Process Evaluation of the Computer Fraud and Abuse Act of 1986.

Anele Nwokoma
Computer Information Systems Department
P. O. Box 863
Grambling State University
Grambling, LA 71245

ABSTRACT

This study is an evaluation of the Computer Fraud and Abuse Act of 1986. The study reviews existing computer crime policy implementation, found the implementation slightly inappropriate, and recommends new process and a model that can be used to enhance implementation of the act and punish perpetrators. The study represents the result of a scholarly endeavor to link information systems and government policy. The report is organized into six primary divisions: problem identification, review of related literature, methodology, findings, conclusion and recommendation, and summary.

Acknowledgements: Throughout this study I depended on the expertise of Dr. John C. Morris of Mississippi State University, and on the cooperation of Honorable Janet Reno, Charles Mathews, Donald Stern, John Scalia, all from the United States Department of Justice, and Patrice Rapaplus of Computer Security Institute. I am extremely grateful to all of you. Special thanks to Dr. Morris who offered direction and constructive criticism.

Keywords: Information Systems, Computer Crime, Process Evaluation, and Government Policy.

PROBLEM IDENTIFICATION

According to the Justice Department, the Computer Fraud and Abuse Act of 1986 was enacted to provide a clear statement of proscribed activity concerning computers to the law enforcement community, those who own and operate computers and those tempted to commit crimes by unauthorized access to computers. Rather than having to "boot strap" enforcement efforts against computer crime by relying on statutory restrictions designed for other offenses, the Computer Fraud and Abuse Act, 18 U.S.C. 1030, sets forth computer crime statute. The act prohibits and provides criminal penalties for unauthorized use of computers to obtain classified or private financial information, to trespass in Federal Government computers, to commit frauds, or transmit harmful computer viruses.

In both public and private sectors the number of employees who rely on computer processed information to do their tasks are increasing. Naisbitt [19] predicted that many organizations would be in business to create, process, and transmit information. The advances in information technology lead to the increase in computer crime. One of the reasons for the growth of computers and telecommunication systems' technology is to promote the quality of human life. In essence, these systems facilitate human transactional processes in both public and private sectors and our lives. The daily applications of these systems in business and our lives as well have generated multiple problems. One problem is the use of computers to commit crimes. Another common problem is the lack of privacy on data stored on a computer. There has been congressional concern about issues which affect computerization. Particular issues such as computer crime, computer privacy, and computer threat to national security are related to the spread of computerization. Computer crime policy and its administration have become an afterthought in the development and implementation of computer-based systems. This is a serious national problem and there is great potential for future increase in opportunities for such crime unless Congress responds appropriately. How should governmental response to computer crime be improved? Why do there appear to be relatively few prosecutions? What are the limitations of legislative response to computer crime policy? This report will attempt to provide answers to the above questions.

REVIEW OF RELATED LITERATURE

The following review of literature will examine two major topics and two subtopics associated with this report. The major topics include the impacts of computer crime and computer crime legislation. The subtopics are the history of federal computer crime legislative efforts and federal legislation applicable to computer crime.

Computer crime is defined as any crime which is committed by:

- the introduction of fraudulent records or data into a computer system
- unauthorized use of computer-related facilities
- the alteration or destruction of information or files
- the stealing whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable [22].

Impacts of Computer Crime

Computer crime is increasing because of the proliferation of computers in today's society. "As computer crime proliferates, states and county prosecutors face increasing demand for prosecution strategies and technical expertise in this expanding area. In some cases local prosecutors will need to work cooperatively with federal prosecutors, addressing cases with both intrastate and interstate aspects. In other instances computer crimes will have a purely local impact and be prosecuted under state law. Existing federal legislation defines several computer crimes, but does not clearly specify what agencies or personnel shall have investigation responsibility" [15]. This means that prosecuting agencies may not have adequate policies to address computer offenders. Thus, the agencies may be unresponsive and incompetent because of their lack of knowledge about computer crime.

Inevitably, as computers become widespread in society, all law enforcement agencies will need to have or be able to obtain access to investigators who are familiar with computer crime [17]. Presently most law enforcement agencies do not have this capability. Remedying this situation would require the federal government to mandate programs which would enable colleges to train computer crime experts and prosecuting agencies to hire these individuals who have expertise in the collection of computer crime evidence and introduce it successfully for prosecution.

