United States General Accounting Office 149663

GAO

Testimony

Before the Subcommittee on Information, Justice, Agriculture, and Transportation, Committee on Government Operations, and the Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, House of Representatives

For Release on Delivery
Expected at
10:00 a.m.
July 28, 1993

NATIONAL CRIME INFORMATION CENTER

Legislation Needed to Deter Misuse of Criminal Justice Information

Statement of
Laurie E. Ekstrand, Associate Director
Administration of Justice Issues
General Government Division

GAO/T-GGD-93-41

NATIONAL CRIME INFORMATION CENTER: LEGISLATION NEEDED TO DETER MISUSE OF CRIMINAL JUSTICE INFORMATION

SUMMARY STATEMENT OF LAURIE E. EKSTRAND
ASSOCIATE DIRECTOR, ADMINISTRATION OF JUSTICE ISSUES
U.S. GENERAL ACCOUNTING OFFICE

The National Crime Information Center (NCIC) is the nation's most extensive criminal justice information system and is maintained by the Federal Bureau of Investigation (FBI). NCIC contains over 24 million records in 14 files and provides user agencies with information on items such as missing and wanted persons, stolen vehicles, and criminal history records. Over 19,000 law enforcement and other criminal justice agencies in the United States and Canada can access NCIC through their computer systems.

The Chairman of the Subcommittee on Information, Justice, Agriculture, and Transportation, House Government Operations Committee, requested that GAO review NCIC to (1) determine if the system has adequate controls to prevent misuse and (2) obtain any FBI and state assessments of the extent and nature of NCIC misuse and examples of such misuse. To fulfill the request, GAO interviewed officials from the FBI and the 54 state agencies that oversee local user agencies; visited user agencies in 3 states; and reviewed relevant documentation.

GAO found that NCIC is vulnerable to misuse from individuals with authorized access, or "insiders" because of (1) the system's inherent risk and (2) the control limitations in some state criminal justice information systems through which users access NCIC. Since NCIC is a network of coordinated state systems, and the same information can be accessed from any one of these systems, the control limitations in one system render the entire network vulnerable to misuse. While the security features of the upgraded NCIC 2000 system are positive steps to address the system's vulnerability, potential capability and implementation limitations could diminish their effectiveness. Most significant of these limitations is that the states will not be required to implement NCIC 2000's security features.

GAO also found that the FBI and states do not systematically assess the extent and nature of NCIC misuse. However, examples of such misuse showed that NCIC has been misused both intentionally (disclosing information to private investigators in exchange for money) and unintentionally (conducting background investigations on applicants for noncriminal justice employment). The individuals misusing NCIC generally have not been criminally prosecuted, in part because of the lack of directly applicable federal and state statutes. Instead, these individuals have generally received administrative sanctions, ranging from reprimands to termination of employment. GAO recommends that (1) Congress enact legislation with strong criminal sanctions for misuse of NCIC to provide a better deterrent to such misuse and (2) NCIC's security policy requirements be re-evaluated.

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to testify about work we did at the request of the Chairman of the Subcommittee on Information, Justice, Agriculture, and Transportation, House Government Operations Committee, on the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC). NCIC provides federal, state, and local law enforcement and other criminal justice agencies with information on items such as missing and wanted persons and stolen vehicles and other property. NCIC also provides criminal history record information on individuals through its largest file, the Interstate Identification Index (III). Federal regulations and NCIC policy have classified NCIC information as sensitive and have restricted access to and use of such information to authorized criminal justice agencies for criminal justice purposes. These purposes include conducting criminal investigations or screening applicants for employment in criminal justice positions.

In December 1991, 20 individuals in New Jersey and Florida were indicted under federal bribery, theft of government property, and computer fraud statutes[1] for selling criminal history information obtained from NCIC. The Subcommittee viewed these indictments as support for general allegations that NCIC information is routinely made available for unauthorized purposes by some federal, state, and local law enforcement agencies. Citing these allegations, the Subcommittee requested that we (1) determine whether the FBI and user agencies have adequate controls to ensure access to NCIC is for authorized purposes, and deter and detect misuse[2] of NCIC information; and (2) obtain the FBI's and the states' assessments of the extent and nature of any NCIC misuse and examples of such misuse.

To fulfill the Subcommittee's request, we interviewed FBI officials responsible for NCIC; reviewed NCIC and state and local agency security and other relevant documentation; and visited state and local law enforcement agencies who use NCIC in California, Nevada, and Texas and interviewed relevant officials from these agencies. We did this work to obtain a description of the system and its controls and to learn how it operates. We also observed the physical security of NCIC terminals at the locations visited and the controls and safeguards for accessing and disseminating information from the system.

---

[1]18 U.S.C. 201, 18 U.S.C. 641, and 18 U.S.C. 1030.

[2]Misuse refers to access to, and disclosure and use of, NCIC information for unauthorized purposes, such as background investigations for noncriminal justice employment.

In addition, we did a telephone survey of all 54[3] state control terminal agencies (SCTA) that oversee local user agencies in the United States and Canada to obtain information on state and local agency access to NCIC; access and dissemination controls; and the extent of unauthorized disclosure and use of NCIC information. We administered our survey between January 25 and February 18, 1993. We did not verify the accuracy of the information provided during the survey.

Finally, to obtain assessments of NCIC by computer security experts, we reviewed an NCIC risk analysis by MITRE Corporation prepared for the FBI in 1989; a report by Computer Professionals for Social Responsibility prepared for the Subcommittee on Civil and Constitutional Rights, House Judiciary Committee, in 1989; and a report by SRI International (formerly Stanford Research Institute) prepared for the FBI in 1990. We also interviewed the author of the SRI report. A more complete description of our scope and methodology appears in Appendix I.

BACKGROUND

NCIC is the nation's most extensive computerized criminal justice information system. The system consists of a central computer at FBI headquarters in Washington, D.C.; dedicated telecommunications lines; and a coordinated network of federal and state criminal justice information systems. NCIC provides users with access to over 24 million records in 14 files, such as files on wanted persons, stolen vehicles, and missing persons. NCIC's largest file, the III file, provides access to about 17 million criminal history information records contained in state systems.

Because it is a cooperative effort between the federal government and the states, NCIC is a decentralized system. Specifically, the NCIC Advisory Policy Board (APB), which is composed of managers of state and local user systems, is responsible for establishing and implementing the system's operational policies, including security. The FBI is responsible for overall management of NCIC. The 54 SCTAs, through agreements with the FBI, are responsible for maintaining their state's criminal justice information systems through which local user agencies access NCIC. The SCTAs also are responsible for overseeing the federal, state, and local user agencies in each state.

Over 19,000 federal, state, and local law enforcement and other criminal justice agencies in the United States and Canada can access NCIC directly. About 97,000 computer terminals in these agencies can access NCIC. An additional 51,000 law enforcement

---

[3]This number represents the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and Canada.

and other criminal justice agencies can access NCIC indirectly through agreements with user agencies that have direct access. More than 500,000 individuals within the user agencies can access NCIC, either directly from their own computer terminals or indirectly through computer terminal operators.

The Originating Agency Identifier (ORI), a nine-character code assigned by the FBI to each user agency, is the primary control for accessing NCIC. The ORI controls user agency access to NCIC by identifying each agency to the system and determining the levels of access to NCIC files and types of functions allowed, such as inquiries and requests for records.

