane Soran
October 14, 1983

GLICKMAN SUB-COMMITTEE

HST-Glickman-Sub-Committee-Hearing

Witness List

| | |
|---|---|
| OMB<br>(Office of management and Budget) | Joe Wright, Deputy Director |
| GAO<br>(Government Accounting Office) | Warren Reed, Director, Information Management & Technology |
| NBS<br>(National Bureau of Standards) | Dr. Lyons, Deputy Director |
| NSA<br>(National Security agency) | Melvin Klein, Director, DOD., Computer Security Center |
| FBI | Mr. Clarke, Deputy Assistant Director<br>Criminal Investigation Division |
| TREAS<br>(Dept. of Treasury) | Richard Shriver, Assistant Secretary<br>Electronic Systems and Information Technology |



Congressional Hearing 10/17/83

L. Dottie

Diane Soran
October 14, 1983

GLICKMAN SUB-COMMITTEE

HST-Glickman-Sub-Committee-Hearing

Witness List

| | |
|---|---|
| OMB<br>(Office of management and Budget) | Joe Wright, Deputy Director |
| GAO<br>(Government Accounting Office) | Warren Reed, Director, Information Management & Technology |
| NBS<br>(National Bureau of Standards) | Dr. Lyons, Deputy Director |
| NSA<br>(National Security agency) | Melvin Klein, Director, DOD., Computer Security Center |
| FBI | Mr. Clarke, Deputy Assistant Director<br>Criminal Investigation Division |
| TREAS<br>(Dept. of Treasury) | Richard Shriver, Assistant Secretary<br>Electronic Systems and Information Technology |

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

FOR RELEASE ON DELIVERY
Expected at 9:30 a.m.
Monday, October 17, 1983

STATEMENT OF JOSEPH R. WRIGHT, JR.
DEPUTY DIRECTOR
BEFORE THE SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIALS
OF THE COMMITTEE ON SCIENCE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES
ON OMB'S EFFORTS TO IMPROVE FEDERAL COMPUTER SECURITY

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss OMB's role in computer security. Recently, national attention has been brought to this topic by the real-life actions of the Milwaukee computer hackers as well as fictional exploits of the youthful protagonists of television shows and movies like Wargames. It is important to note that hackers represent but a tiny part of the problem. I commend your committee for holding these hearings and focusing public scrutiny on the broader aspects of this issue.

I believe the real significance of the Wargames/hacker phenomenon is not that a group of amateurs could break into important data bases, seemly at will. Indeed, the ease with which the so-called 414 group obtained access appears to be due more to the failure of management controls, i.e., laxness of the system operators in changing factory passwords, than to exceptional skill on the part of the group.

The real significance of this phenomenon is the extent to which we as a society are accepting and using computers in all facets of our lives without full recognition of their vulnerability. Sophisticated technology that a few years ago was the sole province of the technocrat is increasingly being placed in the hands of any user. Soon a computer in the home could well be as widely accepted as a telephone. Very basic changes are taking place in the ways in which our society operates; the automation of information processes is at the heart of these changes.

Naturally, the Federal Government has participated in this revolution since we are the nation's largest user of automated information. Our investment in information technology is huge: we currently spend about 1.6% of our budget for ADP and telecommunications equipment and services which, in 1984, represents over 12 billion dollars. The General Services Administration (GSA) estimates that we currently operate over 18,000 medium and large scale computers at some 4,500 sites. By the end of the decade that equipment total will grow to nearly 25,000. Moreover, as we integrate end-user computing into the management of our federal programs through the use of microcomputers, the GSA estimates we could have between 250,000 and 500,000 micros in place by 1990.

The Department of Commerce's Federal Information Processing Standards program is an effort to confront the very serious problems of hardware and software compatability that this exponential growth will bring. Uniform standards will enable agencies to share and consolidate information when appropriate.

If computer hackers pose a danger, it is that their activities may undermine the confidence of the public in our ability to protect the data that are essential to the operation of agency programs. Individuals may fear that others will be able to examine their tax records; corporations may fear that competitors will be able to uncover important information about their operations or manufacturing processes. And, fears like these may directly affect the quality of information our citizens furnish, thereby eroding the integrity of our data bases and ultimately affecting the quality of our programs.

In the mid 1970's, congressional concern over a number of issues helped focus our attention and stimulated our efforts in this area. Hearings leading to the Privacy Act of 1974 pinpointed the potential for harm that automated data banks might represent to individuals. In other hearings, the Congress focused on the operational integrity of important automated systems such as the NORAD Air Defense System and the FAA Air Traffic Control System. In addition, a 1976 congressional staff study focused directly on federal computer security and system integrity issues. As a result, OMB has been concerned about computer security for several years.