Computer crimes have surprisingly wide impact and variety, from sophisticated institutional transactions to the victimization of individuals [9]. Government is one of the victims of computer crime because it has undergone rapid computerization without adequate safeguards against crime. Since government services are highly dependent upon computers and telecommunication systems, it should have adequate policy to punish computer crime offenders.

Computer Crime Legislation

Before we indict the businessman or the employee as a conspirator abetting the computer criminal, it is only fair to point out that computer crime is extremely difficult to prove [6]. This statement raises the question, is it the crime before the law or the law before the crime? In this report's opinion, it is neither but the skills required to prosecute the computer criminal and the prosecuting process.

Laws are created to deter unethical behavior. In unclear areas, where parts of the public may not be sure which acts are right and which are wrong, people look to laws as moral beacons [3]. Some computer crimes could be dealt with using applicable federal and state laws, yet there are computer crimes that do not have appropriate laws for prosecution. Thus, the "society is seeing an increasing number of computer-related types of unethical behavior which have not been met with proper laws. For example, a student at the University of Wisconsin made unauthorized use of the university's computer to commit crime for over six months, yet the local district attorney could find no law with which to prosecute the student" [4]. Consequent to the increase of computer crimes, federal and state legislators enacted a series of laws and modified existing statutes to cover computer offenses. However, the present laws are not enough. New legislation is needed to supplement the present arsenal [2]. Therefore, it can be inferred that computer crime legislation is a topic of public interest as well as national importance. It is likely that computer crime may have outpaced its legal responses from the government. The legislative efforts made to date both at the state and federal levels to stop computer crimes are not encouraging.

A Brief History of Federal Computer Crime Legislative Efforts:

Since the 95th Congress, the Congress of the United States has considered various measures to protect both the public and private sectors business from computer crime [1]. "Senator Abraham Ribicoff sponsored the first computer crime bill in 1977, entitled Federal Computer Systems Protection Act of 1977, S. 1776. There was no action on the bill for two years. Senator Charles Percy introduced another bill in 1979, titled the Federal Computer Systems Protection Act of 1979, S. 240. Hearings on this bill were held, yet no further action was taken. In 1980, House of Rep. menbers Rose and Nelson introduced H.R. 3790 which was similar to the earlier computer crime bills. No action was received on this bill either" [22].

Representative Dan Glickman, the former chairman of the House Subcommittee on Transportation, Aviation,

and Materials, held hearings on computer crime. He also wrote a report which concluded that "Congress should charter a national commission to examine computer crime issues. Whitehouse should develop uniform standards for identifying and reporting computer crimes" [23]. These represent a merging of earlier legislative concerns on computer crime.

Federal Legislation Applicable to Computer Crime

If computer crime is not a uniquely new crime, then existing law may be applicable [22]. Computer crime is a unique type of crime which existing federal law may not be applicable for prosecutorial purpose. According to McFarlane [18], a federal prosecutor would be able to charge and seek conviction for a federal computer crime under one of the nearly forty potentially applicable federal statutes. Well as of now, federal prosecutors are not able to apply the existing statutes to prosecute computer crime perpetrators.

Nycum [20] divide federal statutes applicable to computer crime into seven broad categories: Theft and related crimes, Abuse of federal channels of communication, National security offenses, Trespass and burglary, Deceptive practices, Malicious mischief and related offenses, and Miscellaneous other statutes. None of these statutes can properly be used to punish computer criminals. Therefore, using the above statutes for computer crime prosecution would involve a substantial procedure and difficulties as well. Similar important federal laws for prosecuting computer criminal are the Electronic Communications Privacy Act of 1986, the Credit Card Fraud Act of 1984, the Federal Copyright Act of 1976, and the Wire Fraud Act of 1976 [22]. These federal laws do not have adequate provision to punish computer criminals. There are state statutes similar to the above; however, this report does not consider them. It is evident that there are some fundamental computer crime policy issues appropriate for congressional consideration.

METHODOLOGY

The principal data collection strategy was document analysis received from the Office of the Attorney General, FBI, Bureau of Justice Statistics, United States District Attorney's Offices, and Computer Security Institute. This information was supplemented with literature review and telephone discussion. The United States Congress and the Department of Justice, the Computer Security Institute (CSI), and criminals sentenced under the Computer Fraud and Abuse Act of 1986 were identified as the major stakeholders of this report. An initial telephone enquiry was made to the Justice Department and Computer Security Institute. The positive response of this enquiry lead to additional telephone discussions and obtaining the documents which form the basis for the evaluation.

