TESTIMONY OF

DEPUTY ASSISTANT DIRECTOR

FLOYD I. CLARKE

CRIMINAL INVESTIGATIVE DIVISION

FEDERAL BUREAU OF INVESTIGATION

WASHINGTON, D. C.

BEFORE THE

HOUSE SUBCOMMITTEE

ON

TRANSPORTATION, AVIATION, AND

MATERIALS

OCTOBER 17, 1983

THANK YOU MR. CHAIRMAN FOR PROVIDING ME AN OPPORTUNITY TO PRESENT THE FBI'S VIEWS ON THE SUBJECT OF TELECOMMUNICATIONS, SECURITY AND PRIVACY, AND TO RESPOND TO YOUR SPECIFIC AREAS OF CONCERN.

PRIOR TO RESPONDING TO YOUR SPECIFIC QUESTIONS, I WOULD LIKE TO POINT OUT THREE THINGS THAT WE IN THE FBI BELIEVE ARE KEY TO UNDERSTANDING THE FBI'S PERSPECTIVE ON COMPUTER RELATED CRIMES.

THE FIRST OF THESE ISSUES IS THAT A COMPUTER IS AN INSTRUMENTALITY OF SOME OTHER FORM OF TRADITIONAL CRIME, FOR INSTANCE THEFT OR LARCENY. IT IS MUCH LIKE A GUN, A KNIFE, OR A FORGER'S PEN.

THE SECOND ISSUE IS OF A MORE ACADEMIC NATURE, BUT NEVERTHELESS IMPORTANT IN THAT THERE DOES NOT EXIST, AT THIS TIME, ONE GENERALLY RECOGNIZED AND ACCEPTED DEFINITION AS TO WHAT COMPUTER RELATED CRIME IS. THEREFORE, WE DO NOT HAVE AN OBJECTIVE STANDARD TO MEASURE THE TRENDS OF COMPUTER RELATED CRIME.

LASTLY, IN VIEW OF THE FBI'S CURRENT STRUCTURE OF MANAGEMENT BY PROGRAM, RATHER THAN BY CASE, THERE IS NO METHOD IN PLACE NOW TO OBSERVE THE STATISTICAL DIMENSIONS OF COMPUTER RELATED CRIME.

WITH THAT IN MIND, I WOULD LIKE TO DISCUSS THE NATURE, EXTENT, AND DIMENSIONS OF CRIMES INVOLVING COMPUTERS AND COMMUNICATIONS FROM THE FBI'S PERSPECTIVE.

AS YOU ARE AWARE, THERE IS NO ONE AGENCY AT THIS TIME THAT HAS JURISDICTION FOR COMPUTER RELATED CRIMES AND VERY PROBABLY THERE CANNOT BE BECAUSE OF THE WIDE APPLICATION OF COMPUTERS. THE FBI'S JURISDICTION IN COMPUTER RELATED CRIMES IS DERIVED FROM

JURISDICTION PREVIOUSLY ASSIGNED TO THE FBI BY CONGRESS OR THE ATTORNEY GENERAL OF THE UNITED STATES IN MORE TRADITIONAL AREAS. GENERALLY SPEAKING, THE STATUTES MOST FREQUENTLY USED BY THE DEPARTMENT OF JUSTICE AND THE FBI TO PROSECUTE AND INVESTIGATE COMPUTER RELATED CRIMES ARE FRAUD BY WIRE, INTERSTATE TRANSPORTATION OF STOLEN PROPERTY, BANK FRAUD AND EMBEZZLEMENT, DESTRUCTION OF GOVERNMENT PROPERTY, AND THEFT OF GOVERNMENT PROPERTY. HOWEVER, COMPUTER RELATED CRIMES TRANSCEND ALL THE CRIME CATEGORIES AND JURISDICTIONS, LOCAL, STATE AND FEDERAL, AGAIN MAKING IT DIFFICULT TO MEASURE TRENDS IN THIS TYPE OF CRIME.

