

FEATURE ARTICLES



Cybercrime and the Judicial System: Assessing the Needs of North Carolina State Prosecutors' Offices

[This article was written by Douglas L. Yearwood, Director of the North Carolina Criminal Justice Analysis Center and Richard Hayes, Senior Research Analyst. The article is based on research funded by the Bureau of Justice Statistics through its State Justice Statistics Program.]

The incidence of cybercrime has increased steadily during the last decade, and high profile media cases, Internet scams, and hoaxes have brought this issue to the attention of politicians, policymakers, other members of the criminal justice system, and the general public. Unfortunately many law enforcement officials and judicial personnel have only recently begun to strengthen their investigative and prosecutorial efforts in this area. Some have created trainings, investigative manuals, and technological tools in response to their growing concern. Some larger urban jurisdictions have formed highly specialized cybercrime units, while many smaller suburban and rural jurisdictions are giving these investigative and prosecutorial units more serious consideration than they did even three or four years ago.

A study recently conducted by the North Carolina Criminal Justice Analysis Center, which is the state's Statistical Analysis Center (SAC), sought to examine cybercrime in North Carolina from the judicial perspective, specifically, the district attorney's point of view. The primary purpose of the study was to ascertain the specific needs of the district attorneys relative to cybercrime. The research sought to answer program

and policy-relevant questions such as: How prepared are the state's prosecutors for handling these cases? What types of equipment, training, and personnel needs do these offices have? What do the district attorneys see down the road regarding the future of these crimes in North Carolina? The study also sought to obtain a better indication of the nature and extent of cybercrime in North Carolina, i.e., we sought to capture case-based statistics in this area. It is anticipated that this explorato-

ry study will be a first step for addressing the issue of cybercrime in North Carolina.

Survey Instrument

A four-part, 26-item questionnaire was designed in an effort to define and specifically pinpoint both the strengths and weaknesses of the district attorneys' offices in the area of cybercrime. Part one of this needs assessment

(See **CYBERCRIME**, p. 5)

Developing a NIBRS-Compatible Homicide Database: Part 2

[This report, written by Lisa Walbolt, a JRSA Project Manager, is a continuation of Developing a NIBRS-Compatible Homicide Database: A Multistate Pilot Test, printed in the April 2003 edition of The JRSA Forum. This is the second of two parts.]

JRSA recently completed a national study on the feasibility of using the National Incident-Based Reporting System (NIBRS) in the development of a homicide information system. Funded by the Bureau of Justice Statistics, the study involved data collection and analysis in six states: two with relatively extensive involvement with NIBRS (Massachusetts and Utah), two states that are not NIBRS-compliant but have well-developed incident-based data collection established in some jurisdictions (Illinois and Michigan), and two states with little or no

experience with NIBRS (Hawaii and New Mexico). The first installment of this report focused on the background, purpose, and methodology of the project. This part focuses on the research findings and conclusions.

Analysis of the Homicide Data File

Availability of NIBRS Data Elements

The first step in determining whether the development of a NIBRS homicide database is feasible is to look at whether NIBRS data elements are available, that is, whether they are being reported and are accessible. Since it is possible for a data element in NIBRS to be correctly reported as "unknown," NIBRS data in this study are considered missing only if no response was provided. For example,

(See **HOMICIDE DATABASE**, p. 9)

JRSA ACTIVITIES 

JRSA Project Updates

Juvenile Justice Evaluation Center

Exemplary Juvenile Justice Evaluations and Programs

Over the past several months, the Juvenile Justice Evaluation Center (JJEC) has begun modifying the Juvenile Justice Evaluation Program Areas page on the JJEC Web site. JJEC developed a rigorous coding scheme to identify evaluations with sound designs and programs with demonstrated efficacy. Updating of the first program area, Aftercare, was completed in April. Visit www.jrsa.org/jjec/programs for more information.

Publications

“Evaluation Strategies for State Juvenile Justice Programs: Case Studies From Washington and Pennsylvania” describes two states’ approaches to evaluating juvenile justice programs. The report was posted on the JJEC Web site in February and can be downloaded at <http://www.jrsa.org/jjec/about/wa-pa-2003>.

In June, JJEC published its sixth briefing in the Program Evaluation Briefing Series. The briefing, “Evaluability Assessment: Examining the Readiness of a Program for Evaluation” discusses the role that evaluability assessment can play in helping to prepare for an evaluation. It describes how to conduct an evaluability assessment and includes sample assessment questions.

Trainings/Conferences

Again this year JJEC has been invited to present at Coalition for Juvenile Justice conferences. In July, JJEC is conducting a session entitled, “Evaluation Issues Regarding Mental Health Programming in the Juvenile Justice System.” At an August conference, JJEC will present on the topic of disproportionate minority contact and evaluation.

The work of three SACs, Illinois, Indiana, and Wyoming, will be highlighted during a panel presentation at the 2003 National Institute of Justice Research and Evaluation Conference. The presentation, “State Evaluation Partnerships to Address Gender Specific Programming,” will report on the 2002 Juvenile Justice Evaluation Partnership Projects conducted by the SACs.

In an effort to provide more people with introductory training on evaluation in a cost-effective manner, JJEC converted its training session, “Evaluation: A Tool for Program Improvement” to an electronic tutorial. A draft of the tutorial was tested in April. The tutorial should be ready for use this month.

Improving Crime Data

The Improving Crime Data project, formerly known as the Great Cities’ Universities project, has begun the phase of convening groups of practitioners to determine the needs and problems in implementing data-driven policy and programming in criminal justice agencies. JRSA staff met with Uniform Crime Reporting specialists and crime analysts in June to discuss the project’s goal of establishing statistical indicators to help analyze and predict crime patterns for policymakers. Staff attended the confer-

ences of the Northeast Regional Association of State Uniform Crime Reporting Programs (ASUCRP) in Portsmouth, NH, and the Massachusetts Crime Analysts in Hyannis, MA, and discussed with participants how a system of data shared and integrated among agencies could best be used for problem analysis and projection of future crime patterns. These discussions will help shape the discussion in focus groups to be held in July with policy and program practitioners in Illinois, Oklahoma, and Pennsylvania. The findings of those focus groups will be incorporated into a national survey of chiefs of police to provide a comprehensive overview of current practice in data-driven policymaking and programming.

JAIBG Program Technical Support Center Prepares for Changes

Congressional changes to the Juvenile Accountability Incentive Block Grants (JAIBG) Program will soon result in corresponding changes to JRSA’s JAIBG Technical Support Center. The program is now to be called the Juvenile Accountability Block Grants (JABG) Program. The formula used to calculate allocation amounts to local governments will incorporate changes specified by Congress, including the use of juvenile expenditure data at the local level. Since these data are not currently accessible, the formula will instead direct funding toward localities most responsible for juvenile justice services. To achieve this goal, the formula, which currently calculates allocations based on two thirds of the proportion of justice expenditures and one third of the proportion of Part 1 violent crimes, will calculate allocations based on three fourths of the proportion of justice expenditures and one fourth of the proportion of crime. In addition, the justice expenditures, which did include police, judicial/legal, and corrections expenditures, will include only judicial/legal and corrections expenditures.