NCIC IS VULNERABLE TO MISUSE

NCIC is vulnerable to misuse because of its inherent risk and the inadequacy and ineffectiveness of some of its controls. Individuals with authorized access, or "insiders", pose the greatest security threat to the system. Since NCIC is a network of coordinated state systems and the same information can be accessed from any one of these systems, the control limitations in one system render the entire network vulnerable to misuse. While NCIC 2000's security features are a positive development in the effort to address the system's vulnerability, potential limitations in their capabilities and implementation could diminish their effectiveness.

Insiders Are the Greatest Security Threat to NCIC

A 1989 NCIC risk analysis by MITRE Corporation concluded that insiders were the greatest security threat to NCIC. Another security expert, who has studied NCIC, and FBI and SCTA officials we spoke with also identified the insider as the greatest security threat to NCIC. These sources indicated that insiders pose the greatest threat to NCIC because they know the system and can misuse it by obtaining and selling information to unauthorized individuals, such as private investigators, or altering or deleting information in NCIC records. Insiders can access NCIC either by pretending they are involved in legitimate law enforcement activity, or by masquerading their real identity when identifying themselves to the system.

NCIC Is Inherently Risky

NCIC is inherently risky[4] because (1) its security policy is too broad, contains only minimum requirements, and does not require

---

[4]To determine NCIC's inherent risk, we used criteria contained in a GAO policy guide titled Assessing Compliance With Applicable Laws and Regulations, (GAO/OP-4.1.2, Dec. 1989). This guide supplements the Yellow Book standards on internal controls.

specific controls, thus resulting in state systems with different controls; (2) its many users generate a large number of transactions; (3) the information contained in its files is valuable and in demand and can be used for unauthorized purposes; (4) the incentives for misuse outweigh the potential penalties; and (5) misuse has been repeatedly reported in FBI audits.

NCIC Security Policy Is Too Broad and Contains Only Minimum Requirements

According to the GAO policy guide criteria for determining inherent risk, vague regulations contribute to such risk. Even though the NCIC APB regards the NCIC Security Policy as a comprehensive document, the Policy is too broad and contains, by its own acknowledgement, only minimum requirements for NCIC security in six general areas: (1) background screenings of employees and discipline standards for policy violators; (2) physical security and access to NCIC terminals; (3) authorization and oversight of user agencies; (4) technical safeguards, such as automated audit trails; (5) dissemination of NCIC information; and (6) biennial audits of local users to measure compliance with NCIC policies. While the Policy allows the SCTAs to establish stricter requirements at their discretion, it does not require specific access controls.

Specific access controls not required

While the NCIC Security Policy requires some minimum controls, it does not require specific controls, such as unique passwords or identifiers, to control access and identify authorized users. According to FBI officials and a computer security expert, the Policy does not require such controls because of potential resistance by the states to federal encroachment on their sovereignty, restrictions imposed by state security policies, and the lack of funding to implement passwords and other controls. In addition, FBI officials stated that since most NCIC files do not contain sensitive information, they may not require additional protection. However, this position seems to be inconsistent with the fact that the Policy has classified all information in the system as sensitive and in need of protection.

The Security Policy's position on access controls and identifiers also appears to be inconsistent with the fact that insiders have been identified as the greatest security threat to NCIC. In this regard, there is no requirement to identify such individuals through unique identifiers that cannot be compromised. While the Policy requires that automated audit trails identify the terminal operator, requester, and secondary recipient of III file information "in some way," including name, badge or serial number, or other unique number, such identifiers are not confidential, nor are they monitored by NCIC's central computer. Insiders can use identifiers that are not confidential to

disguise their identities and prevent their identification in audit trails. Furthermore, the data fields that record such identifiers can sometimes be bypassed, either by entering erroneous data, or simply using the space bar on a computer terminal's keyboard to exit the data fields without entering any data. For example, a user, or users, in a law enforcement agency in Texas were able to disguise their identity by using the name of a former employee of that agency and the names of months. Users in another law enforcement agency in Texas were able to bypass an identification data field by entering letters such as "XYZ," while users in an agency in Nevada were able to bypass an identification data field by using the keyboard space bar.

Computer security experts have determined that unique identifiers are important for user identification, authentication, and accountability. Unique identification is the process through which individuals identify themselves to a computer system. Authentication is the process of ensuring that the identification provided to the system is likely to be correct. Accountability combines authentication with the review of audit trail information to trace a sequence of events in a computer system back to a specific individual. According to a computer security expert and Department of Defense computer security criteria, these three steps in combination are the most fundamental requirements for deterring and detecting misuse and enhancing computer system security.

State systems use different types of access controls

Since the NCIC Security Policy does not require specific access controls, state systems use different types of controls for accessing NCIC. For example, systems such as those in Alabama, Arizona, California, and Texas use computer terminal configurations, sometimes called "security tables," to control access to NCIC. These configurations control which individuals can access NCIC, the types of information they can access, and the functions they can perform. For example, a terminal operator may be authorized to access all NCIC files except the III file, which contains criminal history information. Within the files accessed, this individual may be authorized to perform only inquiries. State systems such as those in Illinois, Nebraska, and Washington use ORIs in terminal configurations to identify users accessing NCIC and control access to the system's files.

Although not required by the Security Policy, some state systems also use passwords or other identifiers to control access to NCIC. Specifically, only 19 systems require unique or general passwords or identifiers to access NCIC. However, it should be noted that 30 state systems require either unique or general passwords or identifiers for initial access to these state systems through which local user agencies access NCIC. Some state systems, such as those in Maryland and New York, use

passwords or other identifiers in combination with terminal configurations to control access to NCIC. The FBI also uses passwords to control access to NCIC. However, the FBI requires passwords only for accessing NCIC from terminals located in its headquarters, while FBI field offices adhere to password and other security policies established by the states in which they are located. According to FBI officials, they do not have influence over the establishment and implementation of state security policies.

Most state systems use automated audit trails to track NCIC user activity and the dissemination of criminal history information. The Security Policy requires that audit trail information be maintained for a minimum of 1 year for the III file. To meet this requirement, states maintain III file audit trail information for different lengths of time. For example, states such as Colorado, Kentucky, and Wyoming maintain audit trail information for a minimum of 1 year, while states such as Montana, Virginia, and Washington maintain such information indefinitely. The FBI maintains NCIC audit trail information for 10 years.

The minimum requirements in the Security Policy, which do not call for specific access controls, have allowed the states to implement relatively simple controls, such as computer terminal configurations, for their own systems and still meet these minimum requirements. Furthermore, since NCIC is a network of coordinated state systems and the same information can be accessed from any one of these systems, simple controls in some systems compromise the entire network and render it vulnerable to misuse. For example, an employment firm obtained III file information from a law enforcement agency in Georgia. However, when this activity was discovered in Georgia, the firm began using a law enforcement agency in South Carolina to obtain the same information.

NCIC Users Generate Large Numbers of Transactions

According to the GAO policy guide criteria, the more transactions there are involved in an activity, the greater the chances of noncompliance with policies due to errors, irregularities, and abuse. This is especially true if the activity is delegated outside the government's control, in this case to the SCTAs and local user agencies, without active monitoring or oversight. Furthermore, the large number of transactions increases the difficulty of detecting such abuse. FBI, SCTA, and local user agency officials told us that the large number of transactions generated by NCIC's users makes it easier for insiders misusing the system to disguise their activities and more difficult for the system's audit trails to detect these activities.

In this regard, since NCIC is the nation's most extensive criminal justice information system, the more than 70,000 agencies and 500,000 individuals who use the system generate a large number of transactions, including inquiries and requests for records. The number of NCIC transactions has increased significantly since 1967, when the system became operational. Specifically, in 1992 NCIC users generated about 438 million transactions, or about 1.2 million a day, compared to about 2 million transactions in all of 1967. Over 28 million of the 1992 transactions involved NCIC's III file.