ANOTHER PROBLEM THAT HAS BEEN ENCOUNTERED IS A RELUCTANCY ON THE PART OF SOME BUSINESSES, ESPECIALLY THOSE IN THE FINANCIAL COMMUNITY, TO REPORT LOSSES ATTRIBUTABLE TO COMPUTER RELATED CRIMES IN AN ATTEMPT TO AVOID DEVELOPING AN IMAGE OF FISCAL INSECURITY. THEREFORE, IN THE ABSENCE OF A GENERALLY ACCEPTED DEFINITION OF COMPUTER RELATED CRIME, COUPLED WITH THE LACK OF A CENTRAL REPOSITORY FOR THE STATISTICS ON COMPUTER RELATED CRIMES, IT WOULD APPEAR THAT THE ANSWER TO YOUR QUESTION REGARDING THE EXTENT OF COMPUTER RELATED CRIME IS THAT NO ONE KNOWS FOR SURE.

SINCE THE EARLY 1970'S, THE FBI HAS BEEN INVOLVED IN COMPUTER RELATED CRIME INVESTIGATIONS, AND SINCE THAT TIME WE HAVE NOTED NO DRAMATIC INCREASE IN THE NUMBER OF THESE FBI INVESTIGATIONS. LOGIC WOULD INDICATE THAT WITH THE EVER INCREASING NUMBER OF COMPUTERS IN USE TODAY, THERE OUGHT TO BE A CORRESPONDING INCREASE IN COMPUTER RELATED CRIMES; HOWEVER, WE HAVE NO CREDIBLE DOCUMENTATION TO SUPPORT THIS SORT OF CONCLUSION.

AS TO THE DIMENSION OF COMPUTER RELATED CRIMES, THERE IS A LARGE POTENTIAL FOR EXTREMELY LARGE LOSSES. MOST FINANCIAL INSTITUTIONS,

OUR GOVERNMENT AND GOVERNMENTS OF OTHER COUNTRIES, UTILIZE COMPUTERS TO FACILITATE THEIR OPERATIONS. THIS CREATES A POTENTIAL FOR ABUSE BY PERSONS WHO HAVE THE NECESSARY KNOWLEDGE, TIME AND ACCESS TO THE CORRECT HARDWARE OR SOFTWARE. IN A VERY SHORT PERIOD OF TIME, PROGRAMS, HIGH TECHNOLOGY INFORMATION, PROPRIETARY INFORMATION OR CLASSIFIED INFORMATION CAN BE TAKEN FROM A COMPUTER WITHOUT LEAVING MUCH EVIDENCE OF THE CRIME. THIS IS TO SAY NOTHING OF THE THEFT OF LARGE AMOUNTS OF MONEY TRANSFERRED BY WIRE BETWEEN FINANCIAL INSTITUTIONS.

IN RESPONSE TO YOUR REQUEST FOR ILLUSTRATIONS OF COMPUTER RELATED CRIME THAT THE FBI HAS BEEN INVOLVED IN, I WOULD LIKE TO BRING TO YOUR ATTENTION SOME SPECIFIC INSTANCES OF THESE TYPE CRIMES.

IN 1979, THE NEW YORK DIVISION OF THE FBI IDENTIFIED A COMPUTER INFORMATION SERVICE COMPANY (WHICH IS A COMPANY THAT ENTERS, EDITS, STORES, AND RETRIEVES INFORMATION IN A TEXT FORMAT) THAT WAS, WITHOUT AUTHORIZATION, ACCESSING AND MODIFYING RECORDS OF A SIMILAR COMPUTER INFORMATION SERVICE IN THE STATE OF CALIFORNIA. THE SECOND COMPUTER SERVICE WAS THE PRIMARY COMPETITOR TO THE FIRST AND THE ACTIONS OF THE FIRST COMPUTER SERVICE CAUSED AN ESTIMATED LOSS OF $7.5 MILLION.

IN 1980, THE NEW YORK DIVISION AGAIN IDENTIFIED A GROUP OF CHILDREN OF MIDDLE SCHOOL AGE WHO ACCESSED WITHOUT AUTHORIZATION, OVER 20 COMPUTERS FROM THE COMPUTER LOCATED AT THEIR SCHOOL. THE UNAUTHORIZED ACCESSES BY THIS GROUP IN BOTH THE UNITED STATES AND CANADA NOT ONLY CAUSED THE LOSS OF COMPUTER TIME AND DISRUPTED COMPUTER SERVICES, BUT CAUSED THE DESTRUCTION OF INVENTORY AND BILLING FIGURES OF A CANADIAN FIRM, WHICH NECESSITATED SUBSTANTIAL EFFORTS BY THAT FIRM TO DUPLICATE.