The FBI and the Office of the Attorney General each required me to complete a data form, which must include a University's valid e-mail account before releasing any information and documents. The data forms were completed and sent through their respective home pages. The Computer Security Institute required my e-mail account and office telephone number and that of my supervisor. The initial contact with the Bureau of Justice Statistics lead to the subsequent contacts of the other agencies within the Department of Justice and CSI. Presentation of the methodology involves document analysis, telephone discussion, and statistical technique.

Document Analysis

The report studied the documents provided by the above organizations. The defendants sentenced under the federal guideline whose criminal conduct involved computer fraud and abuse were also studied. The department of Justice confirmed the contention in literature review that certain cases involving computer fraud and abuse were prosecuted under traditional criminal statutes rather than under the computer fraud and abuse statute, 18 U.S.C. 1030. Data obtained from the Justice Department include only 76 cases in which conviction was based on 18 U.S.C 1030. Of these 76 cases, only 50 were used.

Telephone Discussion

Telephone talk with CSI Director, Patrice Rapaplus, indicates that Corporate America and some organizations are still fearful of negative publicity. This is the primary reason for not reporting computer crime. There are organizations which do not have computer emergency response team in place. Computer crime is costing America more than $100 million a year, said Rapaplus. Rapaplus advised organizations to spend shrewdly on information security, training, and services than to incur heavy financial losses and public relation nightmare later on.

Further telephone discussion with FBI's special agent, Charles Mathews reveals that computer crime is a problem. Supporting Rapaplus, Mathews said that "there appears to be a reluctance on the part of the private sector to report allegations of computer crime to law enforcement. The FBI will continue to listen to and work with the private sector with goal of increased reporting."

To support this, the FBI established International Computer Crime Squads in selected locations throughout the United States. The mission of these squads is to investigate violations of Computer Fraud and Abuse Act of 1986, including other crimes where the computer is a major factor in committing the offense.

According to Janet Reno, Senators John Kyl, Patrick Leahy, and Charles Grassley are introducing legislation which will dramatically increase federal protection of data. Referring to the computer fraud and abuse act, Reno said "current law protects the confidentiality of financial information. This legislation would protect all government data against access without permission as well as criminalizing access by any one who exceeds his/her authority to gain access to both government and private data. As technology advances, computer crime has grown, so we have to ensure that the law keeps up with changing time." United States District Attorney, Donald Stern, said that wiretap order typically employed to monitor telephone conversations of organized crime and drug suspects are now used to trace and identify the illegal computer intruder. All of these statements support the theme of this report.

Statistical Technique

This report used sentencing data obtained from the Bureau of Justice Statistics, U. S. Department of Justice. The data consist of the fifty states in the U.S. including Washington D.C. SPSS summarize and descriptive statistics were used to generate the various tables found in this report.

FINDINGS

The report found that the present state of federal government computer crime policy shows a lack of central leadership, insufficient attention, and limited technical resources for investigating and punishing offenders. Without trained personnel who have expertise in the collection of computerized evidence, important evidence may be lost, or destroyed. In relation to the question, "why do there appear to be relatively few prosecutions? " The report found it unfortunate that computer crime tends to be glamorized by the media [21]. Often, the perpetrator is portrayed as an eccentric genius stealing from a faceless machine that epitomizes the establishment [16]. The glamorized image of the computer criminal by the media diverts public's attention from the damage caused by the computer criminal to the society.

In addition, fearful of negative publicity, corporations have an annoyingly schizophrenic attitude toward punishing offenders especially when the crime is committed by an employee [26]. Covering computer crime case saves face for companies because they are afraid to lose customers, especially if the victim is a financial corporation. There are cases where companies dismissed computer criminals but threw a lavish farewell party for the perpetrators to cover up the true reason for their departure [14]. Even though computer crime is immoral, offenders are presently evading justice. The study further provided answer to the question, "what are the limitations of legislative response to computer crime policy?" There are serious questions about the nature, extent, and direction of computer crime. "Much of the legislative effort to date has been based upon relatively simple minded assumptions about computer crime. The lack of an established knowledge base of computer crime and the mass media-influence push for legislation have created the potential for an ineffective response to the problem" [11]. This citation indicates that there are a number of relatively simple and general assumptions affecting how computer crime legislation is developing. The first assumption could be crime causality [5]. The assumptions based on causality are treated as certainties. Thus, they could affect legislative approaches to such issue as the type of individuals committing the crimes, their reasons for such acts, and the appropriate punishment against the perpetrator.