The program will also change, introducing additional purpose areas in which to focus funding. A competitive set-aside for

INSIDE	
Feature Articles	
Cybercrime and the Judicial System: Assessing the Needs of North Carolina State Prosecutors’ Offices . . .	1
Developing a NIBRS-Compatible Homicide Database: Part 2	1
JRSA Activities	
JRSA Project Updates	2
JRSA Hosts Brown Bag Lectures	4
JRSA Welcomes New SAC Directors . . .	4
Weed & Seed Data Center Adds New Staff	4
Announcements	
New Book Describes Effective Programs for At-Risk Youth	10
CSUN Offers Crime and Intelligence Analysis Certificate Program	10
Book Review	
Reentry and Criminal Justice	11

tribes will be implemented. The minimum allocation amount will be increased from \$5,000 to \$10,000. Localities currently receiving under \$10,000 will most likely not receive a direct award under the new program. Additional reporting requirements will be in place for both state and local grantees.

The changes will go into effect in 2004 and will not affect 2003 allocations. Information on the planned changes will be available on both the JRSA JAIBG Program Technical Support Center Web site (<http://www.jrsa.org/jaibg>) and OJJDP's JAIBG Web site (<http://www.ojjdp.ncjrs.org/jaibg>) beginning at the start of the new fiscal year in October.

Weed & Seed Data Center Introduces New Look

JRSA attended the Executive Office for Weed and Seed's (EOWS) 2003 National Conference in Albuquerque, NM, May 25-28. The conference brought together representatives of local Weed and Seed sites, EOWS staff, representatives from U.S. Attorneys' Offices, researchers, consultants, and service providers from across the nation.

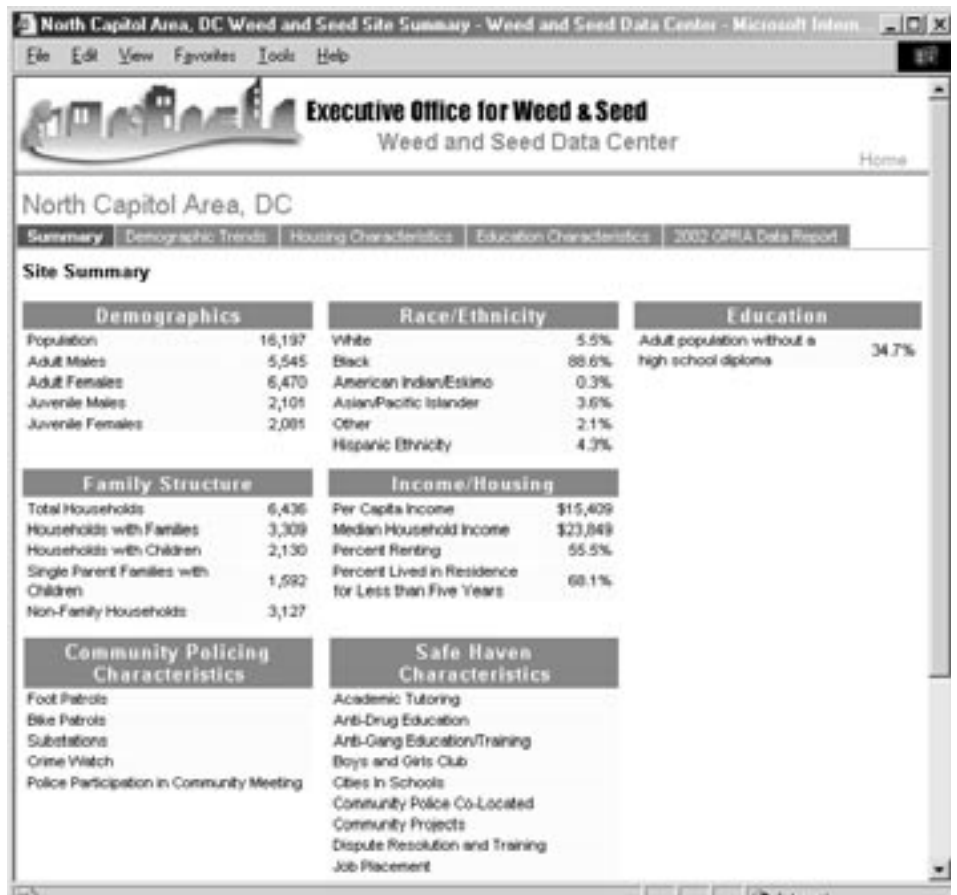
Weed and Seed conferees visited the JRSA booth to preview the latest version of the Weed and Seed Data Center before its official Internet launching. Now available for public viewing at <http://www.weedandseeddatacenter.org>, the Data Center allows Weed and Seed participants to review their reported program data and to identify and learn from similar efforts throughout the nation.

Site representatives took turns viewing maps of their sites, with community resources highlighted, and looked at selected 2000 Census Data and 2002 estimates for the Weed and Seed area. Access to these data proved particularly helpful to a handful of site representatives who had grant applications due that week. Because these data include estimates for census tract segments, they can be very difficult to replicate outside of the Weed and Seed Data Center. The data section of the Web site also includes PDF reproductions of grant reports submitted by each site.

(See **PROJECTS**, p. 4)



Home page of a Washington, D.C. Weed and Seed site. Target area boundaries and Safe Havens are clearly delineated.



Weed and Seed page for a Washington, D.C. site showing demographic information and other relevant site characteristics.

(PROJECTS, from p. 3)

Jim Zepp, Director of JRSA's Training and Technical Assistance Center, and Matt Perkins, JRSA's Weed and Seed Project Manager, delivered presentations on "Increasing Effectiveness by Evaluating Your Weed and Seed Strategy" and on "Mobilizing Housing Agencies for Crime Reduction," respectively. Jack O'Connell, Director of the Delaware SAC, and Terry Dunworth, Director of the Justice Policy Institute at The Urban Institute, both of whom are consulting on JRSA's Weed and Seed evaluation project, were also presenters.

Mr. O'Connell is involved in the Weed and Seed Crime Pattern Data Collection effort to collect and analyze pre- and post-implementation crime data for all Weed and Seed sites. The effort attempts to collect site-specific and jurisdiction-wide crime data for locally identified target crimes from the two calendar years prior to program implementation through subsequent years.

Dr. Dunworth discussed a crime mapping and analysis effort aimed at providing in-depth analysis of criminal patterns in and around Weed and Seed sites. Through geographic analysis, JRSA and the Urban Institute can more accurately determine the effectiveness of Weed and Seed programs, including neighborhood and block-level changes, to take into account potential problems from crime displacement.