IN LATE 1982, OUR WASHINGTON FIELD OFFICE IDENTIFIED A FORMER EMPLOYEE OF THE FEDERAL RESERVE BANK WHO WAS THEN EMPLOYED PRIVATELY AS A FINANCIAL ANALYST, WHO ATTEMPTED TO CONTINUE TO ACCESS INFORMATION IN THE FEDERAL RESERVE BANK'S MONEY ONE FILE WITHOUT AUTHORIZATION. ANY INFORMATION HE MIGHT HAVE OBTAINED FROM THIS FILE WOULD HAVE BEEN USEFUL IN THE ANALYSIS OF HIS CLIENT'S HOLDINGS.

EARLY IN 1983, OUR OFFICE IN ALEXANDRIA, VIRGINIA, IDENTIFIED AN INDIVIDUAL WHO WITHOUT AUTHORIZATION ACCESSED COMPUTERIZED CONSUMER CREDIT INFORMATION TO OBTAIN CREDIT ACCOUNT INFORMATION ON OVER 80 PEOPLE. THEREAFTER HE USED THIS INFORMATION TO CHARGE GOODS INCLUDING ADDITIONAL COMPUTER EQUIPMENT TO THE MAJOR CREDIT CARDS OF THE PEOPLE WHOSE CREDIT INFORMATION HE HAD ACCESSED.

THESE EXAMPLES ARE CERTAINLY NOT ALL INCLUSIVE OF OUR EFFORTS IN COMPUTER RELATED CRIMES, BUT THEY GIVE A BROAD VIEW OF THE TYPES OF COMPUTER RELATED CRIMES THAT ARE PRESENTED TO THE FBI FOR INVESTIGATION. WE HAVE SO FAR BEEN ABLE TO IDENTIFY AND LOCATE THE PERSON(S) COMMITTING EACH OF THE BEFOREMENTIONED CRIMES. WE HOPE TO CONTINUE TO DUE SO.

WE IN THE FBI HAVE NOT HAD, TO DATE, ANY SIGNIFICANT PROBLEMS IN PROSECUTION OF COMPUTER RELATED CRIME UNDER ALREADY EXISTING STATUTES OVER WHICH WE HAVE JURISDICTION, SUCH AS THE FRAUD BY WIRE STATUTE.

OUR EXPERIENCE INDICATES THAT CERTAIN LEGAL ISSUES INVOLVING COMPUTER RELATED CRIME COULD BE CLARIFIED, PARTICULARLY THE DEFINITION OF PROPERTY IN THE SENSE OF A COMPUTER PROGRAM HAVING ITS OWN CLEARLY DEFINED INHERENT VALUE AND THE ISSUE OF TRESPASS. ALSO,

THE MOST FREQUENTLY HEARD DEFENSE FOR SIMPLE UNAUTHORIZED ACCESS INTO SOMEONE ELSE'S COMPUTER IS THAT THE INDIVIDUAL MAKING THE ACCESS HAS NO CRIMINAL INTENT, MEANT NO HARM, THERE WAS NO SECURITY SYSTEM AND THEREFORE THERE IS NO TRESPASS. HOWEVER, IT IS FAIRLY COMMONLY HELD THAT IF AN INDIVIDUAL WITHOUT AUTHORIZATION ENTERS THE UNLOCKED HOUSE OF ANOTHER AND RUMMAGES THROUGH THAT PERSON'S CLOSETS WITH NO INTENT TO STEAL OR TO DO HARM THAT PERSON COULD STILL BE GUILTY OF TRESPASSING. IT IS IMPORTANT THAT A LEGAL CLARIFICATION BE MADE IN THIS REGARD.

IN REGARD TO PREVENTIVE MEASURES NECESSARY TO DEAL WITH COMPUTER RELATED CRIME IT APPEARS FROM OUR EXPERIENCE THAT THIS IS MORE OF A HUMAN PROBLEM THAN A TECHNOLOGICAL ONE. IN MOST INSTANCES WHERE WE HAVE BEEN INVOLVED IN AN INVESTIGATION OF COMPUTER RELATED CRIME THE CRIME WAS PERPETRATED BY SOMEONE WHO HAD ACCESS TO THE COMPUTER AND AUTHORIZATION TO USE IT. THE CRIME WAS FACILITATED BY THE ACCESS AND IN MOST CASES THE AUTHORIZATION WAS EXCEEDED OR MISUSED.