In fact, "in the testimony given before congressional committees and in public statements of legislators, computer-hackers tend to be considered as the prime computer criminals. Thus, legislative efforts on regulating computer crime often have significant hacker-type sections while overlooking the fact that a large proportion of cases of computer crime have been committed by trusted inside employees who have minimal computer sophistication" [13]. This emphasis on hackers and types of computer crime is influenced by the role of the media in affecting public opinion as well as legislative interest. This media-effect and its definition of computer crime could create pressure for quick legislative responses rather than policies which can be based upon years of legislative and legal precedents.

The second assumption underlying computer crime legislation is that computers and telecommunications systems are forms of technology [5]. This means that present day computer crime legislation lag behind technological advancements because current criminal and business laws are based upon earlier forms of technology. According to Roy Freed [12], the rules of law actually are dynamic and responsive to social needs when new fact situations are described accurately from a legal point of view. Complaints of inadequacy of existing rules with respect to computer subject matter mask frequently

either desires for legal treatments that are incompatible with social policy, such as the enlargement of rights of copyright owners, and failures to perform the legal steps professionally. The legislative responses dealing with computer crime is limited. There is a need for improving the implementation of computer crime policy.

The question, "how should governmental response to computer crime be improved?" can be partly answered from the analysis of federal statutes which indicate that there are absences of precise statute to combat computer crime. The statutes can partially be applied to some type of computer crime. They can not be completely used to punish offenders. Therefore, their use to punish offenders would create difficulties in gathering and presenting crime evidence. Courts would continue to lose computer cases because there are no precise computer crime statutes. Solving this problem requires enhancement of computer crime legislation drafted to sufficiently define the wrongful activity, deter computer crime, add certainty and uniformity for prosecutions, and encourage reporting of computer crimes [24]. Presently, computer crime statutes are becoming obsolete since computer technology and its application are changing and creating new methods of engaging in computer crime. The enhancement should be based on the present computer crime techniques and technological development of computers.

Furthermore, analysis of results found that computer criminals were frequently charged under general fraud offenses. Table 1 presents the distribution of cases charged by subsections of the Computer Fraud and Abuse Act of 1986, 18 U.S.C 1030. Table 1 shows that majority (54%, n = 27) of the criminals were charged and convicted of section 1030 (a)(4) known as general fraud. This means that existing fraud guideline adequately addressed the offense. Similarly, 24% (n = 12) of the defendants were convicted of subsection (a)(2) which is called accessing financial information improperly. The motivation here was to commit a fraud.

Table 1: Distribution of Cases Convicted Under 18 U.S.C 1030 by Subsection Charged

Subsection	Offense	Number	Percent[1]
(a)(1)	National Security Effect	0	0
(a)(2)	Accessed Financial Infor.	12	24
(a)(3)	Affect Government Computer	5	10
(a)(4)	General Fraud	27	54
(a)(5)	Information Alteration	1	2
(a)(6)	Password Trafficking	6	12

[1] Percentage total more than 100 percent because a defendant was charged under two subsections (a)(2) and (a)(4).

Among the 12 cases, 10 involved credit card fraud and 2 involved embezzlement of monies from financial institution. In addition, five defendants were convicted of accessing government computer under subsection (a)(3). Similarly, one defendant was convicted under subsection (a)(5), alteration of information. Six defendants who violated subsection (a)(6) were convicted of trafficking telephone access passwords. Existing fraud guideline provision of 18 U.S.C. 1030 adequately covered the above offenses.

