

049-9



INFORMATION SECURITY CONSULTANTS

Phone: (508) 653-7101

5 Keane Terrace, Natick, MA 01760 FAX: (508) 650-0157

**Written Testimony Submitted to
the United States Sentencing Commission
In Support of the Proposed Amendment Regarding
Computer-Related Offenses**

**Sanford Sherizen, Ph.D.
President
Data Security Systems, Inc.
Natick, MA**

March 15, 1994

March 15, 1994

United States Sentencing Commission
One Columbus Circle, NE
Suite 2-500
South Lobby
Washington, DC 20002-8002
Attention: Public Information

Dear Commissioners of the United States Sentencing Commission,

I would like to go on record as encouraging the Commission to support the proposed amendment regarding computer-related offenses. It is imperative that the Commission act favorably on this amendment during this period when computer crime problems are becoming increasingly serious.

For purposes of identification, I write to you as an information security professional actively engaged in consulting, conducting seminars, and writing books and articles. I have written analyses for the Office of Technology Assessment (OTA) and testified before U.S. Senate as well as state legislative committees on computer crime and privacy issues. My information security consulting has been with businesses as well as Government agencies and I have lectured around the U.S. as well as internationally.

Based on the twelve years that I have involved with information security and the prior ten years in criminological research and university teaching, I find that computer crime has grown into a complex legal and social problem and current trends are quite worrisome. Computer crime can best be understood as the computerization of traditional crimes. While new crimes are possible with the use of computers (such as those criminal acts for which laws have not been defined or which are so unique that they are not possible without the technology), the majority of computer crimes are well known crime activities that existed prior to computerization. There is a need to differentiate between new information crimes that are possible only because of the existence of a new technology (computer viruses) from traditional crimes using new technology (desktop publishing fraud and forgery).

The computer criminal has changed from the "old days" of just a few years ago. In the majority of financial offenses which I have come across, computers are essential to the act or play a major role in the occurrence. Hackers who break into computer and phone systems and those who develop and spread viruses are still a problem today. Yet, there are now new and potentially more destructive computer criminals, including competitors who want product designs, angry employees seeking revenge for downsizing, inside traders searching for strategic plans, professional criminals

manipulating credit information and criminal histories, and journalists investigating scandals. More types of "new" computer criminals are expected.

Yet, despite these threats, information security in many organizations has failed to keep up with technological advances and information vulnerabilities. Few senior executives realize that they have to fulfill information security responsibilities in order to meet legal and fiduciary requirements. Relatively few organizations have achieved a level of information security sufficient to meet today's skilled computer criminal.

With these comments as background, I view the proposed amendment as an **interim but important response** to computer-related offenses. The next phase of the Commission's treatment of computer-related offenses should be to revisit this issue and, as suggested by the Working Group in cooperation with the Department of Justice's Computer Crime Unit, consider more specific action, such as a new computer guideline regarding these offenses. I would hope that the drafting of a new guideline will not be overly delayed since, as the Working Group correctly indicates, new cases (and, I would add, new harms) will almost certainly surface soon.

It is important for the Commission to develop a sentencing approach to computer-related crime which does not focus on harsh punishment, since that alone will not solve the computer crime problem. In research which I have recently completed on the effectiveness of deterrence, a review of the relevant empirical social science studies leads to the conclusion that deterrence is much more complex than theory (and common sense) suggest. Criminals may not act as rationally as the theories assume, there are complicated rules affecting how an individual perceives risky situations, and many individual as well as organizational factors intervene between the threat of legal sanctions and behavioral outcomes.

Even though there are state and Federal computer crime laws, there have only been a handful of criminal prosecutions to date. If the perception of the certainty and severity of punishment is a key variable in explaining deterrence, then the law has not been an effective force in controlling computer crime. Deterrence of computer crime should focus on tailoring penalties to computer crime severity, with special attention being paid to key information processes, industries, and types of violations.

Detering computer crime will require careful consideration of the seriousness of computerrelated crime for sentencing purposes. The Commission might weigh the larger number of harms beyond invasion of privacy and consequential recovery costs. Computerrelated crimes can add significant burdens to organizations and individuals who are victimized. These include direct financial losses as well as the less direct costs of additional information security personnel, security access control and identification products, system redundancies and other additional operating expenses due to security, and staff time spent cooperating with investigating law enforcement personnel.

There is also a need to review wire and mail fraud laws so that they will more directly apply to new technological development. These fraud laws, as well as other statutes, have often been used by prosecutors in place of weak or outdated state and federal computer crime laws. Prosecutors have expressed concern that computer crime legislation does not take into consideration their prosecutorial needs and, as a result, they are often forced to "shoehorn" computer-related crimes.

The Commission can assist with computer crime prevention by highlighting the importance of the issue and by providing direction for judges. In this symbolic as well as functional role, the nation can gain an increased protection. In a similar sense, the guidelines' model program provides senior executives with a clear view of their responsibility for crime control. Information protection must become a priority business and agency requirement. Senior executives must realize that they now have a major obligation to ensure that information is adequately protected. Deterring computer crime will require the Congress to pass improved legislation and for Government agencies and the private sector to develop and implement appropriate security measures.

I thank you for this opportunity to present these comments as written testimony and I stand ready to assist the Commission in this important effort.