Incident-Based Reporting Resource Center Adds Sections

JRSA's Incident-Based Reporting Resource Center (IBRRC) continues to expand. The Center now includes 15 sections, with several new sections providing visitors information on using incident-based data in ACCESS and mapping crime data. A calendar of upcoming training and meetings allows agencies to find out about local events. Users can also view the status of the National Incident-Based Reporting System (NIBRS) in the states, and can read descriptions of the projects and programs currently underway.

Several sections provide examples of how incident-based data can be used to answer research questions, including a section that focuses on individual data

elements. This section provides data quality information, examples of how the FBI has used incident-based data, and examples from state publications. Future plans include an updated fact sheet and an improved site map.

JRSA Hosts Brown Bag Lectures

JRSA continued its in-house Brown Bag lecture series in April with presentations over lunch by three speakers. Kim Hunt, Executive Director of the District of Columbia Advisory Commission on Sentencing, reviewed his discussion of a "continuous learning system" from the Fall 2001 issue of *Justice Research and Policy*, applying that model to D.C. sentencing policy development. He then discussed more directly the sensitive political environment faced by the D.C. commission when dealing with both the D.C. government and the U.S. Congress.

Russell Butler, Executive Director of the Maryland Crime Victims Resource Center, supplied a brief summary of the organization's history and functions. He then led a dialogue with staff regarding the needs and politics of the victims community in criminal justice and policy-making. Finally, Greg Kern spoke to JRSA staff on his work in international relief efforts through World Vision, including time he spent in Bosnia and Pakistan. He related the often difficult personal and political challenges faced by relief workers, including frequent killings, and expressed the hope that U.S. relief work would not be substantially affected by recent events.

JRSA regularly invites noted authorities in criminal justice to speak at "brown bag" lunches throughout the year. Future guests will include Jack O'Connell, Director of the Delaware Statistical Analysis Center.

JRSA Welcomes New SAC Directors

New SAC directors have been appointed in Minnesota and Wisconsin. Congratulations go to Nevada, which recently established a SAC and chose a director. A biography of Dick McCorkle, Ph.D., the new director, will be published in the

next issue.

Gail Carlson is the new SAC Director at the Minnesota Statistical Analysis Center, which, by executive order, was moved to the Office of Justice Programs at the Minnesota Department of Public Safety. She has been with the SAC since April 2002, most recently as a research analyst. Ms. Carlson was the project leader for the 2002 Minnesota Crime Survey, which will be released this summer. Previous to her work at the SAC, she was a research analyst at the Minnesota Demographer's Office, where her major duty was to answer the demography helpline, and at the Research and Statistics Office of the Minnesota Department of Economic Security, where she computed employment estimates. Ms. Carlson has spent much of the past three months planning and overseeing the move of the SAC, which included integrating the criminal justice Web site with that of the new agency and updating the criminal justice data. She has a B.A. in psychology, an M.A. in public affairs from the Humphrey Institute of Public Affairs, and an M.S. in applied economics, all from the University of Minnesota.

Dean Ziemke was appointed the new SAC Director in Wisconsin in April. He worked with the Wisconsin Court System for 17 years in policy analysis and statistics and was a director of the statewide Circuit Court Automation Program. Dr. Ziemke also worked with the State Prosecutors' Information Technology (IT) organization and, most recently, with the Wisconsin Executive Branch IT Department, encouraging collaboration and coordination among justice agency IT projects. His goals for the Wisconsin SAC are to expand Incident-Based Reporting (IBR) implementation and research efforts, to improve the Internet infrastructure to make more agency data available interactively, and to work with the State Prosecutors' Office to develop state prosecution statistics. Dr. Ziemke has a Ph.D. in mass communications and an M.A. in journalism.

Weed & Seed Data Center Adds New Staff

Lorena Sobhi joined JRSA in May as an administrative coordinator. She is responsible for providing administrative support

to the Weed and Seed data collection and analysis project. Prior to joining JRSA, Ms. Sobhi worked as a consultant for the Finance and Basic Infrastructure Division of the Inter-American Development Bank (IADB), an international

financial institution created to help accelerate the economic and social development of its member countries in Latin America and the Caribbean. In this position, she provided assistance to project teams in the preparation and pro-

cessing of loan documents, technical cooperation, and project reports. Ms. Sobhi is fluent in Spanish and has experience managing technical assistance and consulting projects at IADB. We are pleased to welcome her to JRSA. 

(CYBERCRIME, from p. 1)

sought to ascertain whether the state's prosecutors' offices had individuals who had either specific training or knowledge related to cybercrime. Questions also dealt with the clarity of the current statutes as they relate to prosecuting and managing cybercrime, and respondents were asked to identify how many cybercrimes their office had prosecuted, including the number internal and external to their prosecutorial districts.

Part two listed numerous types of computer crime and asked respondents to identify the number of cases prosecuted within the last three fiscal years, as well as the disposition of those cases. Part three contained questions about the extent to which the prosecutors' offices were prepared to adequately prosecute cybercrime. Respondents were asked to rate their office in the areas of equipment, training, personnel, and law enforcement coordination. Open-ended questions were included to allow participants to document their specific needs in each of these areas.

The final section of the survey addressed the future of cybercrime and included items on barriers to successful prosecution, the perceived future impact of cybercrime, and the use of investigative grand juries with these types of cases. Respondents were also asked to list any other needs or issues they deemed relevant.

Study Sample

Surveys were mailed to each of the state's 39 district attorneys, with follow-up phone calls being made because of a low return rate. These follow-up phone calls bolstered the return rate by approximately 50% and produced a more even distribution of responses from both rural and urban areas. The higher return also provided a better geographical representation of offices throughout the state.

Results

Questionnaires were completed and returned by 20 prosecutors' offices. This equated to a 51.3% response rate, with responses being obtained from prosecutors representing urban and rural jurisdictions. Responses were received from all three major geographical areas of North Carolina.

Needs Assessment. In response to the questions in part one, eight district attorneys noted that their offices have individuals who currently possess specialized cybercrime knowledge. Of these eight offices, 75% noted that the individuals with cybercrime knowledge had received instruction on the unique search and seizure aspects of cybercrime. Only two prosecutors' offices had staff whom they identified as being specialists in this area; one office had one specialist, while the other had three attorneys who were considered to be specialists. Only one respondent noted that the prosecutor's office had plans to develop a specialized cybercrime unit within the near future.

The majority of the cybercrime cases prosecuted to date are locally occurring events, with both the plaintiff and defendant residing in the prosecutor's home jurisdiction. Fifty-eight percent of the survey participants noted that all of their cybercrime cases fell into this category; the remaining 42% noted that their office had prosecuted at least one case in which one of the parties was located outside of their judicial district. A total of 19 cases were prosecuted in which one of the parties was outside the prosecutor's judicial district.