The monetary loss due to computer crime can be found in Table 2, which shows that the median loss due to computer crime was between $10,000 and $20,000. A little over 78.3 percent of the cases involved loss less than $70,000. On final analysis of result, the report found that imposed penalties were not proportional to the type of offense committed. The mean sentence imposed was 6.8 months imprisonment. However, the data indicate

Table 2 Distribution of Cases Convicted Under 18 U.S.C 1030: by Monetary Loss

MONETARY LOSS	# OF CASES	PERCENT	CUM. %
$2,000 or less	10	21.7	21.7
More than $2,000	6	13.0	34.7
More than $5,000	6	13.0	47.7
More than $10,000	4	8.7	56.4
More than $20,000	6	13.0	69.4
More than $40,000	4	8.7	78.1
More than $70,000	3	6..5	84.6
More than $120,000	1	2..2	86.8
More than $200,000	2	4.4	91.6
More than $350,000	2	4.4	95.6
More than $500,000	0	0.0	0.0
More than $800,000	2	4.4	100.0

that defendants who committed offenses such as minor vandalism of computer or data, browsing computer system, or demonstrating computer prowess were placed on probation. The average sentencing for defendants who committed fraud, theft, or embezzlement was 7 months imprisonment. Whereas the defendants whose crime affected administration of justice or committed industrial espionage received 17.3 months imprisonment on average.

Crime Occurs	Attention Given to Prosecuting	Investigate and Arrest Perpetrator	Charge Perpetrator to Court and Investigate
Objectives Stopping Crime and Maintaining Crime Data			
Prosecute Perpetrator	Fine/Serve Term	Maintain Data on Crime Causality, Investigation, and Detection Process	Computer Crime is Favorably altered

.

CONCLUSION AND RECOMMENDATION

The potential for grave computer crimes against the public and private sectors information systems are a major challenge to Congress. The advances in technology and information systems suggest the need for immediate concerted efforts to control computer crime. Therefore, this report concludes and recommends that (a) there is no consensus definition of computer crime, (b) law enforcement agencies should treat computer crime as a priority, (c) existing laws should be enhanced to more specifically cover computer crime problems, and (d) creating legislation which would include computer crime as a part of a larger coordinated information technology legislative review.

There are few individuals who are capable of providing detective and preventive services to agencies that prosecute computer criminals. Therefore, adequate implementation provision should be made to train law and computer professional. In addition, Congress should (a) provide funding for basic research on computer crime problems, and (b) mandate extensive crime detection and reporting efforts.

In conclusion, evaluation provides the means to continuously monitor policy or program activities so as to determine how well it is meeting its objectives or even whether the objectives should continue to prevail [25]. If the program objectives are not met, then a measure would be taken to meet the desired implementation or outcomes in the prescribed period. Moreover, evaluation generally requires an agreed period of stability before a program is evaluated. This agreed period of stability may be monthly, quarterly, semi-annually, annually, etc., depending on the type of program [9].

Thus the report, in addition to all the above recommendation, further recommends that legislative oversight [7] through rotating zero-base budgeting [10] be used to evaluate the computer crime problem. This would be incorporated with the application of sunset legislation [7]. Although, traditional zero-base budgeting is done annually, but this report calls for three year periodic evaluation. This would enable the programs to have meaningful stability before formal evaluation can be done. The proposal will use Figure 1 as its evaluative model.

Figure 1: Computer Crime Policy Implementation and Evaluation Model:

Objectives Identifying Crime

(Adapted from Public Budgeting: Program Planning and Evaluation by Fremont J. Lyden and Ernest G. Miller, 1978; 153 but slightly modified).

The model assumes that computer crime would be exposed, prosecuted, maintain data, and be altered. Each objective would have measuring scales ranging from 1 to 10 depending on how Congress would want it to be. The scales would be used for evaluation.

SUMMARY

In summary, computer crime is a major problem that has not been addressed. Congress has tried to enact laws that would stop computer crimes over the years, yet its effort is hampered by speedy technological advancements and inappropriate definition of computer crime. Presently, law enforcement agencies are not equipped with the necessary skills and the manpower required to investigate and prosecute computer criminals. Even though 18 U.S.C 1030 is the predominant law over computer crime. There are many statutes which can be used to punish offenders.

REFERENCES:

[1] Becker, L. **Computer Security: An Overview of National Concerns and Challenges**. Washington, D. C.:Congressional Research Service,1983.

[2] Bequai, A. **Computer Crime**. Lexington: Lexington Books, 1988.

[3] Bentham, J. **An Introduction to the Principles of Morals and Legislation.** New York: Oxford University Press, 1823.

