Attachment B

Computer Incident Report Form

Attachment B
(Continued)

Alabama Criminal Justice Information Center
ACJIC
at the center of justice

Maury Mitchell
Director

201 South Union Street, Suite 300
Montgomery, AL 36130
334.517.2400

COMPUTER INCIDENT REPORT FORM

Instructions: Please complete each field on this form. Provide as much detail as possible. Attach additional sheets if necessary, and indicate which question you are answering on the attachment.

Reporting Agency/Section:_____ ORI:_____

Agency Point of Contact: _____ Phone:_____

Point of Contact E-Mail Address:_____

****

Date Incident Began: ____/____/____ Time Incident Began: _____ Time Zone: _____

Was this incident reported to the ACJIC Command Terminal (State ISO)? _____ Yes _____ No

Remedy Ticket # _____

Street Address of Affected System/Network:_____

Describe the systems/networks affected at your agency:_____
_____
_____

IP Address of affected machine:_____

Type of hardware (check all that were affected):
_____ Stand alone personal computer
_____ with image capabilities _____ without image capabilities
_____ Networked personal computer
_____ with image capabilities _____ without image capabilities
_____ LiveScan workstation
_____ CAD/MDT server
_____ Mainframe
_____ Other (describe):_____

Brand and Model of hardware:_____

Attachment B (Continued)

COMPUTER INCIDENT REPORT FORM (page 2)

Operating System:

____ Windows 98 ____ Windows NT ____ Windows XP ____ Windows 2000 ____ Unix

____ Other (describe):_____

List any software applications running on the affected system at the time of the incident. Include brand names and version number if known. Also indicate software patches installed:

_____

_____

_____

Describe the incident in detail. Include dates, method of intrusion, tools used by the intruder, and any other relevant information:

_____

_____

_____

_____

_____

_____

_____

Who discovered the incident? (Include full name, title, and who employed by):

_____

_____

_____

Was any ACJIC/NCIC data or images accessed by the intruder? _____ Yes _____ No

Attachment B (Continued)

COMPUTER INCIDENT REPORT FORM (page 3)

What actions were taken once the incident was discovered? Provide time when each action was taken.

Describe any damage that occurred to the system and/or network:

Were other organizations affected by this incident? If so, please list them below:

Attachment B (Continued)

COMPUTER INCIDENT REPORT FORM (page 4)

What corrective measures were taken to prevent this type of incident in the future?

Do you know the IP address, domain name, or any other identifying information of the intruder? If so, please provide all available information. Also, indicated whether you know the location of or have had any contact with the intruder.

Estimate the cost of handling this incident (manpower, additional resources, etc.)

Please provide copies of transaction logs or other evidence of this incident. If you have any questions, please contact the ACJIC Command Terminal/ Network Control Center at 1-800-392-8025.