Thirty-seven percent of the responding prosecutors reported that their offices had prosecuted cybercrimes with at least one out-of-state party, either plaintiff or defendant. Four cases of this type were reported. Out-of-state cases involved parties from Texas, Virginia, and Kentucky. None of the participating

district attorneys' offices had prosecuted any international cases.

Crime Type and Prosecution Frequency.

As part of the needs assessment survey, each district attorney was asked to provide data on the number of cybercrimes filed within their judicial districts from fiscal year 1999/2000 to fiscal year 2001/2002. As Table 1 demonstrates, the most frequently reported type of cybercrime was fraud (86.8%), followed by the use of a computer to lure children (4.7%) and identity theft (4.1%).

Criminal Offense	Number Filed	Percent
Fraud	1,392	86.8
Use of computer to lure children	75	4.7
Identity theft	66	4.1
Data theft	43	2.7
Unauthorized computer access	12	.7
Cyber stalking	10	.6
Pornography	6	.4
Computer sabotage	0	0
External or unauthorized system shutdowns	0	0
Total	1,604	100

It should be noted that only seven prosecutors' offices were able to provide case filing statistics specific to cybercrime cases. The majority of the respondents were unable to provide extracted statistics that disaggregated cybercrime cases from the total number of cases their office had prosecuted during the three-

(See **CYBERCRIME**, p. 6)

(**CYBERCRIME**, from p. 5)

year period. Comments in this portion of the questionnaire included: “No such statistics have been maintained by this office”; “We have no way of pulling these statistics”; and “I do not know the numbers. The majority of what we see in our county is fraud, identity theft and pornography. We have had a handful of ‘use of a computer to lure children’ and a few cyberstalking cases.”

Thus the data presented in Table 1 provide a minimum number of computer crime cases in North Carolina, with some of the information representing an estimate, or best “guesstimate,” on the part of the prosecutors’ offices. Generalizations based upon this information should therefore be approached with caution. It is difficult to ascertain the extent to which this low, or minimum, number of case filings reflects the actual number of true cybercrime cases. It could also be due to other factors, such as a lack of aggressive investigation and prosecution, or a statistical reporting issue in which raw administrative data on these types of cases are not readily available.

Office Adequacy for Prosecuting Cybercrime. The third section of the survey addressed the specific strengths and weaknesses of the prosecutors’ offices on a range of cybercrime issues. Respondents were encouraged to rank their respective offices on a 10-point scale ranging from 1 (totally unprepared or inadequate) to 10 (totally prepared or adequate). Each prosecutor was given the opportunity to rate the agency’s level of preparedness and discuss its specific needs, relative to cybercrime, for the following areas: equipment, personnel, training, law enforcement coordination, and adequacy and utility of the general statutes for prosecuting cybercrime cases.

Equipment. The majority of the prosecutors reported that their offices lacked adequate computer equipment and were lagging in technological capability. Using the 10-point scale, the average equipment rating was 3.2. Only two respondents noted that their office was somewhat prepared, indicated by their assigned ranking of six or greater. No respondents felt that their office’s equipment and technological capabilities were completely adequate for prosecuting and managing cybercrime cases.

Seventy percent of the survey participants said their offices would need significant computer and network upgrades to be in a position to successfully manage and prosecute cybercrime cases. Basic computer equipment, such as PCs, laptops, and office suite software, were reported as the greatest need. A few respondents mentioned the need for advanced evidence management and presentation equipment, such as ELMO, which allows for the visual electronic presentation of multiple exhibits.

Personnel. Preparedness ratings for office personnel had similar results. The overall average personnel rating was only 4.2 on the 10-point scale, lower than the scale midpoint. Twelve respondents reported rankings below the midpoint, five indicated a rating at the scale midpoint, while the remaining three reported a personnel preparedness score of 6 or greater.

Training. Seven offices described their greatest personnel need as more staff training. Four respondents noted a need for more personnel in addition to more training specific to the prosecution of cybercrimes. Only one respondent rated the office training preparedness as higher than 5, with 16 reporting a score of less than 5 (average score = 3.2).

In sum, the respondents mentioned a strong need for more training related to cybercrime at all levels and as part of an attorney’s continuing legal education. Thirty-five percent of the participants noted a need for extensive training that would include not only senior attorneys but also other investigative and support staff. Twenty-five percent recommended expanding this training to local law enforcement personnel. Specific recommendations called for both substantive and procedural training, and noted the need for personnel to understand basic information on how cybercrimes are perpetrated, the dynamics of the Internet, file transfer methods, and telecommunication protocols. It was suggested that procedural training should, at a minimum, include information on search and seizure, as well as evidence management and presentation, and technology training for electronically presenting evidence to the jury.

Law enforcement coordination. Comments on the extent of law enforcement

and investigative support for prosecuting cybercrimes were more favorable, with a higher average preparedness ranking of 4.2. Score distribution showed more variance, however, ranging from 2 to 10. Sixty-seven percent of the survey participants noted an urgent need for law enforcement training, with some suggesting a joint training initiative that would involve members of the law enforcement community and staff of the prosecutors’ offices. Respondents noted that while SBI agents are adequately trained and normally called upon for assistance, local law enforcement must also know how to handle and process cybercrime evidence and cases.

Statutes. Seventy-five percent of those who responded to the survey thought that the current general statutes that address cybercrimes clearly delineate jurisdictional boundaries and issues. Members of the prosecutors’ offices rated the adequacy of the current general statutes from a low of 3 to a high of 10, with a mean ranking of 5.4. Thus, as a general rule the respondents felt that the statutes were not necessarily inadequate, but nor were they completely adequate either.

As part of the survey, the respondents were asked what is needed in terms of federal and state statutes to enhance effective and efficient prosecution of cybercrime cases. Eight provided illuminating responses, with concerns about the length of time required to prosecute these cases and the lack of “real” penalties for violators. Other comments centered on expanding current state law to allow for a “good faith” exception in searches and seizures, clarifying and strengthening existing child pornography laws, and the need to clarify jurisdictional issues and promote more collaborative investigative and prosecutorial endeavors.

General comments. In general, respondents identified the lack of training about cybercrime as the most significant obstacle that limits their abilities. An overwhelming number of comments were received about how the lack of training handicaps the prosecutors in performing their roles in the most effective and efficient manner. Sample comments include: “Takes a lot of time to prosecute one of these cases”; “Not enough law enforcement officials assigned to cases”; “Under-

(See **CYBERCRIME**, p. 8)

Prosecuting Computer Crime: Chasing A Silent Intruder

Every two years the Bureau of Justice Statistics (BJS) conducts the National Survey of Prosecutors, a survey of chief prosecutors who tried felony cases in state courts of general jurisdiction, about their offices' resources, policies, and practices. In 2001, the latest survey for which results are available, 2,243 prosecutors' offices (96% of the 2,341 offices nationwide) responded to the survey. Forty-two percent of prosecutors' offices reported prosecuting computer-related crimes in the 12 months preceding the survey. Three in ten offices reported that they had prosecuted crimes related to the transmittal of child pornography. A quarter of all offices prosecuted credit card fraud (27%) and bank card fraud (22%). Five percent prosecuted computer sabotage, and 3% the theft of intellectual property.