NCIC Information Is Valuable and Has Been Used For Unauthorized Purposes

According to the GAO policy guide criteria, assets such as NCIC information that are readily marketable or could be used for personal purposes are very susceptible to improper use and contribute to a system's inherent risk. Federal regulations[5] and the NCIC Security Policy regard NCIC information as sensitive and generally restrict access to and use of such information to authorized criminal justice agencies for criminal justice purposes. These purposes include conducting criminal investigations and screening applicants for criminal justice employment, or, through special agreements with authorized federal agencies, for granting security clearances.

However, in addition to its legitimate uses, information contained in NCIC's files is valuable and has been used by insiders for unauthorized purposes. Specifically, the examples of misuse we obtained in our review showed that insiders used NCIC information for personal purposes, such as determining whether friends or relatives had criminal records, or sold it to private investigators who used the information to conduct background investigations on applicants for employment. Furthermore, during a July 1992 congressional hearing on the sale of criminal history records, FBI officials testified that there was a demand for NCIC information because such information is valuable to individuals other than criminal justice professionals, including private citizens, employers, parents, and politicians.

Incentives For Misuse Outweigh Potential Penalties

According to the GAO policy guide criteria, certain characteristics of a system, such as incentives for misuse, increase the susceptibility to noncompliance and thus contribute to inherent risk. In this regard, the examples of NCIC misuse we obtained showed that the incentives for such misuse, such as personal gain or money, may have outweighed the potential

---

[5]28 C.F.R., Chapter I, Part 20, Section 20.33.

penalties. As discussed later, there are no federal or state statutes specifically directed at misuse of NCIC. In the majority of cases, the penalties for such misuse have in the past been limited to administrative sanctions, such as written or oral reprimands, suspensions, or termination of employment.

During the July 1992 congressional hearing, FBI officials also testified that existing federal statutes have not been adequate to deter misuse of NCIC because the market for its information is too lucrative. Individuals are willing to pay to obtain NCIC information, even though they are not authorized to receive it.

Misuse Repeatedly Reported in User Audits

According to the GAO policy guide criteria, the repeated disclosure of problems in audits is a factor in assessing the inherent risk of a system. Our review of audits of NCIC user agencies, conducted by the FBI, showed that misuse of NCIC, such as using the system to conduct background investigations of applicants for noncriminal justice employment, and other incidents of noncompliance with NCIC policy were repeatedly reported.

More specifically, our review of FBI audits of SCTAs showed that 46 SCTAs had not corrected misuse and other problems identified during the most recent audits. Uncorrected problems included using the III file for noncriminal justice purposes, not meeting the biennial audit requirement, and not implementing training programs. Six SCTAs had corrected problems identified during previous audits. Audit reports for Canada and the U.S. Virgin Islands were not available.

Some NCIC Controls Are Either Not Adequate or Are Not Being Used Effectively to Deter or Detect Misuse

Office of Management and Budget Circular A-130 establishes policy guidance for systems like NCIC. More specifically, the circular requires that agencies establish a level of security commensurate with the sensitivity of the information and the risk and magnitude of the loss or harm that could result from the improper operation of the system. The guidance further indicates that for applications considered sensitive, the management control process shall, at a minimum, include security specifications and design review and system tests. It further advises that the tests ensure that administrative, technical, and physical controls are operationally adequate. While the NCIC Security Policy includes security specifications, as discussed below, the controls in some state systems in the NCIC network are not adequate, nor are they being used effectively to promote a level of security that effectively detects and deters misuse. The control limitations, combined with NCIC's inherent risk, could increase the system's vulnerability to misuse.

Access Controls of Some State Systems Are Not Adequate

The access controls of some state systems are not adequate to deter and detect misuse of NCIC, even though these controls appear to meet the minimum requirements of the NCIC Security Policy. The controls are not adequate because they lack unique individual user identification, authentication, and accountability. For example, SCTA officials from Arizona, Michigan, New York, and Washington cited as a weakness in their systems accessing NCIC the lack of user identification and accountability. As discussed earlier, computer security experts have emphasized that identification, authentication, and accountability are essential in deterring and detecting misuse of computer systems.

We found that security controls in state systems could be adversely affected by the lack of unique user identification. Specifically, the most commonly used control, terminal configurations, are not adequate to control access if users do not use unique identifiers. According to a computer security expert, while ORIs are used as identifiers, they often identify only the agency, rather than individual users or terminals. For example, the Los Angeles Police Department had over 1000 terminals with which to access NCIC but presented only 1 ORI to the system. Insiders seeking to misuse NCIC can use systems such as this without disclosing their identity. For example, a police officer conducted background searches on an individual from a court terminal, instead of his own, seeking to disguise his identity. The state in which this incident occurred does not require unique or general passwords or other identifiers for accessing NCIC. Instead, access to NCIC is controlled by a terminal identifier and an agency ORI. The officer was detected because the subject of his searches complained.

The lack of unique identifiers in state systems can also affect accountability in audit trails. Specifically, 17 state system audit trails do not identify the individual accessing NCIC, but only the terminal from which a transaction originated, thus potentially hindering the identification of those responsible for misuse. According to computer security experts, user identification is essential for audit trails because they are the last recourse for detecting and identifying those misusing NCIC. For example, SCTA audits of five large law enforcement agencies in Texas, a state which does not require a unique password or other identifier to access NCIC, determined that these agencies' audit trails were not recording the identities of terminal operators, or, in some cases, the identities of requesters of criminal history record information, making the identification of those responsible for misuse virtually impossible.

Insiders who know the state systems and their control weaknesses, can take advantage of inadequate controls to access the system by

using false identities, also known as masquerading. For example, a terminal operator in a sheriff's office in Texas accessed NCIC using fictitious identifiers and used the information he obtained for unauthorized purposes. An ensuing investigation could not conclusively determine the nature of these purposes.

In contrast, we found several examples of state systems with relatively more extensive controls for accessing NCIC. These controls emphasized user identification, authentication, and accountability. For example, one state system required a unique operator identifier to access NCIC. This identifier consisted of one alphabetic character, operator social security number, and an optional eight-character identifier. Another state system required a terminal identifier, an individual access code, and an individual password to access NCIC. In addition, the system required a system-wide access code and password to access NCIC's III file.

Some Existing Controls Are Not Being Used Effectively

Some existing controls, specifically audit trails and biennial audits, are not being used effectively to detect or deter NCIC misuse. On the basis of our discussions and telephone survey, we found that the FBI and 25 of the SCTAs review audit trail information only during the biennial audits of SCTAs and local user agencies. According to FBI and SCTA officials, they do not review such information more frequently because of the large number of transactions generated by users and staff shortages. The lack of frequent reviews of audit trail information may result in significant incidents of misuse not being detected. For example, according to FBI officials, even though transactions related to the misuse were recorded in audit trails, the most significant case of NCIC misuse was detected through an anonymous tip. The FBI was alerted about the misuse when a price list was mailed to a federal agency advertising the availability of government information, including NCIC information. The FBI investigated this incident and then, using audit trail information, uncovered an extensive network of insiders misusing NCIC.

