U.S. Department of Justice

National Institute of Justice

121067

Office of the Director

Washington, D.C. 20531

OPENING REMARKS

BY

THE HONORABLE JAMES K. STEWART, DIRECTOR

NATIONAL INSTITUTE OF JUSTICE

BEFORE

THE NATIONAL INSTITUTE OF JUSTICE COMPUTER CRIME ADVISORS MEETING

9:00 A.M.

THURSDAY, SEPTEMBER 14, 1989

THE OMNI GEORGETOWN HOTEL

WASHINGTON, D.C.

121067

This gathering of expert advisors to NIJ on computer crime research is a significant event in the Institute's history. It marks the end of a preliminary investigation phase and, we hope, the emergence of a new program that will complement Attorney Dick General Thornburgh's white collar crime initiative and respond to a national need.

When I arrived as Director of the National Institute in 1982, our white collar crime unit had noticed and called to my attention an increase in the use of computers for crimes such as embezzlement and fraud. As a way of investigating this lead, we began to include several questions about computer crime in our periodic national assessments of criminal justice priorities. Over the next several years, what had been an interesting anomaly in 1982 grew into a distinct trend. In 1986 -- just to give you one example -- two-thirds of the police chiefs and sheriffs who responded gave the handling of computer crime a very high priority for further research and information sharing.

This information became the basis for the Institute's undertaking in 1988. Two new computer crime projects, whose results you have recently received, and the revision of a third, which is expected shortly.

- The first project looked at the few jurisdictions in the country which had <u>established</u> dedicated computer crime units in law enforcement or prosecutors' offices. This report, as you know, was entitled "Dedicated Computer Crime Units." Its author, Tom McEwen of the Institute for Law and Justice, is here today, and I am pleased to be able to acknowledge his fine work.

- The second project explored how jurisdictions which did not have computer crime units -- but were experiencing computer crime -- handled specific cases. This project discovered a whole range of options, including some that make sense even for smaller jurisdictions. The report, "Organizing for Computer Crime Investigation and Prosecution," was written by Cathy Conley of Abt Associates, who is also here today. Cathy, congratulations on your sterling efforts.
- The third project -- the updating of Donn Parker's highly-regarded Computer Crime Resource Manual -- will be available through the National Criminal Justice Reference Service in October. Donn wrote the original resource manual a decade ago and it has been widely used. We are pleased to have been able to support the Second Edition.

It is now time to take the next step. Our purpose in bringing you together is to help us at the National Institute think about and plan for the future investment of research resources that will provide the greatest return in this area. For not only are computer crime and other forms of white collar criminality an important program area for NIJ. They are also among the highest priorities of Attorney General Dick Thornburgh.

Today, our discussions will center on issues; tomorrow you will be asked to focus on suggesting topics and projects that fit into NIJ's mandate. The choices we make with our scarce dollars will determine how successful we are in the future.

In preparation for this planning conference, nine of you were asked to write papers on a wide range of issues dealing with computer crime -- providing us with an excellent starting point for our discussions. After perusing those papers, I have to tell you that I -- normally an enthusiastic and "can-do" sort of person -- am greatly sobered by the scope and complexity of the challenge that faces us.

Your agenda is a kind of blueprint of the major problems:

- technological: the speed, geographical reach, and secrecy of the transactions; the consequent difficulty of detection and apprehension;
- legal: especially around the rights of privacy;
- jurisdictional: a crazy-quilt of different laws, organizations, and communications providers;
- managerial: new standards for recruiting and training; added complexity to coordination.

Finally -- and to me most chilling of all -- I note the ethical ambivalence underlying computer crime. For if it is true that many computer crime perpetrators consider privileged information to be fair game, knowledge that ought somehow to be in the public domain and therefore a challenge to their undoubted ingenuity at breaking codes, then deterrence strategies have to be rethought from the ground up. Even the general public has not taken computer crime seriously; indeed, the transgressing hacker is often glorified as an embodiment of the American entrepreneurial spirit. He is seen as one person against the monolithic bureaucracy or institution rather than a thief stealing the future.

So as you begin your work on these daunting tasks, I am gratified that you are who you are -- the most experienced and knowledgeable group of law enforcement officials, prosecutors, private security managers, and researchers that we could gather. And I want especially to acknowledge the contributions of the steering committee, who helped us to find you and bring you to this place:

** Gail Thackeray, Assistant Attorney General from Arizona;

** Sergeant Jim Black, Los Angeles Police Department;

** Steve Purdy, U.S. Secret Service; and

** Dan Piskur, of Compuserve.

The challenges facing us in the field of computer crime are tremendous. Clearly, knowledge of computers and their innovative uses in committing crime is essential for successful investigation and prosecution in the years to come.