But calculating the true incidence of cybercrime is difficult. The first issue is that the definition of cybercrime is subject to interpretation. Incident reports may include crimes committed using computers and automated information systems as well as those where computer equipment or electronic files were the property stolen, damaged, or illegally accessed. Some crimes such as credit card fraud may require only stealing copies of paper credit card receipts where the perpetrator never touches a machine. Because estimates of cybercrime usually include incidents in which computers may be the instruments and/or the objects of a criminal offense, they may overstate the frequency of the popular notion of a computer-related crime, i.e., a sophisticated hacker breaking into critical electronic systems.

On the other hand, there is a likelihood of underreporting of certain cybercrimes where the victims either are not aware of a crime being committed against them or fail to report because of the possible embarrassment. In some jurisdictions, the existing laws may not be applicable to a computer-related action that would be a criminal offense in other locations (e.g., unauthorized access of electronic files may not be a crime if no overt damage is done) or the

local officials are not familiar enough with or trained in technology-related crimes. These circumstances may result in the undercounting of some cybercrimes.

The Internet Fraud Complaint Center, a partnership between the FBI and the National White Collar Crime Center (NW3C), reports that only one in four complaints filed with them had been reported to the police. The Computer Security Institute in San Francisco conducts an annual survey, now in its eighth year, of U.S. corporations, government agencies, financial institutions, medical institutions, and universities about the nature and extent of computer crime they have experienced. Highlights of the 2003 Computer Crime and Security Survey (528 respondents) include:

- 56% of respondents reported unauthorized computer use.
- Total annual loss was \$201,797,340, down from \$455,848,000 in 2002, but in line with amounts reported prior to 2001.
- As in previous years, theft of proprietary information caused the most serious financial loss (\$70,195,900); in a shift from earlier years, the second most expensive computer crime was denial of service, costing about \$65,643,300.
- 30% of respondents said they had reported incursions to law enforcement, more than in the NW3C survey, but still a low percentage.
- Virus incidents (82%) and insider abuse of network access (80%) were the types of attack most frequently cited.

In August 2001, BJS and the Census Bureau began a feasibility study of collecting nationwide statistics on computer crime against businesses. They produced the Computer Security Survey (CSS), which was sent to 500 businesses nationwide. CSS asked about prevalence and nature of computer crime, computer infrastructure and security used by businesses, and economic losses sustained as a result of computer crime.

Highlights include:

- Pilot sample consisted of 500 businesses representing 37 industries of all sizes,

representing 11% of employment and 16% of payroll nationwide.

- Survey development included three rounds of cognitive testing with 69 companies representing 14 industries in 7 states and Washington, D.C.
- Of the 208 responding companies, 198 used computers in 2001.

Results for companies with computers include:

- Response rates for detection of cybercrime incidents were 95%, on average.
- Nearly 75% of respondents detected at least one cybercrime incident.
- Fewer than 5% of companies detecting computer attacks said the offender was a company employee.
- Nearly 90% of companies detecting embezzlement reported incidents to law enforcement, compared to 12% of those detecting computer attacks.
- Of the 127 companies detecting virus infections, 87% detected more than one.
- Of the 50 companies detecting denial of service, 64% detected more than one.

The good news is that computer crime is increasingly recognized as a serious threat, and more effort is being made to categorize and control it. A list of computer crime and security resources follows.

- BJS/U.S. Census Bureau Survey form is available at: <http://www.census.gov/eos/www/css/cs1i.pdf>
- Computer Security Institute: <http://www.gocsi.com/>
Copies of the 2003 CSI/FBI Computer Crime and Security Survey are available for downloading.
- Internet Fraud Complaint Center: <http://www1.ifccfbi.gov/strategy/wn030409.asp>. The 2002 Annual Internet Fraud Report is available for downloading.
- Security Stats: <http://securitystats.com>. Begun in 2000, this Web site acts as a repository for what it terms "interesting computer security statistics." The site contains numerous links to other related Internet sites.

(**CYBERCRIME**, from p. 6)

staffed prosecutors"; "Witnesses may be out of state – too expensive to prosecute"; "Difficult to prove who was actually in front of the computer sending/receiving information"; "High caseload already and lack of familiarity with statutes makes it difficult to prosecute"; "Lack of law enforcement interest"; "Lack of AV equipment and equipment in general."

Respondents were also asked to recommend how to minimize these barriers to investigating and prosecuting cybercrime cases. Few specific and detailed recommendations were offered. Responses tended to be more global and centered around offering more training, updating existing equipment, purchasing state-of-the-art equipment and needed technological peripherals, improving federal and state cooperation, and adding more staff who would specialize in cybercrime case investigations and prosecutions. Offering training through the Conference of District Attorneys and establishing an interstate network to assist in the prosecution of cases were two of the more specific recommendations. Establishment of specialized prosecutors who would work statewide until local capabilities are developed and strengthened was also recommended.

Recommendations specific to the Governor's Crime Commission, the governmental organization that serves as the chief advisory board to the Governor on all criminal justice issues, included conducting a joint training session with the Conference of District Attorneys, using federal grant funds to purchase specialized equipment and to finance training, and offering financial assistance for the specialized statewide prosecutor plan should it be implemented.

Cybercrime in the Future. Eighty-one percent of those who responded to the survey felt strongly that cybercrimes would exert a strong, sizeable, and significant impact on North Carolina's prosecutors five years from now. Specific comments included: "Increasing even in rural districts"; "Will increase a lot with widespread use of the Internet and society becoming more computer dependent"; "Seen an increase in number of investigations, expect to prosecute some in the near future"; "Will see increase in identity theft"; "Will grow, i.e., specifically financial and sexual

exploitation cases"; "A very significant increase"; "Moderate increase, more in larger areas"; "Not much, Feds should handle most of it."

Discussion/Policy Implications and Recommendations

Study findings, comments from the prosecutors' staffs, and the low preparedness scale scores all suggest that the state's district attorneys' offices are currently not capable of managing and prosecuting cybercrime cases at the same level of effectiveness and efficiency they demonstrate with non-computer-related criminal cases. Only 35% of the offices were able to provide case statistics specific to cybercrime. Sixty percent of the surveyed offices reported that their current personnel do not have adequate and specialized knowledge for managing and prosecuting cybercrime cases. Average preparedness scores were low for all study factors, with the lowest scores being reported in the areas of equipment and training.