In contrast, 16 SCTAs contacted in our telephone survey told us that they review audit trail information more frequently than during biennial audits. These SCTAs review such information either daily, weekly, monthly, quarterly, or annually. For example, one SCTA official described an extensive security program for NCIC that includes monthly reviews of audit trail information. The monthly review of such information seeks to detect unusual or suspicious levels of activity by individual terminal operators. In addition, the security program includes unannounced security visits to local user agencies where audit trail information is also reviewed, and the required biennial audit of local user agencies. According to this official, the

security program has been successful and there have been very few incidents of NCIC misuse since its inception. He described one incident in which the review of audit trail information detected the most significant case of NCIC misuse in his state. Specifically, the review detected a law enforcement officer who was conducting background searches on individuals seeking employment with a nationally known firm. In another example, an SCTA official also described an incident in which the weekly review of audit trail information detected a police dispatcher who was conducting background searches on her fiance's political opponents.

The NCIC Security Policy requires that the SCTAs biennially audit local user agencies, and that the FBI biennially audit the SCTAs. Our survey and discussions with FBI and some SCTA officials showed that they are not meeting the biennial audit requirement, mainly because of staff shortages, budget constraints, and the large numbers of agencies to be audited. Specifically, according to an FBI official, the FBI is able to audit the SCTAs only every 30 months, while, according to our survey, 16 SCTAs are able to audit local user agencies only every 30 to over 48 months. The delays of the FBI audits could continue, given the staffing shortages at the Bureau's Criminal Justice Information Systems Division. Our survey found that 36 SCTAs currently comply with the biennial audit requirement--2 SCTAs did not know if they were complying with the requirement. Delays of these audits beyond the 2-year requirement may prevent the timely detection of NCIC misuse. Furthermore, the review of such information during the biennial audits of user agencies who maintain audit trail information only for 1 year would not reveal any misuse that may have occurred more than a year from the time of the audit.

The FBI and SCTAs use these audits of user agencies to evaluate the effectiveness of system controls and to measure compliance with NCIC policies. However, during our telephone survey, only 45 SCTAs reported using these audits as a means to detect misuse of NCIC, usually by sampling audit trail information. Similarly, the NCIC Security Policy does not require a specific audit step to detect misuse.

NCIC 2000 Attempts to Address Security Concerns, But Potential Limitations Could Diminish Effectiveness

In 1986, the FBI began planning to upgrade the current NCIC system. The proposed upgraded system, called NCIC 2000, will be composed of a Central Segment at FBI headquarters, workstations for user agencies, and mobile imaging units for patrol cars. NCIC 2000 will provide new system software and additional capabilities, including receiving, storing, and transmitting images of persons and property and analyzing digitized fingerprints. The contract for NCIC 2000 was awarded in March 1993 to Harris Corporation. The FBI expects to implement its

segment of NCIC 2000 by March 1995, while the states are required to be operationally capable by March 1998.

In an attempt to address concerns about security, NCIC 2000 is to also include certain security features that the current system does not have. According to FBI officials, the features are based on findings and recommendations of a 1989 NCIC risk analysis by MITRE Corporation and a 1990 report by SRI International on security controls for computer systems accessing NCIC. NCIC 2000's Central Segment and workstations will have the Department of Defense's C2 and D2 security ratings respectively.[6] Specific security features of the Central Segment include access control, a data encryption system to protect data transmissions from outside intruders (hackers); and a knowledge-based intrusion detection system designed to detect unusual, and potentially unauthorized, levels of user activity based on established usage patterns, called "user profiles."

We believe that while the planned security features may ultimately be helpful in improving NCIC's security, their potential limitations and limited implementation could diminish their effectiveness. The author of the SRI report, while acknowledging that the FBI is making a good effort to address his report's recommendations, also stressed that NCIC 2000 will remain vulnerable to misuse because of the security features' potential limitations and their limited implementation, particularly at the state and local levels.

Potential Limitations of Security Features

NCIC 2000's security features have potential limitations that could diminish their effectiveness. According to SCTA officials, while the security features may reduce NCIC 2000's vulnerability, the threat to the system from insiders will remain. For example, the Chairman of the NCIC APB told us that the threat from insiders will always be present in a system like NCIC because of both its nature and the number of users with authorized access.

According to FBI officials, the system's Central Segment will provide only limited security for the state systems. For example, it will provide accountability only to the ORI level by identifying the user agency accessing the system, rather than to the individual user level. Furthermore, according to a computer security expert, a C2 security rating would be only a minimum starting point for systems accessing NCIC, with evolution to some

---

[6]C2-level security includes individual identification and authentication, access control, and audit. D2-level security includes similar features adapted for personal computers.

of the requirements of higher ratings to further improve security.

According to FBI officials, the data encryption feature will encrypt only data transmitted between the FBI and state systems. The same data will not be encrypted when transmitted from the state systems to local user agencies, leaving the data still vulnerable to potential hackers. One of these officials questioned the need for encryption because NCIC data are already unreadable during their transmission through dedicated communication lines. According to this official, it would be very costly, time consuming, and difficult for hackers to access NCIC data during transmission. It would be more cost effective for such individuals to obtain information from NCIC through an insider. In addition, hackers have not been identified as primary security threats to NCIC. In this regard, none of the examples of NCIC misuse we obtained during our review involved hackers.

According to FBI officials and a computer security expert, the intrusion detection system also has potential limitations. First, according to an FBI official, each individual user will not have a user profile. Instead, groups of users, such as dispatchers and detectives, would have group profiles. Second, individual incidents of misuse, unlike high-volume patterns of such incidents, may not be detected because they may not appear to be all that unusual. In fact, according to an FBI official, the system will primarily detect data input errors and only the most blatant violations. Furthermore, according to a computer security expert, the system will not detect occasional misuse by an insider, but only repeated transactions not authorized for a user agency or the most obvious violations, such as an individual attempting to download an entire NCIC file. Third, the FBI plans to monitor user activity through the Central Segment's own intrusion detection system and alert specific agencies when unusual activity is detected. However, an FBI official acknowledged that given the shortage of FBI personnel in its Criminal Justice Information Systems Division, which is responsible for NCIC, it will be very difficult to adequately monitor and report user activity.

Limited Implementation of Security Features

As currently planned, only the FBI will implement the NCIC 2000 workstations at its headquarters, including the security features, to access the system. According to FBI officials, the states will be offered the opportunity to buy standardized workstation packages, including the security features, to access NCIC 2000. However, the states will not be required to purchase the workstations because of potential incompatibility with their own computer systems and limited funding. FBI officials estimated the cost to outfit all users with workstations at about

$2 billion. To access NCIC 2000, the states will either have to buy the workstation packages, buy and modify them to fit their own systems, or develop their own workstations. Twelve SCTA officials we contacted subsequent to our telephone survey told us that they would either fully implement NCIC 2000 by purchasing through the FBI procurement, modify FBI workstations to be compatible with their states' systems, or develop or modify their own systems to provide the required capability.

When developing their own workstations, the states will also not be required to include NCIC 2000's security features because of funding and system compatibility considerations. Furthermore, according to the FBI, there is no incentive for the states to comply with NCIC 2000 security features. Specifically, as currently planned, the NCIC Security Policy will not be modified to require compliance with NCIC 2000 standards, nor will the states receive financial support for implementing the system. In addition, according to FBI officials, there are no sanctions that the FBI can realistically impose on the states for such noncompliance. For example, revoking a state's access to NCIC would be counter to the system's mission of assisting law enforcement agencies. However, in our follow up to the survey, several of the SCTA officials we contacted told us that they would implement some of the security features, such as data encryption or passwords, if funding becomes available.

