DCJIS INFORMATION SECURITY OFFICER (ISO)

COMPUTER/INFORMATION SECURITY INCIDENT REPORT FORM

AUTHORITY: M.G.L. c. 6, § 167A and the FBI CJIS Security Policy COMPLIANCE: Mandatory;
PENALTY: Loss of access to criminal justice information systems

Agencies shall report criminal justice information system incidents to the DCJIS ISO within 48 hours in compliance with the FBI CJIS Security Policy. Please Print or Type your responses. If a question does NOT apply, enter "N / A" to signify not applicable.

Mail or Email Completed Form To: Massachusetts Department of Criminal Justice Information Services ATTN: Information Security Officer 200 Arlington Street, Suite 2200 Chelsea, MA 02150 cjis.support@state.ma.us	**For Additional Information:** FBI CJIS SECURITY POLICY **Questions / Comments:** Christopher Schreiner Phone: 617.660.4603

I. Agency Information

Point(s) of Contact (First Name, Last Name, M.I.)	Agency Name		Agency ID
Agency Address	City	State	Zip Code
Work Phone Number	Email Address		
Date of Report	Date of Incident		

II. Incident Information

Location(s) of Incident:
System(s) and/or Data Affected (e.g., CAD, RMS, File Server, etc.):
Method of Detection:
Nature of Incident:
Incident Description:
Actions Taken / Resolution:

III. