DEC. 06

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Special **REPORT**

Test Results for Hardware Write Block Device: WiebeTech Forensic SATADock (FireWire Interface)

www.ojp.usdoj.gov/nij

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Alberto R. Gonzales
Attorney General

Regina B. Schofield
Assistant Attorney General

Glenn R. Schmitt
Acting Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
www.ojp.usdoj.gov/nij

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

NIJ

DEC. 06

Test Results for Hardware Write Block Device: WiebeTech Forensic SATADock (FireWire Interface)

NCJ 216300

NIJ

Glenn R. Schmitt
Acting Director

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Office of Law Enforcement Standards of the National Institute of Standards and Technology under Interagency Agreement 2003–IJ–R–029.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Test Results for Hardware Write Block Device: WiebeTech Forensic SATADock (FireWire Interface)

December 2006

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Contents

Introduction **3**

Test Results for Hardware Write Block Devices **4**

1 Results Summary by Requirements 4
2 Test Case Selection 4
3 Testing Environment 5
3.1 Test Computers 5
3.2 Protocol Analyzer 5
3.3 Hard Disk Drives 5
3.4 Support Software 6
4 Test Results 7
4.1 Test Results Report Key 7
4.2 Test Details 8

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, Internal Revenue Service Criminal Investigation's Electronic Crimes Program, and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. This approach to testing computer forensic tools is based on well-recognized methodologies for conformance and quality testing. The specifications and test methods are posted on the CFTT Web site (http://www.cftt.nist.gov/) for review and comment by the computer forensics community.

This document reports the results from testing the **WiebeTech Forensic SATADock (FireWire Interface)** write blocker, against the *Hardware Write Blocker (HWB) Assertions and Test Plan Version 1.0*, available at the CFTT Web site (http://www.cftt.nist.gov/HWB-ATP-19.pdf). This specification identifies the following top-level tool requirements:

- A hardware write block (HWB) device shall not transmit a command to a protected storage device that modifies the data on the storage device.
- An HWB device shall return the data requested by a read operation.
- An HWB device shall return without modification any access-significant information requested from the drive.
- Any error condition reported by the storage device to the HWB device shall be reported to the host.

Test results from other software packages and the CFTT tool methodology can be found on NIJ's computer forensics tool testing Web page, http://www.ojp.usdoj.gov/nij/topics/ecrime/cftt.htm.

Test Results for Hardware Write Block Devices

Device Tested:	WiebeTech Forensic SATADock (FireWire Interface)
Model:	FSDK
Serial No:	40701000039
Firmware:	22:32:43 Jan 11 2004 v1.05.0000
Host to Blocker Interface:	FireWire
Blocker to Drive Interface:	SATA
Supplier:	WiebeTech LLC
Address:	WiebeTech LLC 8200 East 34th Street North #1404 Wichita, KS 67226 866–744–8722 http://www.wiebetech.com/

1 Results Summary by Requirements

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device.
For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation.
For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive.
For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host.
For all test cases run, the device always returned error codes from the protected drive without modification.

2 Test Case Selection

Since a protocol analyzer was not available for the interface between the blocker and the protected drive, the following test cases were appropriate: HWB–02, HWB–04, HWB–05, HWB–07, HWB–08, and HWB–09.

For test case HWB–04, two variations were selected: file (attempt to use operating system commands to create and delete file system objects (files and directories) from a protected drive) and image (use an imaging tool to attempt to write to a protected drive).

For test case HWB–07, one variation was selected: ix (use a stand-alone imaging tool (IXimager) to read from a protected drive).

3 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the hardware (test computers and hard drives) available for testing.

3.1 Test Computers

One test computer was used: **Freddy**, which has the following configuration:

Intel Desktop Motherboard D865GB/D865PERC (with ATA–6 IDE on board controller)
BIOS Version BF86510A.86A.0053.P13
Adaptec SCSI BIOS V3.10.0
Intel Pentium™ 4 CPU
SONY DVD RW DRU-530A, ATAPI CD/DVD–ROM drive
1.44MB floppy drive
Two slots for removable IDE hard disk drives
Two slots for removable SATA hard disk drives
Two slots for removable SCSI hard disk drives

3.2 Protocol Analyzer

A Data Transit bus protocol analyzer (Bus Doctor Rx) was used to monitor and record commands sent from the host to the write blocker. Two identical protocol analyzers were available for monitoring commands.

One of two Dell laptop computers (either Chip or Dale) was connected to each protocol analyzer to record commands observed by the protocol analyzer.

3.3 Hard Disk Drives

The hard disk drives used in testing are described below.

```
Drive label: 109
Partition table Drive /dev/hdg
09728/254/63 (max cyl/hd values)
09729/255/63 (number of cyl/hd)
156301488 total number of sectors
IDE disk: Model (WDC WD800JD-32HKA0) serial # (WD-WMAJ91407692)
 N   Start LBA Length    Start C/H/S End C/H/S   boot Partition type
 1 P 000000063 000016002 0000/001/01 0000/254/63      01 Fat12
 2 X 000016065 156280320 0001/000/01 1023/254/63      0F extended
 3 S 000000063 020482812 0001/001/01 1023/254/63      0B Fat32
 4 S 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 5 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 6 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
```

```
Drive label: 11
Partition table Drive /dev/sda
19456/254/63 (max cyl/hd values)
19457/255/63 (number of cyl/hd)
312581808 total number of sectors
Non-IDE disk
Model (WDC WD1600JD-00G) serial # (WD-WMAEP1785434)
 N   Start LBA Length    Start C/H/S End C/H/S   boot Partition type
 1 X 000016065 312560640 0001/000/01 1023/254/63      0F extended
 2 S 000000063 000032067 0001/001/01 0002/254/63      01 Fat12
 3 x 000032130 000080325 0003/000/01 0007/254/63      05 extended
 4 S 000000063 000080262 0003/001/01 0007/254/63      0B Fat32
 5 x 000112455 312448185 0008/000/01 1023/254/63      05 extended
 6 S 000000063 312448122 0008/001/01 1023/254/63      07 NTFS
 7 S 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 8 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 9 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
10 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
```

```
Drive label: 0A
Partition table Drive /dev/hde
09728/254/63 (max cyl/hd values)
09729/255/63 (number of cyl/hd)
156301488 total number of sectors
IDE disk: Model (WDC WD800JD-32HKA0) serial # (WD-WMAJ91508343)
 N   Start LBA Length    Start C/H/S End C/H/S   boot Partition type
 1 P 000000063 156280257 0000/001/01 1023/254/63 Boot 07 NTFS
 2 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 3 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 4 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
```

P primary partition (1–4)
S secondary (sub) partition
X primary extended partition (1–4)
x secondary extended partition

3.4 Support Software

The software in the following table was used to send commands to the protected drive. One widely used imaging tool, IXimager, was used to generate disk activity (reads and writes) consistent with a realistic scenario of an accidental modification of an unprotected hard drive during a forensic examination. This does not imply an endorsement of the imaging tool.

Program	**Description**
sendSCSI	A tool to send SCSI commands wrapped in the USB or IEEE 1394 (FireWire) protocols to a drive.
FS–TST	Software from the FS–TST tools was used to generate errors from the hard drive by trying to read beyond the end of the drive. The FS–TST software was also used to setup the hard drives and print partition tables and drive size.
IXimager	An imaging tool (ILook IXimager version 1.0, August 25, 2004) for test case 04-img.

4 Test Results

The main item of interest for interpreting the test results is determining the conformance of the device with the test assertions. Conformance with each assertion tested by a given test case is evaluated by examining the Blocker Input and Blocker Output boxes of the test report summary.

4.1 Test Results Report Key

A summary of the actual test results is presented in this report. The following table presents a description of each section of the test report summary.

Heading	Description
First Line	Test case ID; name, model, and interface of device tested.
Case Summary	Test case summary from *Hardware Write Blocker (HWB) Assertions and Test Plan Version 1.0.*
Assertions Tested	The test assertions applicable to the test case, selected from *Hardware Write Blocker (HWB) Assertions and Test Plan Version 1.0.*
Tester Name	Name or initials of person executing test procedure.
Test Date	Time and date that test was started and completed.
Test Configuration	Identification of the following: 1. Host computer for executing the test case. 2. Laptop attached to each protocol analyzer. 3. Protocol analyzers monitoring each interface. 4. Interface between host and blocker. 5. Interface between blocker and protected drive. 6. Execution environment for tool sending commands from the host.
Hard Drives Used	Description of the protected hard drive.
Blocker Input	For test case HWB–02, a list of commands sent is provided. For test cases HWB–02 and HWB–04, an SHA1 value for the entire drive is provided for reference. For test case HWB–05, a string of known data from a given location is provided for reference.
Blocker Output	For test cases HWB–02, HWB–04, and HWB–07, an SHA1 value computed after commands are sent to the protected drive is given for comparison to the reference SHA1 value. For test case HWB–05, a string read from a given location is provided for comparison to known data. For test case HWB–08, the number of sectors determined for the protected drive and the partition table are provided.

Heading	Description
	For test case HWB–09, any error return obtained by trying to access a nonexistent sector of the drive is provided.
Results	Expected and actual results for each assertion tested.
Analysis	Whether or not the expected results were achieved.

4.2 Test Details

Test Case HWB-02 Variation hwb-02 WiebeTech Forensic SATADOCK (FireWire)

Case Summary:	HWB-02 Identify modifying commands blocked by the HWB.
Assertions Tested:	HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device.
Tester Name:	kbr
Test Date:	run start Wed Apr 12 10:13:58 2006 run finish Wed Apr 12 10:17:54 2006
Test Configuration:	HOST: freddy HostToBlocker Monitor: dale HostToBlocker PA: aa00155 HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: SATA Run Environment: Linux
Drives:	Protected drive: 109 109 is a SATA drive with 156301488 sectors (80 GB)
Blocker Input:	SHA of 109 is FE7F2F3B735B37F685E13E14AA5FCF1C42561E08 - Commands Sent to Blocker 42 READ(10) 2 WRITE(10) 1 WRITE(12) 1 WRITE BUFFER 1 WRITE LONG 1 WRITE SAME 2 WRITE/VERIFY 1 XDWRITE(10) 1 XDWRITEREAD(10) 1 XPWRITE(10)
Blocker Output:	CMD: /mnt/floppy/diskhash.csh hwb freddy kbr /dev/sdb 109 - after FE7F2F3B735B37F685E13E14AA5FCF1C42561E08 -
Results:	**Assertion & Expected Result** / **Actual Result** AM-01 Modifying commands blocked / Modifying commands blocked
Analysis:	Expected results achieved

Test Case HWB-04 Variation hwb-04-file WiebeTech Forensic SATADOCK (FireWire)

Test Case HWB-04 Variation hwb-04-file WiebeTech Forensic SATADOCK (FireWire)	
Case Summary:	HWB-04 Attempt to modify a protected drive with forensic tools.
Assertions Tested:	HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device.
Tester Name:	kbr
Test Date:	run start Tue Apr 25 14:48:48 2006 run finish Tue Apr 25 14:58:19 2006
Test Configuration:	HOST: freddy HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: SATA Run Environment: WXP
Drives:	Protected drive: 11 11 is a SATA drive with 312581808 sectors (160 GB)
Blocker Input:	SHA of 11 is 2653AA0443BB572C36DD42E5FF21FA15362740AA - Commands are sent to blocker by OS operations: @echo off REM %1 is the directory where alpha, beta & gamma are created REM Redirect the output to a logfile REM hwb-mod . X: > dir-setup.txt echo "mod: %1" mkdir %1\delta rmdir %1\gamma copy %1\beta\zeta.txt %1\alpha copy %1\beta\omega.txt %1\delta del %1\beta\zeta.txt dir %1 /b /s
Blocker Output:	Results for FAT partition: "mod: d:" 1 file(s) copied. 1 file(s) copied. D:\PQTMP.FIL D:\alpha D:\beta D:\delta D:\alpha\zeta.txt D:\System Volume Information_restore{FC9DC008-32CE-4FBD-9588-4818DCA2C439} D:\beta\omega.txt D:\delta\omega.txt Results for NTFS partition: "mod: f:" 1 file(s) copied. 1 file(s) copied. F:\alpha F:\beta F:\delta F:\alpha\zeta.txt F:\beta\omega.txt

Test Case HWB-04 Variation hwb-04-file WiebeTech Forensic SATADOCK (FireWire)	
	F:\delta\omega.txt Final SHA1 value: CMD: /mnt/floppy/diskhash.csh hwb-04-file freddy kbr /dev/sdb 11 -after 2653AA0443BB572C36DD42E5FF21FA15362740AA -
Results:	**Assertion & Expected Result** / **Actual Result** AM-01 Modifying commands blocked / Modifying commands blocked
Analysis:	Expected results achieved

Test Case HWB-04 Variation hwb-04-img WiebeTech Forensic SATADOCK (FireWire)	
Case Summary:	HWB-04 Attempt to modify a protected drive with forensic tools.
Assertions Tested:	HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device.
Tester Name:	kbr
Test Date:	run start Wed Apr 12 14:07:46 2006 run finish Wed Apr 12 14:19:27 2006
Test Configuration:	HOST: freddy HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: SATA Run Environment: IXimager
Drives:	Protected drive: 109 109 is a SATA drive with 156301488 sectors (80 GB)
Blocker Input:	SHA of 109 is FE7F2F3B735B37F685E13E14AA5FCF1C42561E08 - Commands are sent to blocker by imaging tool
Blocker Output:	CMD: /mnt/floppy/diskhash.csh hwb freddy kbr /dev/sdb 109 -after FE7F2F3B735B37F685E13E14AA5FCF1C42561E08 -
Results:	**Assertion & Expected Result** / **Actual Result** AM-01 Modifying commands blocked / Modifying commands blocked
Analysis:	Expected results achieved

Test Case HWB-05 Variation hwb-05 WiebeTech Forensic SATADOCK (FireWire)	
Case Summary:	HWB-05 Identify read commands allowed by the HWB.
Assertions Tested:	HWB-AM-02 If the host sends a read category operation to the HWB and no error is returned from the protected storage device to the HWB, then the data addressed by the original read operation is returned to the host.
Tester Name:	kbr
Test Date:	run start Wed May 10 11:25:09 2006 run finish Wed May 10 11:31:24 2006

<table>
<tr><th colspan="2">Test Case HWB-05 Variation hwb-05 WiebeTech Forensic SATADOCK (FireWire)</th></tr>
<tr><td>Test Configuration:</td><td>HOST: freddy
HostToBlocker Monitor: dale
HostToBlocker PA: aa00155
HostToBlocker Interface: FW
BlockerToDrive Monitor: none
BlockerToDrive PA: none
BlockerToDrive Interface: SATA
Run Environment: Linux</td></tr>
<tr><td>Drives:</td><td>Protected drive: 0a</td></tr>
<tr><td>Blocker Input:</td><td>Commands Sent to Blocker
Read sector 32767 for the string: 00002/010/08 000000032767</td></tr>
<tr><td>Blocker Output:</td><td>00032/008/08 000000032767</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-02 Read commands allowed</td><td>Read commands allowed</td></tr></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

<table>
<tr><th colspan="2">Test Case HWB-07 Variation hwb-07 WiebeTech Forensic SATADOCK (FireWire)</th></tr>
<tr><td>Case Summary:</td><td>HWB-07 Read a protected drive with forensic tools.</td></tr>
<tr><td>Assertions Tested:</td><td>HWB-AM-02 If the host sends a read category operation to the HWB and no error is returned from the protected storage device to the HWB, then the data addressed by the original read operation is returned to the host.
HWB-AM-03 If the host sends an information category operation to the HWB and if there is no error on the protected storage device, then any returned access-significant information is returned to the host without modification.</td></tr>
<tr><td>Tester Name:</td><td>kbr</td></tr>
<tr><td>Test Date:</td><td>run start Wed Apr 12 10:28:18 2006
run finish Wed Apr 12 14:06:59 2006</td></tr>
<tr><td>Test Configuration:</td><td>HOST: freddy
HostToBlocker Monitor: none
HostToBlocker PA: none
HostToBlocker Interface: FW
BlockerToDrive Monitor: none
BlockerToDrive PA: none
BlockerToDrive Interface: SATA
Run Environment: IXimager</td></tr>
<tr><td>Drives:</td><td>Protected drive: 109
109 is a SATA drive with 156301488 sectors (80 GB)</td></tr>
<tr><td>Blocker Input:</td><td>SHA of 109 is FE7F2F3B735B37F685E13E14AA5FCF1C42561E08 -
Commands Sent to Blocker
Commands are sent to blocker by imaging tool</td></tr>
<tr><td>Blocker Output:</td><td>Apr 12 11:56:50 iimager: SHA-1 Value : fe7f2f3b735b37f685e13e14aa5fcf1c42561e08</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-02 Read commands allowed</td><td>Read commands allowed</td></tr><tr><td>AM-03 Access Significant</td><td>Access Significant</td></tr></table></td></tr>
</table>

Test Case HWB-07 Variation hwb-07 WiebeTech Forensic SATADOCK (FireWire)		
	Information unaltered	Information unaltered
Analysis:	Expected results achieved	