The 12 SCTA officials we contacted also identified certain barriers that may affect the overall implementation of NCIC 2000. First, funding shortages may prevent local user agencies from fully implementing the new system. For example, in one state, local user agencies will not be required to purchase imaging units or fingerprint scanners, while in another state all local user agencies may not immediately implement the mobile imaging units. Second, hardware and software compatibility problems may delay implementation. For example, one SCTA official told us that some hardware and software compatibility problems will delay implementation, making it more difficult to meet the 5-year deadline. Third, staff shortages at the FBI's Criminal Justice Information Systems Division will affect training and other technical assistance to the states. The Chairman of the NCIC APB also said that training will be an issue in every state.

A conference of NCIC users and contractors, scheduled for this fall, is in part intended to address capability and implementation issues for NCIC 2000. We believe that this will be a good forum to discuss and resolve some of the capability and implementation issues we have identified.

EXTENT AND NATURE OF NCIC MISUSE CANNOT BE ASSESSED, BUT INCIDENTS OF MISUSE HAVE OCCURRED

We could not obtain FBI and state assessments of the extent and nature of the misuse of NCIC because the FBI and most SCTAs do not systematically maintain statistics or other information on incidents of misuse. We were, however, able to obtain general information on the extent and nature of NCIC misuse and specific examples of such misuse from the FBI, our review of FBI audits of SCTAs, our visits to SCTAs, and our telephone survey of SCTAs.

FBI and Most SCTAs Do Not Maintain Statistics or Adequate Information on Misuse Incidents

FBI officials could not provide us with a statistical assessment of the extent and nature of NCIC misuse because they do not maintain statistics or other adequate information on such incidents. Of the 54 SCTA officials we interviewed during our telephone survey, 41 expressed the opinion that misuse in their states was a problem to some or little extent, 12 to no extent, and 1 to a moderate extent.[7] However, many of these officials could not provide any statistical or other evidence to support their assessments. Specifically, only 22 SCTAs maintained statistics on misuse incidents, while 32 SCTAs did not maintain any statistics. Furthermore, 21 of 54 SCTA officials stated that their systems' controls were moderately effective in detecting misuse, while 8 stated that they were effective to some or little extent, and 1 to no extent. Thus, these self-assessments may underestimate the extent of the misuse problem.

According to the FBI and 21 SCTA officials, they do not maintain statistics on misuse incidents because there is no policy requirement to report and track incidents of misuse, or they did not believe it was necessary to collect such information, given the small number of misuse incidents that occur within their jurisdictions. Some SCTA officials are generally aware of significant misuse incidents in their states and maintain information about these incidents. For example, the Texas and New Mexico SCTAs maintain information about significant misuse incidents that are reported by local user agencies.

Examples Show NCIC Misused Intentionally and Unintentionally

Even though we could not obtain an overall assessment of the extent and nature of NCIC misuse, we did obtain some general information about the extent and nature of such misuse from the FBI, SCTAs, our visits to user agencies, and our review of FBI audits of SCTAs. Specifically, the FBI reported that its Office

---

[7]Our five-level survey scale ranged from "no extent" to "very great extent."

of Professional Responsibility had investigated a total of eight incidents of NCIC misuse by FBI personnel during 1990 through 1992. Furthermore, our telephone survey showed that 12 SCTAs that maintained statistics on misuse incidents detected 159 such incidents in fiscal year 1992. It should be noted, however, that 100 of these incidents were detected by a single SCTA. In addition, 17 SCTAs that did not maintain statistics, still informed us that they were aware of 94 misuse incidents in their states. The misuse incidents were detected primarily through FBI or SCTA audits, tips from informants, complaints from victims of misuse, reviews of NCIC audit trail information, or by other means. Finally, our review of FBI audits of SCTAs showed that misuse incidents were detected in 58 law enforcement agencies in 30 states.

The FBI and SCTAs were able to provide some information on 62 of the examples of NCIC misuse. We found that 56 examples we obtained involved what we characterized as intentional and 6 involved unintentional misuse of NCIC. Furthermore, all of them involved insiders and none involved outside hackers. It should be noted that these examples were provided to us verbally and mostly without supporting evidence. Consequently, we could not verify the accuracy of these examples. Furthermore, the outcomes of five cases are still pending and the outcomes of eight cases are unknown. Finally, two examples involved an unknown number of additional misuse incidents. (See appendix II for all the examples of misuse we obtained.)

Intentional Misuse of NCIC

Fifty-six examples of misuse we obtained involved the intentional misuse of NCIC. Of these, 40 examples involved insiders using NCIC information either for personal purposes, such as determining whether friends, neighbors, or relatives had criminal records or political purposes, such as inquiring about the backgrounds of political opponents. In certain cases, the misuse of NCIC information jeopardized the safety of citizens and potentially of law enforcement personnel. In one extreme example, a former law enforcement officer in Arizona obtained NCIC information from three other officers and used it to track down his girlfriend and murder her. After an investigation, the three officers who provided the information were prosecuted, convicted, and sentenced to prison under Arizona state law. In another example, a terminal operator in Pennsylvania conducted background searches for her boyfriend, who was a drug dealer. He asked her to check the criminal history records of new clients to determine if they were undercover drug agents. She continued her activity until supervisors detected an unusual number of inquiries from her terminal.

An additional 16 incidents of intentional misuse involved insiders obtaining NCIC information and disclosing it to

unauthorized persons, such as private investigators, in exchange for money or other rewards. In two such incidents, private investigators obtained and used NCIC information to conduct background investigations on individuals seeking employment with nationally known firms. In one example, a law enforcement officer in Alabama used NCIC to conduct background investigations for a national transportation firm. In another example, a private investigator in Texas obtained NCIC information from the chief of a small suburban police department to conduct background investigations for a restaurant chain and a computer firm. It is not known if these firms were aware that the use of NCIC in these investigations was a violation of NCIC policy.

Unintentional Misuse of NCIC

The incidents of unintentional misuse involved the use of NCIC by law enforcement agencies for noncriminal justice purposes. These purposes included conducting background searches on individuals applying for noncriminal justice employment such as shopping mall and school security guards, or on individuals applying for firearm permits, and liquor and taxi licenses. In addition to 6 of the 62 misuse examples we obtained, incidents of unintentional misuse occurred in 58 user agencies in 30 states and, according to some SCTA officials, may have resulted from misunderstanding the policy on use of NCIC for employment background investigations. The FBI has attempted to address the misuse problem by recommending training and clarification of NCIC policies. Some agencies have attempted to implement such recommendations. For example, the South Carolina SCTA held a special training session for Alcohol and Beverage Commission agents who were requesting background searches for liquor license applicants and sent a letter to all NCIC users in the state reminding them of the proper uses of the system.

MOST INDIVIDUALS MISUSING NCIC WERE NOT CRIMINALLY PROSECUTED

The examples we obtained showed that most of the individuals misusing NCIC were not criminally prosecuted. Specifically, individuals in only seven of our misuse examples were criminally prosecuted. FBI and SCTA officials cited the lack of federal and state criminal statutes imposing penalties specifically for misusing NCIC as the reason prosecutors were reluctant to prosecute such incidents. For example, upon her discovery the terminal operator in the Pennsylvania incident was terminated from employment but was not prosecuted because of the lack of a specific statutory penalty for misusing NCIC. In another example, a dispatcher for a police department in Rhode Island conducted background searches on her fiance's political opponents. The dispatcher was terminated from employment but was not prosecuted because of the lack of an applicable statute.

Furthermore, even though some federal criminal statutes, such as theft of government property, computer fraud, and bribery have been used as the basis for NCIC misuse cases, such as those in Florida and New Jersey, FBI and SCTA officials and federal prosecutors regard these statutes as difficult to use in the prosecution of such misuse because they do not address NCIC specifically. For example, the local U.S. Attorney's Office investigating the misuse incident in Texas (discussed on page 17) declined to prosecute the police chief and the private investigator involved, citing the lack of a directly applicable federal statute. As part of a plea bargain, the investigator and the police chief each agreed to perform 160 hours of community service. The investigator had already been convicted for selling credit bureau information and had received a deferred sentence and a fine. In a letter to the FBI explaining his decision not to prosecute, the U.S. Attorney outlined the ineffectiveness of existing federal and state statutes in deterring NCIC misuse and called for a specific federal statute for such misuse. In response, the FBI's Legal Counsel Division pointed out that each of the existing statutes has technical defects that would discourage prosecutors, and indicated that it may be prudent to enact such legislation to protect NCIC from unauthorized access and use. The NCIC APB has also recommended enactment of federal legislation making NCIC misuse a specific federal crime.

When asked about solutions to the misuse problem, FBI officials in charge of NCIC and about half of the SCTA officials interviewed in our telephone survey expressed their support for federal legislation imposing penalties on those misusing NCIC. According to some SCTA officials, federal legislation would serve as a deterrent to potential misuse of NCIC. For example, according to a Pennsylvania SCTA official, if the terminal operator who helped her boyfriend had been arrested and prosecuted, her example could have served as a deterrent to others contemplating misusing NCIC. Federal legislation also would encourage prosecutors to prosecute individuals involved in such misuse. For example, according to a New York SCTA official, federal legislation would not only encourage U.S. Attorneys to prosecute misuse incidents but also would augment existing state statutes and serve as a strong deterrent to those contemplating misusing NCIC.

Currently, most user agencies and individuals who violate NCIC policies or misuse the system receive administrative sanctions. Specifically, local user agencies violating NCIC policy can have their access to the system temporarily revoked either by the FBI or SCTAs until the violations are corrected. The FBI has revoked the access of only one local user agency since NCIC became operational. SCTAs have also revoked the access of local user agencies to NCIC (see appendix II for examples). With regard to individuals who misuse NCIC, the NCIC Security Policy requires only that each criminal justice agency have appropriate written

standards for discipline of such violators. Individuals who misuse NCIC have usually been either reprimanded by their agency, denied further access to the system, suspended without pay, or terminated from employment. Specifically, in 35 of our misuse examples, individuals were either reprimanded, terminated from employment, or received a variety of suspensions. There was no action taken in 7 examples, while the outcome was unknown or pending in 13 examples.

CONCLUSIONS AND RECOMMENDATIONS

We found that the NCIC system, being a network of coordinated state systems, is vulnerable to misuse because of various factors that increase its inherent risk and because the controls of some state systems accessing NCIC are not adequate or are not being used effectively to deter and detect misuse. In an attempt to address NCIC's vulnerability, the FBI will implement new security measures for the Central Segment and its own workstations of the upgraded NCIC 2000 system. The implementation of NCIC 2000's security features is a positive development in the effort to address the system's vulnerability to misuse. However, the potential limitations and limited implementation of these features could diminish their effectiveness. Most significantly, the states will not be required to implement the security features. Consequently, the system will remain vulnerable to misuse.

Furthermore, SCTA officials identified certain barriers that may affect the overall implementation of NCIC 2000. First, funding shortages may prevent local user agencies from attaining the full potential of the new system and its security features. Second, hardware and software compatibility problems may affect timely implementation. Third, staff shortages at the FBI's Criminal Justice Information Systems Division will affect training and other technical assistance to the states. However, we believe that the NCIC user and contractor conference is a good forum to discuss and potentially resolve some of the capability and implementation issues we have identified.

We could not obtain assessments of the extent and nature of NCIC misuse because (1) the FBI and most SCTAs does not systematically maintain statistics or other information on misuse and (2) many state officials could not provide evidence to support their general assessments of misuse. However, we did obtain sufficient examples of misuse to indicate that such misuse occurred throughout the NCIC system and that misuse was both intentional and unintentional. Furthermore, all the reported misuse incidents involved insiders, while none involved outside hackers.

We believe that on the basis of our findings, misuse of NCIC is a problem that needs to be addressed more effectively. We emphasize that any measure aimed at making such misuse less

likely can be effective only if implemented in a coordinated manner with other measures. For example, if NCIC 2000's security features are implemented and consequently detect more incidents of misuse, directly applicable legislation will be needed to ensure that the individuals responsible are prosecuted. On the other hand, while legislation will help prosecute some detected violators, without the additional security measures, some misuse may go undetected.

We recommend that Congress enact legislation with strong criminal sanctions specifically directed at the misuse of NCIC. Such legislation should be aimed at (1) deterring individuals contemplating misusing NCIC and (2) facilitating and encouraging the prosecution of individuals who have misused NCIC.

In view of our findings and the NCIC 2000 implementation, we also recommend that the FBI Director and the NCIC APB re-evaluate the security specifications set forth in the NCIC Security Policy, particularly in the area of accountability. Recognizing the potential cost and implementation concerns involved, at a minimum, the FBI and the APB should amend the Security Policy to endorse and encourage state and local user agencies' enhancing their security features, such as increasing user accountability through identification, authentication, and audit, to meet the C2 security rating.

AGENCY COMMENTS

Justice Department and FBI officials reviewed a draft of our testimony and agreed with our findings, conclusions, and recommendations. According to these officials, federal legislation will be very helpful in deterring insiders from misusing NCIC.

- - - - -

This concludes my prepared statement. In closing, I would like to acknowledge the cooperation of FBI and state and local law enforcement agency officials during the course of our review. I will be happy to answer any questions you may have.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our objectives were to (1) determine whether the FBI and user agencies have adequate controls to ensure that access to NCIC is for authorized purposes and deter and detect misuse of NCIC information and (2) obtain the FBI's and states' assessments of any NCIC misuse and examples of such misuse.

To fulfill the Subcommittee's request, we (1) interviewed FBI officials responsible for NCIC; (2) reviewed NCIC and state and local agency security policies and other relevant documentation; and (3) visited state and local law enforcement agencies who use NCIC in California, Nevada, and Texas and interviewed relevant agency officials.

We judgmentally[8] selected and visited the California Department of Justice and the Sacramento County Sheriff's Department, both in Sacramento, California; the Los Angeles County Sheriff's Department in Los Angeles, California; the Nevada Department of Motor Vehicles and Public Safety, and the Carson City Sheriff's Department, both in Carson City, Nevada; the Douglas County Sheriff's Department in Minden, Nevada; and the Texas Department of Public Safety, Austin Police Department, and Travis County Sheriff's Department, all in Austin, Texas. We did this work to obtain a description of the system and its controls and to learn how it operates. We also observed the physical security of NCIC terminals at the agencies we visited and the controls for accessing and disseminating information from the system.

In addition, we administered a telephone survey to all 54 SCTAs who oversee local user agencies in the United States and Canada to obtain information on (1) state and local agency access to NCIC, (2) access and dissemination controls, and (3) the extent of NCIC misuse and obtain examples of such misuse. We administered our survey between January 25 and February 18, 1993. While we did not verify the accuracy of the information provided, or its relevancy to NCIC, our survey instrument specifically solicited information about NCIC. During the interviews, we reiterated to the SCTA officials that our questions were specifically addressing NCIC.

It should be noted that the misuse examples we obtained were provided to us verbally and mostly without supporting evidence. Consequently, we could not verify the accuracy of these examples. Furthermore, the outcomes of five cases are still pending and the outcomes of eight cases are unknown. We characterized as

---

[8]We used agency size and geographic location as the criteria for selecting our judgmental sample.

intentional those examples which involved the use of NCIC for personal purposes, for profit, and for political gain. We characterized as unintentional those examples which involved the use of NCIC to conduct background investigations for noncriminal justice employment, or licensing purposes because of the apparent misinterpretation of policy prohibiting the use of NCIC for such purposes.

To obtain assessments of NCIC by computer security experts, we reviewed an NCIC risk analysis prepared by MITRE Corporation for the FBI in 1989; a report by Computer Professionals for Social Responsibility prepared for the Subcommittee on Civil and Constitutional Rights, House Judiciary Committee, in 1989; and a report by SRI International prepared for the FBI in 1990. We also interviewed the author of the SRI report.

To determine NCIC's inherent risk, we used the criteria contained in a GAO policy guide titled Assessing Compliance With Applicable Laws and Regulations (GAO/OP-4.1.2, Dec. 1989). This guide supplements the Yellow Book standards on internal controls.

We did our work between September 1992 and July 1993. We did not test the controls that are discussed in this report. Except as noted above, our work was conducted in accordance with generally accepted government auditing standards.

EXAMPLES OF NCIC MISUSE

As part of our review of NCIC, we obtained 62 examples involving misuse of the system. Specifically, 33 of these examples involved the misuse of NCIC for personal purposes, 16 for profit, and 7 for political gain. Six examples involved the misuse of the system because of an apparent misunderstanding of NCIC policy.

We obtained the misuse examples from (1) the SCTAs we visited in California, Nevada, and Texas; (2) the nationwide telephone survey of SCTAs; and (3) the FBI, including its Office of Professional Responsibility. The examples we obtained are grouped by source. It should be noted that these examples were provided to us verbally and mostly without supporting evidence. Therefore, we could not verify the accuracy of these examples. Furthermore, the outcomes of five cases are still pending and the outcomes of eight cases are unknown.

SCTAs VISITED

California

The California Department of Justice received a complaint from a person who suspected his employer of obtaining a copy of his criminal record from the NCIC's III file. A search of the state system's audit trail showed that the record had been accessed by a law enforcement agency in the eastern United States. Apparently, the employer had hired a private investigator, located in the eastern United States, to conduct background searches on prospective employees. The complainant's criminal history record was allegedly sold to the private investigator by an officer in a law enforcement agency. The employer then used the information to terminate the complainant from employment. As a result of an investigation, the private investigator and the officer disclosing the information will be prosecuted.

Nevada

A detective in the Las Vegas Metropolitan Police Department obtained NCIC information from an unsuspecting computer terminal operator, under the false pretense of legitimate police activity, and sold this information to a private investigator. The local U.S. Attorney declined to prosecute the case because of the lack of an applicable statute.

A tribal police agency on an Indian reservation accessed and released NCIC information to individuals connected to tribal elders. The SCTA revoked the agency's access to NCIC with no further action.

Texas

The city manager of a small town conducted NCIC inquiries on a political opponent using a terminal operator. The manager threatened the operator with loss of employment if she did not cooperate. The operator conducted the inquiries but also alerted the local police chief of her activities. In turn, the chief warned the manager about the unauthorized NCIC inquiries and fired the terminal operator for violating NCIC policy. In the meantime, the political opponent filed an official misconduct complaint against the manager, who was then arrested. In apparent retaliation, the manager fired the police chief before being arrested. The chief is considering legal action against the city to gain reinstatement. The city manager is being prosecuted under the state's official misconduct statute. However, the activities related to NCIC are not being prosecuted because of the lack of an applicable statute.

A computer terminal operator in a district attorney's office accessed and obtained NCIC information and disclosed it to her boyfriend. He, in turn, sold this information to private investigators. After an investigation, the operator was terminated from employment.

A sheriff and some of his deputies conducted NCIC inquiries on election challengers and found that one had been arrested for a weapons violation in 1968. This information was made public to discredit the challenger. A terminal operator who alerted the Texas Department of Public Safety of this misuse was fired by the sheriff. Other operators were threatened with similar action. A challenger won the election for sheriff, and no further action was taken.

A terminal operator in a sheriff's office accessed NCIC using fictitious identifiers and used the information he obtained for unauthorized purposes. An ensuing investigation could not conclusively determine the nature of these purposes. The operator received administrative sanctions.

TELEPHONE SURVEY OF SCTAs

Alabama

A law enforcement officer with authorized access to NCIC conducted employment background searches for a nationally known transportation firm in exchange for money. This incident was detected through the review of audit trail information. The officer was terminated from employment but was not prosecuted because the state attorney declined to prosecute the case.

Two law enforcement agencies conducted background searches using the III file for Alcoholic Beverage Control Board liquor license applicants. The outcome of this case is unknown.

A local sheriff's department conducted employment background searches on the III file for the state department of human resources. The outcome of this case is unknown.

Arizona

A former law enforcement officer used information obtained from three individuals in different law enforcement agencies to track down his estranged girlfriend and murder her. After an investigation, the printouts provided by the three individuals were discovered, and the individuals were identified, prosecuted, and convicted.

Arkansas

An ongoing investigation involves a terminal operator who allegedly sold NCIC information to an employer who wanted background information on a prospective employee. The case is pending.

Colorado

A private investigator paid several city employees to conduct NCIC record searches. During the service of a search warrant at the investigator's office in an unrelated fraud matter, state investigators discovered records indicating that payments had been made for NCIC records and notified the Colorado Bureau of Investigation. The ensuing inquiry, with the cooperation of the district attorney, resulted in the indictment of several individuals. Their state trials are pending. However, the local U.S. Attorney concluded that there was no violation of federal law in this case and declined to prosecute.

Connecticut

A state trooper provided a private investigator with information on individuals with NCIC records in exchange for money. The trooper was discovered by chance when the internal affairs department of the state police investigated the private investigator on an unrelated matter. The investigator maintained records listing the information provided, the dollar amounts involved, and his source (the state trooper). The state trooper was dismissed from employment.

Florida

About 2 years ago, a police chief's deputy accessed and obtained III file information and sold it to private investigators. The deputy has been indicted under Florida law for 100 counts of misuse. The case will be tried sometime this year.

A law enforcement agency conducted background investigations using the III file for taxi driver permits. The outcome of this case is unknown.

A police chief in a small rural town conducted background searches on prospective tenants in an apartment complex using the III file. The outcome of this case is unknown.

Iowa

Twelve cases of misuse have been reported to the SCTA during the past 2 years. These cases involved terminal operators conducting background searches on friends and relatives to determine if they had criminal records. None of these incidents involved the disclosure of information for money. The individuals involved received administrative sanctions.

Maine

A police officer conducted a background check on one of his wife's employees using the III file. The employee had a criminal record and was terminated from her position for not disclosing it. The officer conducted the check under the false pretense of a criminal investigation, with the full knowledge of his supervising sergeant. The terminated employee filed a complaint and the incident was investigated by the state police. After the investigation, the police officer and the sergeant were suspended for 2 days without pay.

A State Police officer disclosed the III file record of a drug dealer to this person. This incident was detected by an undercover agent, who was investigating a case involving the drug dealer. The state police requested that the FBI investigate the incident. However, since the incident did not involve money, the FBI declined to investigate. After a state investigation, the officer was demoted from major to lieutenant for misuse of NCIC.

Maryland

Several state police personnel checked the records of friends and relatives and provided information to these individuals about their records. The outcomes of these cases are unknown.