Given the fact that 81% of the respondents predicted a sizeable increase in both the number of anticipated cases and their projected impact on the prosecutors' offices, the following recommendations are offered. These suggestions are presented in an effort to proactively address the issue of cybercrime before it becomes an even more urgent issue or, at the extreme, a significant crisis and burden on the prosecutors.

Recommendation # 1

Cybercrime training should become a priority, with basic to advanced levels of instruction being available. Courses specific to the needs of the state's prosecutors should be developed, with an emphasis on the unique aspects of managing and prosecuting these types of cases. At a minimum this training should be offered to the state's district attorneys and their senior staff, and, if feasible, all assistant district attorneys and others who will be involved with any computer-related criminal cases. Joint training with local and state law enforcement officials is also strongly encouraged and could be offered through a conference format.

The Administrative Office of the Courts, the Conference of District Attorneys, the Institute of Government, and the North

Carolina Criminal Justice Academy are possible agencies that could play a role in developing and administering this training. Alternative training methodologies, such as video and teleconferencing, Internet-based applications, and computer-based training (CBT) modules, should be given serious consideration in light of the state's current fiscal situation. Training should be offered on a continual basis to reflect emerging trends, new technologies, and legal updates.


Recommendation # 2

The needs assessment survey clearly demonstrated the inadequacies of many of the state's prosecutors' offices in terms of their existing computer equipment and the lack of current technology needed to successfully prosecute cybercrime cases. Securing funding will remain a challenge as the current recession makes this an even more difficult proposition. Equipment procurement and computer upgrades for the state's prosecutors should be a top priority, with the need for modern equipment transcending the issue of computer-related crime. The state's prosecutors are encouraged to work closely with the Governor's Crime Commission to obtain the latest information on available funding sources and to receive technical assistance should they decide to submit a grant pre-application for addressing the equipment needs associated with cybercrime.

Recommendation # 3

Empaneling a legislative study commission to investigate the issue of cybercrime as it intersects e-commerce and e-government operations should be considered. The current general statutes regarding cybercrime should be reviewed, as well as the range of available sanctions, fines, and other penalties proscribed for these offenses.

Recommendation # 4

The lack of available case statistics on cybercrimes could pose future problems when financial, personnel, and time management decisions are based upon case management, administrative, and statistical data. Improving, or expanding, existing case management information systems to enable the prosecutors to extract relevant cybercrime data could be beneficial and allow district attorneys' offices to ascertain how cybercrime cases affect their existing workloads and court dockets. 

(HOMICIDE DATABASE, from p. 1)

it is possible to enter unknown for an offender's race; this element is not considered missing since unknown is a viable entry. Where information is reported as unknown in non-NIBRS data collected for this study, it is impossible to determine whether the information is truly unknown or could not be found in the case file. These unknown entries are discussed separately below.

In this study, all data elements required for NIBRS were available for 65% of the 373 incidents examined. The completeness of incident reports varied by state as well as by agency within the same state. In some agencies, information was consistently missing because it was not asked for on the incident report form and little additional information was included in the narrative.

Availability of Additional Data Elements

Besides collecting the data elements required for NIBRS, researchers in this study looked at whether incident reports contained the additional elements of victim and offender employment, marital status, and zip code. The vast majority of incident reports were missing one or more of these data elements. Only 8% of the incidents included all of the NIBRS and additional data elements.

Demographic Data

While it is possible that basic offender information such as age and race could be unknown in cases with no witnesses, it is less likely that the same victim and arrestee information would be unknown. Yet the expected demographic information was spotty in most states, with several entries listed as unknown. One state, for example, reported ethnicity in the case files. Since demographic information is required in NIBRS, agencies reporting NIBRS data were more likely to have such data than non-NIBRS agencies.

Comparison of NIBRS and Homicide Study Data

Two states participating in this study include agencies that are currently reporting NIBRS data. The homicide incidents reported in 2000 as collected in this study were matched to the same incidents reported to NIBRS. Since the incident numbers are encrypted in NIBRS, the incident date and hour were used to match incidents. In large agen-

cies with many homicide incidents, it is possible that different incidents are being compared. In small agencies with few homicides, incidents are easier to match.

Where discrepancies were noted, there was no way to determine which data were "correct," except where data were not reported. Since little emphasis was placed on the property offenses occurring in conjunction with the homicide incidents examined in this study, only the administrative, offense, victim, offender, and arrestee data were compared.

Unknown Entries

In one state, the homicide data collected for this study frequently contained incidents, offenses, victims, and arrestees that could not be found in NIBRS, while in another, the NIBRS data contained offenses, victims, offenders, and arrestees that were not collected in this study. This may be an issue related to the updating of records; as corrections are made at the agency level, the information may not be reported to NIBRS.

Missing or Unreported Data

As can be seen in Table 1, much of the information left blank in NIBRS could be found in the case files reviewed for this study. In the offense segment, NIBRS entries for type of criminal activity are often left blank (41%), despite a coding option of "None." Whether a weapon is an automatic is also missing in the data compared (34%). Two offenses reporting a second weapon in the homicide data were not reported in the NIBRS data (6%). One possible explanation is timing – the data collected for this study are more recent than the NIBRS data file used for comparison. It may be that additional information was known at the time of this study that was not available when the information was first reported to NIBRS.

Although all of the personal information variables in NIBRS include a coding

option for "Unknown," this information is often left blank. Much of the victim, offender, and arrestee information that was blank in NIBRS could be found in the case files. An oddity is that some information not available in the case files was reported to NIBRS. It may be that some details were known to reporting officers but were not included in the case file, or this information was overlooked when the data were collected for this study.

Use of Nonspecific Codes

One issue with data entry systems used to code NIBRS data is the use of default codes. For several variables, for example, the default value may be "None," which is only changed if the user enters different information. The result may be an overuse of nonspecific codes, such as "None," "Other," or "Unknown." To examine how often this occurred, the NIBRS and study data were compared to see whether specific information could be found when these codes were used. As can be seen in Table 2, nonspecific codes are often used in NIBRS when the information is known.

Discrepancies

Some consistent discrepancies were found between the NIBRS and study data. Ethnicity and residence are often missing in NIBRS but can be found in the study data. In addition, weapons are much more likely to be listed as automatic in the data collected for this study. Type of arrest also differs, apparently with some confusion between "taken into custody" and "on-site arrest." Surprisingly, age also varied between the data sets, both for victims and offenders.