During the 1970's, computer security was perceived to be the sole responsibility of the computer facility rather than an overall management concern. To involve top management actively in this area, OMB used the authority for ADP policy given us by the Brooks Act (P.L. 89-306) and issued Transmittal Memorandum No. 1 to OMB Circular No. A-71. This circular, issued

in July, 1978, established a basic federal computer security program. It requires that each agency head:

- Name a computer security officer for each computer installation;
- Establish personnel security policies which provide for screening of individuals involved in design or having access to sensitive computer processing systems or data;
- Establish a management control process to assure that appropriate levels of physical, technical and administrative safeguards are incorporated into data processing applications and facilities;
- Establish an agency program for periodic audits; and,
- Assign responsibility for the conduct of periodic risk analyses of each agency computer installation.

To broaden the base for oversight of this program OMB directed other central management agencies to provide assistance within their areas of expertise. Thus, Transmittal Memorandum No. 1 provided that the:

- Department of Commerce should develop and issue standards and guidelines for ensuring the security of automated information.
- GSA should:
  - -- issue regulations governing the physical security of computer rooms;
  - -- assure that agency procurement requests for computers or related services adequately incorporate computer security considerations;

-- assure that procurement specifications for computer hardware, software, facilities or services are consistent with Commerce, OMB and OPM standards; and,

- OPM should establish personnel security policies that provide for security consideration in the selection of personnel associated with design or operation of computer systems.

To ensure that each agency had an adequate computer security plan, OMB required agencies to submit their plans for implementing the memorandum for OMB review. In 1979, OMB assembled an interdisciplinary multi-agency team to review these plans and assess their strengths and weaknesses. All agencies were provided with critiques of their plans and were asked to revise them to overcome weaknesses revealed through the review process and to implement them.

These efforts represented the best available solutions for the time. But, we should remember that it was a time when most computer centers were discrete entities, telecommunications applications were limited, and agencies were not sharing much information. Our effort was aimed at putting some management controls in place quickly and we believe it resulted in the creation of a computer security program that was effective for its time.

OMB recognizes that times are changing dramatically. We have become substantially more dependent on automation for the operation of many federal programs. As federal programs grow larger, automation provides the most effective and efficient means of administering those programs. Manual systems in many

cases are simply incapable of providing an acceptable alternative, even in the limited role of a backup system. The Social Security Administration processes 36 million retirement checks each month. Can anyone imagine doing all that by hand? Similarly, the Department of Defense operates the Standard Automated Material Management System which centrally manages the Defense Logistics Agency's two million stock items. This inventory is valued at approximately three billion dollars and annual issues of stock exceed 20 million separate items. Only in an automated environment could the Department meet its material management responsibilities with the speed and certainty national security requires. Computers now play a significant role in efforts to identify and bring waste, fraud, and abuse in government programs under control. Over the past six months, for example, use of computer matches in Food Stamp program investigations has resulted in 164 indictments of individuals for underreporting of income, according to the USDA Inspector General. Perhaps the most significant trend in automating federal programs is end-user computing in which program managers are responsible for their own processing rather than relying on a central ADP facility. It promises great savings through increased productivity, but it may exacerbate security problems.

This rapid growth in our reliance on information technology brings the need for an effective federal computer security program into sharp focus. We think that the elements of such a program are already in existence. OMB and the other central management agencies have produced a substantial body of material

including directives, guidelines, and standards that deals with the problem of computer security. We are continuing to produce and update this material. If it were properly applied throughout the federal establishment, it would greatly enhance the security of our information systems.

In our view, the problem is that those tools often are not available to the managers who need them. There are two reasons for this: lack of information - the publicity/distribution process is inadequate; and lack of interest - managers often think about computer security only after the security of their systems has been breached.

In a recent study, which represents the most current data available on the extent of the computer security problem in the Federal Government, the President's Council on Integrity and Efficiency (PCIE) cited "lack of knowledge" on systems controls as a particular point of vulnerability. OMB is working to solve that "lack of knowledge" problem in ways I will describe shortly.

The lack of interest problem is harder to solve, but not impossible. In the national security and intelligence communities for example, computer/information security is an inseparable part of mission operations. A great deal of effort goes into ensuring security. All personnel are routinely and continually trained in security procedures. There are penalties for security violations ranging from administrative measures to criminal prosecution. The recent split up of the ARPANET system by the Department of Defense into two component parts, one containing operational information, the other scientific,

indicates the seriousness with which that Department pursues the goal of computer security.

In domestic agencies, however, the consequences of computer system vulnerability are not as apparent to managers. As a result they often do not view security as an integral part of the operation of their programs. Since it has no visible payoff -- the end result of good security is that nothing changes -- there is a tendency to give this area low priority. We need to reach such managers and ensure that they are giving security proper consideration.