Several personnel from a local user agency checked the records of friends and relatives for these individuals. Some of the friends and relatives sold NCIC information to private investigators. The outcomes of these cases are unknown.

Montana

A law enforcement agency conducted criminal history searches on volunteers for the Big Brother, Big Sister program. These inquiries were technically violations of NCIC policy on background searches, but, according to an SCTA official, were apparently based on a misinterpretation of this policy. The case is still pending.

A law enforcement agency conducted criminal history searches on individuals residing in a privately owned and operated halfway house for the state corrections system. These searches were technically violations of NCIC policy, but, according to an SCTA official, were based on the lack of specific guidance to address such a unique situation. According to this official, the officers involved thought that they were simply following their agreement with the corrections system. The case is still pending.

Nebraska

According to a SCTA official, numerous incidents involved criminal justice personnel who did not understand the proper use of NCIC and, thus, technically violated certain policies, particularly by conducting employment background searches. The outcomes of these cases are unknown.

New York

An insider from a law enforcement agency disclosed criminal history information to be used for employment background searches. A grand jury issued an indictment, but the insider was acquitted.

An insider from a law enforcement agency disclosed criminal history information to a local politician to be used against opponents during an election campaign. The insider received administrative sanctions.

North Carolina

A dispatcher accessed the criminal history record of her deceased husband seeking to erase it. However, her terminal was not authorized to erase the record. The dispatcher's activity was

discovered during a state audit, and her operator certification was put on probation.

Ohio

An ongoing case may eventually involve law enforcement officials in other states and will be presented to a grand jury soon. The Ohio State Patrol received a "tip" that a detective used his position to obtain NCIC criminal history record information. He then sold this information to a private firm. This firm conducted employment background searches for Ohio-based companies. At least five other police officers in Ohio may be involved in this case; the detective is implicating his accomplices. In the meantime, the firm that hired the detective has moved to another state. Ohio is trying to prosecute this case under the Racketeer Influenced and Corrupt Organizations statute by charging the alleged criminals with grand theft of computer information.

Pennsylvania

A terminal operator in a user agency, involved in an election campaign, accessed and disclosed criminal history information on a political opponent. The operator was terminated from employment.

A police officer accessed and widely disseminated a fellow officer's criminal history record in order to discredit him. The officer was terminated from employment, settled a civil suit for $25,000, and was not prosecuted.

A computer terminal operator conducted background searches for her boyfriend, who was a drug dealer. He asked her to check the criminal history records of new clients to determine if they were undercover drug agents. Her activities were discovered when supervisors at the agency detected an unusual amount of inquiries from her terminal. Upon her discovery, the operator was terminated from employment but was not prosecuted because of the lack of an applicable statute.

Rhode Island

The weekly review of audit trail information discovered that a police department was conducting III file searches early in the morning using NCIC purpose code "J", which is used for criminal justice employment investigations. An investigation found that the unusual activity involved a dispatcher engaged to a local politician. This individual conducted background searches on her fiance's political opponents. The dispatcher was terminated from

employment but was not prosecuted because of the lack of an applicable statute.

A state trooper conducted III file searches for his attorney who was defending the trooper against misconduct complaints filed by a private citizen. The trooper was investigated by a police panel of three peers and found "not guilty."

South Carolina

An employment firm obtained III file information from a law enforcement agency in Georgia. However, when this activity was discovered in Georgia, the firm began using an agency in South Carolina. This activity was also discovered, and the South Carolina SCTA revoked the agency's NCIC access.

A law enforcement agency conducted background searches on local politicians who were members of the city council. When a victim complained, this activity was discovered and administrative sanctions were imposed on those misusing the system. The SCTA revoked the agency's NCIC access, and an individual was terminated from employment.

Tennessee

A mayor illegally fired the police chief and the city administrator of a small town and appointed a new chief. In a related action, the mayor ordered III file searches on the administrator in order to discredit him. The police chief and the administrator filed suit against the city and won reinstatement to their positions. The mayor's actions were voided, and her powers were curtailed by the city council. No further action was taken.

Virginia

During an election campaign, a sheriff released the criminal history record of an inmate in county jail. This inmate had written several letters to the local newspaper complaining about conditions at the jail and sought to embarrass the Sheriff during the campaign. In turn, the sheriff sought to downplay these charges and discredit the inmate, who already had an extensive criminal record, by releasing this information. The sheriff was charged with improperly releasing criminal history information under a Virginia statute. He was convicted on this misdemeanor charge and received a suspended sentence.

A state employee released criminal history information to a private investigator and was charged under the federal mail fraud statute. These charges were later dismissed because it was

determined that the fraud statute was not appropriate for this case. The employee was terminated from employment. However, this individual filed a complaint with the state's grievance panel and won reinstatement through a binding ruling.

A chief of police released criminal history information to an unauthorized person. The state prosecutor reviewed the case and declined to prosecute. However, administrative sanctions were imposed on the chief whose access to NCIC was revoked for 60 days.

Washington

A police officer conducted criminal history searches from a court terminal and harassed a victim using this information. The officer used the court terminal instead of his own to disguise his identity. The outcome of this case is unknown.

A police officer disclosed criminal history information to a private investigator. This case is currently under investigation.

FBI AND FBI OFFICE OF PROFESSIONAL RESPONSIBILITY

A police chief of a small suburban police department provided criminal history information on individuals to a private investigator for nominal awards. The private investigator sold the information to nationally known firms, including a computer firm and a restaurant chain, which used the information to conduct preemployment background investigations. The FBI was alerted to the misuse by a disgruntled employee in the police department and investigated the case using audit trail information. On the basis of the investigation, a grand jury served subpoenas against the police chief and the private investigator. The investigator had already been convicted for selling credit bureau information and had received a deferred sentence and a fine. The assistant U.S. Attorney in charge of the case assessed the possibility of indicting the two individuals, but settled for a preindictment plea bargain, citing the lack of applicable federal statutes for misusing NCIC. Under a pretrial diversion program, the police chief and the private investigator agreed to perform 160 hours of community service.

An FBI special agent accessed and disclosed FBI records in NCIC for unauthorized purposes. The agent was censured, suspended for 10 days, and placed on probation.

A support employee disclosed NCIC information to an individual she was dating. The employee received a letter of censure.

A support employee disclosed information from NCIC's license plate file to an acquaintance. This person was being investigated by the FBI and was aware of the investigation, most likely through the information disclosed by the FBI employee. The support employee resigned from the FBI during the investigation and before the case could be referred for administrative adjudication.

A support employee disclosed NCIC information to a friend engaged in the repossession of automobiles. The employee advised the friend on whether the automobiles were stolen. The support employee resigned from the FBI before the case could be referred for administrative adjudication.

A support employee disclosed NCIC information to her father, who was serving a 10-year prison sentence for drug trafficking. An FBI investigation found that three additional persons received the NCIC information as a result of the employee's disclosures. The support employee was censured, suspended without pay for 14 days, and placed on probation for 1 year.

A support employee allegedly disclosed information from NCIC's III and driver's license files to a pawn shop, in exchange for interest-free loans. The employee denied any impropriety but resigned during the investigation and before the case could be referred for administrative adjudication.

An FBI special agent disclosed NCIC information related to a homicide case to a police department. An FBI investigation found that the agent was not acting in his official capacity when disclosing the information. The agent received a letter of censure.

A former FBI employee requested that a support employee provide NCIC information about the father of her child. The information was apparently needed to obtain public assistance. The support employee was orally reprimanded for providing the information.

(184418)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1000
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066.

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100