Ability to Collect NIBRS

It seems clear that the agencies included in this study that are not currently collecting incident-based data are able to report most of the required information

(See **HOMICIDE DATABASE, p. 10**)

Table 1. Data Elements Collected in One Data Set But Missing in the Other

Segment	Missing in NIBRS	Missing in Study
Administrative	0%	4%
Offense	84%	9%
Victim	76%	3%
Offender	48%	0%
Arrestee	58%	21%

ANNOUNCEMENTS



New Book Describes Effective Programs for At-Risk Youth

Doug Yearwood and James Klopovic of the North Carolina SAC have collaborated on a new book with Michael Vasu of North Carolina State University that offers approaches for developing, establishing, and strengthening community-based services for youth. The book, *Effective Program Practices for At-Risk Youth: A Continuum of Community-Based Programs*, is scheduled for publication this month by Civic Research Institute in Princeton, NJ. The book describes how to start model programs and improve existing programs by basing practices on projects shown to be effective. Step-by-step instructions explain how to use community

resources in a productive way, and numerous examples are given to show how other programs and practitioners have successfully addressed the problems of at-risk youth. The book is meant to be a practical guide for use by those working in the field. For more information, contact the Civic Research Institute at (609) 683-4450.

CSUN Offers Crime and Intelligence Analysis Certificate Program

The Crime and Intelligence Analysis Certificate Program offered by the College of Extended Learning at California State University, Northridge (CSUN) was developed in 1997 to meet the growing need for trained analysts within law enforcement. Participants gain a solid foundation of practical knowledge and skills required in the many

activities of crime and intelligence analysis.

The CSUN certificate consists of 8 courses, ranging in length from 16 to 40 classroom hours, and carries POST certification, level IV. Participants who complete this program also earn a certificate from the California Department of Justice, designating them as Certified Crime and Intelligence Analysts. Designed for the busy professional, courses in this program meet on the weekend, with most classes beginning at noon on Friday. Classes begin in September.

For additional information visit http://www.csun.edu/exl/program/01certificate/crml_prgm.htm or contact Joyce Mikus, Senior Program Coordinator, at 818 677-3404, or email her at joyce.mikus@csun.edu

(HOMICIDE DATABASE, from p. 9)

for homicides. In most of the agencies visited, however, the necessary information was found only in the case files, not in the records management system (RMS) or incident reports. The time constraints in locating the appropriate information, coupled with the need for training on NIBRS codes and the costs of updating records management systems, however, make it unlikely that agencies will commit to collecting the necessary data.

Conclusion

It seems clear that NIBRS changes the way in which the data are collected, but it does not appear to have a great effect on the amount of information collected. Most of the agencies participating in this study were able to provide the information required for NIBRS, even though the information could not always be found in the RMS.

Reporting NIBRS data for homicides is possible for all of the agencies in this study. The information was available, if not always readily accessible. In order for agencies to report the NIBRS data, they

would have to update their RMS systems to allow the additional data to be entered, or they would have to create new forms to capture the additional information.

In non-NIBRS agencies, supplemental forms are already completed for every homicide reported. Although participation in the Supplemental Homicide Reporting (SHR) program is voluntary, most agencies do choose to participate. These forms, either in hard copy or computerized format, are sent to the state program and then to the FBI.

Rather than creating a new platform for collecting homicide data, perhaps the

time has come for the existing program to be updated to be compatible with NIBRS. Rather than requiring law enforcement to capture information on a second form, only one form that captures incident-based data should be used. The SHR program should be expanded to include the more detailed information in NIBRS. This would negate the need for an additional database on homicides by using the infrastructure already in place for SHR data.


(For more information about this research, please look for the *Developing a NIBRS-Compatible Homicide Database: A Multistate Pilot Test*, available soon.) 

Table 2. Use of Nonspecific Codes in One Data Set for Information Present in the Other

Segment	Nonspecific in NIBRS	Nonspecific in Study
Administrative	4%	0%
Offense	31%	9%
Victim	67%	9%
Offender	3%	0%
Arrestee	26%	11%



Reentry and Criminal Justice

A Review of Petersilia's *When Prisoners Come Home: Parole and Prisoner Reentry*

[This review was written by Michael Connelly, JRSA Project Manager, and Jill Farrell, a doctoral student at the University of Maryland.]

Policymakers and researchers have begun to pay more attention to reentry in recent years and to detail its scope, structure, and implications. Foremost among these is Joan Petersilia, who has brought together her work and that of others in a comprehensive examination of prisoner reentry, *When Prisoners Come Home: Parole and Prisoner Reentry* (2003).

After exhaustive detailing of the nature and conditions of prisoners rejoining their communities after release from prison, Petersilia thoroughly discusses the releasees, the parole system, ways to help and to obstruct successful prisoner reentry, recidivism of releasees, and victims and their roles in reentry. She then outlines four general reforms (with 12 detailed recommendations) that she believes will lead to better outcomes for the offenders and for the communities they reenter:

- Reinvestment in prison work, education, and substance abuse programs.
- Reinstitution of discretionary parole in the states that have abolished it and reversal of the current trends toward automatic mandatory release.
- Front-loading of postprison services into the first six months after release, the period in which the offenders are most likely to recidivate.
- Establishment of procedures to allow some offenders to put their offending in the past, permitting regaining of voting privileges, and answering "no" to employment and other questions about past criminality.

These reforms do not address the problem she sees of sending too many offenders to prison who should not be there, who may in fact turn into greater costs to society and victims for having been there. Regarding that problem, she

(See **BOOK REVIEW**, p. 12)

Additional Resources on Prisoner Reentry

[Jill Farrell, a doctoral student in criminal justice at the University of Maryland, compiled this bibliography.]