Test Case HWB-08 Variation hwb-08 WiebeTech Forensic SATADOCK (FireWire)		
Case Summary:	HWB-08 Identify access significant information unmodified by the HWB.	
Assertions Tested:	HWB-AM-03 If the host sends an information category operation to the HWB and if there is no error on the protected storage device, then any returned access-significant information is returned to the host without modification.	
Tester Name:	kbr	
Test Date:	run start Wed Apr 12 10:23:55 2006 run finish Wed Apr 12 10:25:13 2006	
Test Configuration:	HOST: freddy HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: SATA Run Environment: Linux	
Drives:	Protected drive: 109 109 is a SATA drive with 156301488 sectors (80 GB)	
Blocker Output:	cmd: /mnt/floppy/partab hwb-08 freddy kbr /dev/sdb 109 -all 156301488 total number of sectors	
Results:	**Assertion & Expected Result**	**Actual Result**
	AM-03 Access Significant Information unaltered	Access Significant Information unaltered
Analysis:	Expected results achieved	

Test Case HWB-09 Variation hwb-09 WiebeTech Forensic SATADOCK (FireWire)	
Case Summary:	HWB-09 Determine if an error on the protected drive is returned to the host.
Assertions Tested:	HWB-AM-04 If the host sends an operation to the HWB and if the operation results in an unresolved error on the protected storage device, then the HWB shall return an error status code to the host.
Tester Name:	kbr
Test Date:	run start Wed Apr 12 10:25:46 2006 run finish Wed Apr 12 10:27:26 2006
Test Configuration:	HOST: freddy HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: SATA Run Environment: Linux

<table>
<tr><th colspan="2">Test Case HWB-09 Variation hwb-09 WiebeTech Forensic SATADOCK (FireWire)</th></tr>
<tr><td>Drives:</td><td>Protected drive: 109
109 is a SATA drive with 156301488 sectors (80 GB)</td></tr>
<tr><td>Blocker Output:</td><td>09728/254/63 (max cyl/hd values)
09729/255/63 (number of cyl/hd)
156301488 total number of sectors
cmd: /mnt/floppy/diskchg hwb-09 freddy kbr /dev/sdb -read 256301488 0 1
Disk addr lba 256301488 C/H/S 15954/7/38 offset 0
Disk read error 0xFFFFFFFF at sector 15954/7/38</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-04 Error code returned</td><td>Error code returned</td></tr></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

About the National Institute of Justice

NIJ is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety. NIJ's principal authorities are derived from the Omnibus Crime Control and Safe Streets Act of 1968, as amended (see 42 U.S.C. §§ 3721–3723).

The NIJ Director is appointed by the President and confirmed by the Senate. The Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the U.S. Department of Justice, and the needs of the field. The Institute actively solicits the views of criminal justice and other professionals and researchers to inform its search for the knowledge and tools to guide policy and practice.

Strategic Goals

NIJ has seven strategic goals grouped into three categories:

Creating relevant knowledge and tools

1. Partner with State and local practitioners and policymakers to identify social science research and technology needs.
2. Create scientific, relevant, and reliable knowledge—with a particular emphasis on terrorism, violent crime, drugs and crime, cost-effectiveness, and community-based efforts—to enhance the administration of justice and public safety.
3. Develop affordable and effective tools and technologies to enhance the administration of justice and public safety.

Dissemination

4. Disseminate relevant knowledge and information to practitioners and policymakers in an understandable, timely, and concise manner.
5. Act as an honest broker to identify the information, tools, and technologies that respond to the needs of stakeholders.

Agency management

6. Practice fairness and openness in the research and development process.
7. Ensure professionalism, excellence, accountability, cost-effectiveness, and integrity in the management and conduct of NIJ activities and programs.

Program Areas

In addressing these strategic challenges, the Institute is involved in the following program areas: crime control and prevention, including policing; drugs and crime; justice systems and offender behavior, including corrections; violence and victimization; communications and information technologies; critical incident response; investigative and forensic sciences, including DNA; less-than-lethal technologies; officer protection; education and training technologies; testing and standards; technology assistance to law enforcement and corrections agencies; field testing of promising programs; and international crime control.

In addition to sponsoring research and development and technology assistance, NIJ evaluates programs, policies, and technologies. NIJ communicates its research and evaluation findings through conferences and print and electronic media.

To find out more about the National Institute of Justice, please visit:

http://www.ojp.usdoj.gov/nij

or contact:

National Criminal Justice
Reference Service
P.O. Box 6000
Rockville, MD 20849–6000
800–851–3420
e-mail: *askncjrs@ncjrs.org*