To this end OMB has a number of ongoing activities. Some are designed to gather information so that the Federal Government can determine the extent of the problem. Others are designed to ensure that managers are putting the proper management controls in place. Among these activities are the following:

- Vulnerability assessment and internal control reviews under OMB Circular No. A-123, "Internal Controls," and the Federal Managers Financial Integrity Act. The circular requires agencies to develop directives and plans for internal control systems to ensure the safeguarding of agency resources and assure the reliability and accuracy of its information. The Act requires reporting of the results to the President and the Congress. We expect that many agencies in performing vulnerability assessments and internal control reviews will follow the suggestion in the PCIE computer security report and give particular emphasis to assessments of the internal controls in automated systems.

- The efforts of the Inspectors General through the PCIE to define the scope of the computer security problem. While their initial effort represented the most extensive examination of computer fraud and abuse in federal systems to date, it was somewhat limited by the fact that agencies had not regularly tracked cases of computer fraud and abuse. Even so, the twelve agencies responding reported 172 cases (69 fraud and 103 abuse). Estimated losses ranged from $0 to $177,383 in fraud cases and $0 to $5,214 in abuse cases. The PCIE report recommended a continuation of this effort and OMB concurs in that recommendation.
- The Information Resources Management Review (IRM) process. These reviews flow out of OMB's responsibilities under the Paperwork Reduction Act to examine specific agency IRM activities. A number of these reviews focused on automated systems and computer security issues. For example, a study by the Department of the Interior showed that the department-wide effort to comply with the established directives on computer security was well below an acceptable level. The study recommended that a full-time departmental ADP Security Officer be appointed to manage the ADP Security Program. The Department is currently in the process of implementing the recommendations of the study in order to bring every bureau and office up to full compliance with security requirements.

- The Privacy Act system of records review process under OMB Circular No. A-108. This circular was aimed at implementing the Privacy Act of 1974 (5 USC 552a) and provided that each agency head should: "establish reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access and otherwise to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." The circular also requires that agencies report to OMB how they intend to safeguard systems containing personal information prior to operating those systems. OMB staff typically review 120 such reports each year. To date these reviews suggest agencies are appropriately matching the degree of protection needed with the sensitivity of the data in the systems.
- The review of "matching program" reports and the issuance of Guidelines to Govern Computer Match Operations. With the advent of computer matching of data bases containing personal information to further the government's anti-fraud and abuse efforts, OMB issued a set of Matching Guidelines. These were designed to insure that matching activities were conducted in conformance with the requirements of the Privacy Act and that matching agencies maintained effective security for the processes and the

data developed. This guidance was updated in 1982. The Matching Guidelines require matching agencies to submit reports on their activities to OMB and the Congress. Computer security is a key part of these reports. In addition, the Veterans Administration Inspector General developed for the PCIE a model control system for conducting matching programs which provides substantial guidance on computer security.

- The Budget Review Process. Through this process, OMB has helped agencies improve the security of many of their mission systems. For example, the Social Security Administration is presently engaged in a $500 million upgrade of its ADP systems and computer security considerations were a significant consideration in approving the resources for that upgrade. Likewise, the Internal Revenue Service is engaged in a computer upgrade budgeted at $214 million in FY 1984. Here too, computer security was a key concern.

In addition to these ongoing efforts, OMB is preparing to take some new steps. For example:

- We are in the process of updating our circulars on Privacy and Computer Security (A-108 and A-71). On September 12, 1983 we invited public comment on a proposal to rescind our existing information policy circulars and create a new circular that will address, in a comprehensive fashion, the entire spectrum of information resources management,

including the safeguarding of automated information resources. We expect to have a first draft of this effort by the end of this year.

- We are working with Commerce's Institute for Computer Science and Technology (ICST) to help them better disseminate information about safeguards. ICST has tools that can help federal managers deal effectively with computer security problems. We are exploring methods for seeing that these tools are available to the managers. Among the possibilities are the development of training programs for top level managers and the operation of computer security conferences to highlight particular problems. Our aim is to bring the level of computer security awareness of the general federal manager to the same level as his military or intelligence counterpart.
- We are also exploring ways to tap private sector expertise in this area and to make that expertise available to the federal agencies. In areas such as electronic data funds transfers, we believe we have much to learn from the private sector.

In closing, let me reiterate that our interest in this subject is not a new one. It has been an area of concern to us for some time I can assure you, even when the publicity generated by the whizkids dies down, it is an area in which we will continue to be active.

This concludes my prepared remarks. I will be happy to answer any questions you may have.