- Austin, J. (2001). Prisoner reentry: Current trends, practices, and issues. *Crime & Delinquency*, 47, 314-34.
- Bradley, K., Oliver, R.B., Richardson, N., & Slayter, E. (2001). *No place like home: Housing and the ex-prisoner*. Boston: Community Resources for Justice.
- Clear, T.R., Rose, D.R., & Ryder, J.A. (2001). Incarceration and the community: The problem of removing and returning offenders. *Crime & Delinquency*, 47, 335-51.
- Hagan, J., & Dinovitzer, R. (1999). Collateral consequences of imprisonment for children, communities, and prisoners. In M. Tonry & J. Petersilia (Eds.), *Prisons*. Chicago: University of Chicago Press.
- Hammett, T.M., Roberts, C., & Kennedy, S. (2001). Health-related issues in prisoner reentry. *Crime & Delinquency*, 47, 390-409.
- Herman, S., & Wasserman, C. (2001). A role for victims in offender reentry. *Crime & Delinquency*, 47, 428-45.
- Lurigio, A.J. (2001). Effective services for parolees with mental illnesses. *Crime & Delinquency*, 47, 446-61.
- Lynch, J.P., & Sabol, W.J. (2000). *Prisoner reentry in perspective* (Urban Institute Crime Policy Report). Washington, DC: Urban Institute Press.
- Maruna, S. (2001). *Making good: How ex-convicts reform and rebuild their lives*. Washington, DC: American Psychological Association.
- Mauer, M., & Chesney-Lind, M. (2002). *Invisible punishment: The collateral consequences of mass imprisonment*. New York: The New Press.
- Nagin, D., & Waldfoegel, J. (1998). The effects of conviction on income through the life cycle. *International Review of Law and Economics*, 18, 25-40.
- O'Brien, P. (2001). "Just like baking a cake:" Women describe the necessary ingredients for successful prisoner reentry after incarceration. *Families in Society: The Journal of Contemporary Human Services*, 82, 287-95.
- Petersilia, J. (1999). Parole and prisoner reentry in the United States. In M. Tonry & J. Petersilia (Eds.), *Prisons*. Chicago: University of Chicago Press.
- Petersilia, J. (2000). When prisoners return to the community: Political, economic, and social consequences. In *Sentencing & Corrections, Issues for the 21st Century*, 9. Washington, DC: National Institute of Justice.
- Petersilia, J. (2001). Prisoner reentry: Public safety and reintegration challenges. *The Prison Journal*, 81, 360-75.
- Petersilia, J. (2003). *When prisoners come home: Parole and prisoner reentry*. Oxford: Oxford University Press.
- Petersilia, J., & Turner, S. (1993). Intensive probation and parole. In M. Tonry (Ed.), *Crime and justice: A review of research* (Vol. 17). Chicago: University of Chicago Press.
- Richie, B.E. (2001). Challenges incarcerated women face as they return to their communities: Findings from life history interviews. *Crime & Delinquency*, 47, 368-89.
- Rose, D.R., & Clear, T.R. (1998). Incarceration, social capital and crime: Examining the unintended consequences of incarceration. *Criminology*, 36, 441-79.
- Rose, D.R., Clear, T.R., & Ryder, J.A. (2001). Addressing the unintended consequences of incarceration through community-oriented services. *Corrections Management Quarterly*, 5, 69-78.
- Seiter, R., Kadela, K. (2003). Prisoner reentry: What works, what doesn't, and what's promising. *Crime & Delinquency*, 49.
- Shapiro, C. (2001). Coming home: Building on family connections. *Corrections Management Quarterly*, 5, 52-62.
- Travis, J. (2000). But they all come back: Rethinking prisoner reentry. In *Sentencing & Corrections, Issues for the 21st Century*, 7. Washington, DC: National Institute of Justice.
- Travis, J., & Petersilia, J. (2001). Reentry reconsidered: A new look at an old question. *Crime & Delinquency*, 47, 291-313.
- Travis, J., Solomon, A.L., & Waul, M. (2001). *From prison to home: The dimensions and consequences of prisoner reentry*. Washington DC: Urban Institute.
- Uggen, C., Manza, J., & Behrens, A. (2002). Stigma, role transition, and the civic reintegration of convicted felons. In S. Maruna & R. Immarigeon (Eds.), *After crime and punishment: Ex-offender reintegration and desistance from crime*. Albany: State University of New York Press.
- Western, B., Kling, J.R., Weiman, D.F. (2001). The labor market consequences of incarceration. *Crime & Delinquency*, 47, 410-27.
- Wilkinson, R. (2001). Offender reentry: A storm overdue. *Corrections Management Quarterly*, 5, 46-51.


(BOOK REVIEW, from p. 11)

calls for greater assessment of the criminalizing effects of prison, the collateral damage of the war on drugs, the inter-generational impacts of imprisonment on families and children, the decreasing power of prisons to deter, and the increased selectivity in prison sentencing.

Specialized and general readers alike will find much of value in Petersilia's analyses and her descriptions of effective programs and strategies. For those who want one book on prisoner reentry, this is it, and it probably will be for many years to come. Those who want to read more on the topic should examine some or all of the following, which are available on the Internet, or they may review the literature detailed in the bibliography that accompanies this article:

- *Why Planning Release Matters* from the Vera Institute provides a shorter overview of the topic with good descriptions of programs such as Project RIO in Texas, Ohio job fairs, and

Montgomery County, Maryland's Pre-Release Center.

- *The Three "R's" of Reentry* from Justice Solutions approaches reentry from victims' perspectives and emphasizes reparative justice, relationships, and responsibility
- *Prisoner Reentry in Perspective* from the Urban Institute outlines reentry in admirable depth for a shorter work and does an excellent job discussing the problems of offenders who "churn" in and out of the system repeatedly.
- *Offender Reentry: A Storm Overdue* from *Corrections Management Quarterly* details the "Ohio Plan" and that state's reentry court initiative.
- *The Ex-Offender Employability Task Force Report to the Illinois Workforce Investment Board* from Sommers Consulting describes the issues of employability for releasees, the task force's analysis of "best practices" in improving offenders' employability, and an "advocacy agenda" to lay a foundation for successful reentry through successful employment. 

SAVE THE DATE!

Bureau of Justice Statistics/
Justice Research and
Statistics Association

2003 National Conference

October 2-3

Westin St. Francis Hotel
San Francisco, California

For up-to-date conference
information, visit
www.jrsa.org

If you did not receive a conference announcement by e-mail a few weeks ago, it may mean we have an incorrect address for you. Please e-mail kmaline@jrsa.org to update our records.

The JRSA Forum is supported by the U.S. Department of Justice, Bureau of Justice Statistics. JRSA is a national nonprofit organization. For membership or other information, call (202) 842-9330, e-mail cjinfo@jrsa.org, or visit our Web site: <http://www.jrsa.org>.

Karen F. Maline, Editor
Nancy Michel, Managing Editor

JRSA Officers and Staff

Robert F. McManus, President
William Clements, Vice President
Douglas Yearwood, Secretary/Treasurer
Nancy Arrigona, Delegate
Michelle Bynum, Appointed Delegate
Tom Murphy, Past President

Joan C. Weiss, Executive Director
Ali Burnett, Office Manager
Linda Carter, Administrative Assistant
Michael Connelly, Project Manager
Loyce Craft, Assistant Director of Administration
Sandra Dayton, Director of Finance and Administration
Deborah Levy, Research Analyst
Karen F. Maline, Director of Information and Member Services
Eileen McDermott, Program Assistant
Nancy Michel, Director of Publications
Ashley Nellis, Research Associate
Stan Orchowosky, Research Director
Marc Osman, Web Site Manager
Matthew Perkins, Project Manager
Mary Poulin, Project Manager
Lorena Sobhi, Administrative Coordinator
Veronica Puryear, Research Associate
Marylinda Stawasz, Special Assistant to the Executive Director
Jason Trask, Research Analyst
Lisa Walbolt, Project Manager
Lisa Wilson, Secretary/Receptionist
Stan Wolfe, Project Manager
James Zepp, Director, Training and Technical Assistance Center

Justice Research and Statistics Association
777 North Capitol Street, NE
Suite 801
Washington, DC 20002

First Class
U.S. Postage
PAID
Permit No. 5356
Washington, DC