[4] Bloombecker, J. The Trial of Computer Crime. **International Business Lawyer**, 1981, vol. 9 (September), 429-432.

[5] Burk, R. D. The Philosophies of Computer Crime Legislation: An Editorial Collection. **Computer Law Reporter**, 1984, Vol. 3 (Nov), 3.

[6] Carroll, J. **Computer Security**. Boston: Butterworth Publishers,1987.

[7] Chandler, C. R. & Plano, C. J. **The Public Administration Dictionary.** Santa Barbara: ABC-Clio, Inc., 1988.

[8] Conly, H. C. **Organizing for Computer Crime Investigation and Prosecution**. Washington, D. C.: National Institute of Justice,1989.

[9] Deniston, O. L., Rosenstock, I., Welch, W., & Getting, V. A. Evaluation of Program Effectiveness and Program Efficiency. **In F. J. Lyden & E. G. Miller (Ed.), Public Budgeting: Program Planning and Evaluation**. Chicago: Rand McNally College Publishing Company, 1978.

[10] Fogarty, B. A., & Turnbull, A. Legislative Oversight through a Rotating Zero - Base Budget. **In F. J. Lyden & E. G. Miller (Ed.), Public Budgeting: Program Planning and Evaluation**. Chicago: Rand McNally College Publishing Company, 1978.

[11] Samantha Fordyce, S. Computer Security: A Current Assessment. **Computers and Society**, 1982, Vol. 1 (January), 12.

[12] Freed, R. Legal Interests Related to Software Programs. **Jurismetrics**, 1985, Vol. 25 (March).

[13] Glynn, A. E. Computer Abuse: The Emerging Crime and the Need for Legislation. **Fordham Urban Law Review**,1984, Vol. 12 (Jan), 83-84.

[14] Hefner, K. Is Your Computer Secure? **Business Week**, 1988, 70 (August 1), 70.

[15] Hollinger, R., and Lanza-Kaduce, L. The Process of Criminalization: The Case of Computer Crime Laws. **Criminology**, 1988, vol.16 (January), 104.

[16] Mandell, S. L. Computer Crime. **In M. D. Ermann, M. B. Williams, & C. Guitierez (Ed.), Computers, Ethics, and Society.** New York: Oxford University Press, 1990.

[17] McEwen, T. & Nugent, H. **Results of the National Assessment Survey: Police and Sheriffs, Research In Action**. Washington, D. C.: National Institution of Justice, 1988.

[18] McFarlane, J. D. **Senate Judiciary Subcommittee Hearings on S.240: The Federal Computer Systems Protection Act of 1979**. Washington, D. C.: House of Senate, 1980.

[19] Naisbitt, J. **Megatrends: Ten Directions Transforming Our Lives**. New York, New York: Warner Books, 1982.

[20] Nycum, S. H. The Criminal Law Aspect of Computer Abuse: Part II: Federal Criminal Code. **Rutgers J. Computers of Law**, 1976, Vol. 297 (April), 305-310.

[21] Oz, E. **Ethics for the Information Age**. Boston, MA: Wm. C. Brown Communications, Inc., 1994.

[22] Parker, D. **Computer Crime: Criminal Justice Resource Manual**. Washington, D. C.: National Institute of Justice, 1989.

[23] United States House Subcommittee on Transportation, Aviation and Material. **Computer and Communications Security and Privacy**. Washington, D. C.: House of Representatives, 1984, 28, 30, 198.

[24] Wharton, L. Legislative Issues in Computer Crime. **Harvard Journal on Legislation**, 1984, Vol. 21 (Winter), 239-254.

[25] Wildavsky, A. **Speaking Truth to Power: The Art and Craft of Policy Analysis**. New Brunswick, NJ : Transaction Books, 1987.

[26] Computer World. **The Real Target**. Feb. 27, 1989, 20.

[27] Charles Mathews, **FBI, U.S. Department of Justice**, Chicago, IL.

[28] Patrice Rapalus, **Computer Security Institute**, San Francisco, CA.

[29] Janet Reno, Attorney General, **U.S. Department of Justice**, Washington D. C.

[30] John Scalia, **Bureau of Justice Stattistic, U.S. Department of Justice**, Washington D.C

[31] Donald Stern, United States Attorney, **District of Massachusetts, U.S. Department of Justice**, Boston, MA.