FINALLY, YOUR STAFF REQUESTED THAT I ADDRESS THE NEED OF LAW ENFORCEMENT AGENCIES FOR COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY IN THEIR OWN OPERATIONS. IT IS A WELL DOCUMENTED FACT THAT GOVERNMENT LAW ENFORCEMENT AGENCY RADIO COMMUNICATIONS ARE MONITORED BY NON-LAW ENFORCEMENT ELEMENTS, RANGING FROM THE HOBBYIST, WHO GAINS A VICARIOUS THRILL FROM BEING "IN" ON LAW ENFORCEMENT OPERATIONS, TO THE ENTREPRENEUR, WHO LISTENS FOR PROFIT; THE NEWS MEDIA OR THE PERSON WHO MARKETS LISTS OF GOVERNMENT FREQUENCIES EXHIBITING INTERESTING ACTIVITY, TO THE CRIMINAL WHO LISTENS TO EVADE LAW ENFORCEMENT OPERATIONS AS WELL AS THE FOREIGN INTELLIGENCE OPERATIVE. THESE ELEMENTS MONITOR OUR RADIO CIRCUITS TO GAIN INFORMATION ON OUR OPERATIONS, THROUGH INTERCEPT AND ANALYSIS OF OUR RADIO TRAFFIC;

TO DISRUPT OPERATIONS BY LEARNING OF OUR MOVEMENTS IN ADVANCE AND EVADING OR COUNTERING THEM; TO IDENTIFY AND ASSOCIATE AGENTS WITH ONGOING OPERATIONS. IN SHORT, WE PAY A SEVERE PENALTY DUE TO THE VULNERABILITY OF OUR CLEAR TEXT VOICE RADIO SYSTEM USED TO CONTROL OUR OPERATIONS. WE PAY THIS PENALTY IN TERMS OF PERSONNEL OVERHEAD. UP TO 20% OF A SURVEILLANT'S TIME MAY BE SPENT TO ACCOMODATE THE VERBAL CODES, ADDITIONAL SURVEILLANCE VEHICLES, AND OTHER BURDENS IMPOSED TO PROTECT OPERATIONS. THERE ARE COMPROMISED CASES, WHEREIN HUNDREDS OF HOURS OF EFFORT MAY BE WASTED BECAUSE THE SUBJECT LEARNED OF OUR OPERATIONS BY MONITORING OUR CIRCUITS AND SUCCESSFULLY EVADED APPREHENSION OR, FOREWARNED, WAS ABLE TO DESTROY VITAL EVIDENCE, THUS JEOPARDIZING PROSECUTION. THERE IS A HAZARD TO AGENTS, AGENT IDENTITY, LOCATION OR COVER, AND IF COMPROMIZED, IT COULD PLACE HIM IN A HIGHLY DANGEROUS POSITION. SUBJECTS HAVE USED INTERCEPTED RADIO TRANSMISSIONS TO IDENTIFY AND ENDANGER THE LIFE OF OPERATIVES.

TO COUNTER THE THREAT, VOICE PROTECTION MEASURES MUST BE APPLIED TO OUR RADIO SYSTEM. IN OUR COUNTERINTELLIGENCE OPERATIONS, NATIONAL DEFENSE IS AT STAKE AND FULL SPEECH "SECURITY" IS REQUIRED. IN CONDUCTING OUR LAW ENFORCEMENT OPERATION; HOWEVER, A SIGNIFICANT DEFICIENCY EXISTS IN COUNTERING THE KNOWN THREAT. IN THIS AREA, SPEECH SECURITY IS NOT ALWAYS WARRANTED, BUT THERE IS A DISTINCT AND PRESSING NEED FOR VOICE "PRIVACY" ON OUR RADIO SYSTEM NATIONWIDE.

CONGRESS RECOGNIZED THIS CRITICAL NEED AND HAS APPROPRIATED $64,600,000 IN THE FBI'S 1984 BUDGET FOR A VOICE PRIVACY RADIO SYSTEM. THIS MONEY, COMBINED WITH THE FUNDS APPROPRIATED IN 1982 AND 1983 WILL MAKE OUR VOICE PRIVACY SYSTEM 70% COMPLETE.

THIS CONCLUDES MY PREPARED REMARKS MR. CHAIRMAN. I WILL BE HAPPY TO ADDRESS ANY QUESTIONS YOU MAY HAVE.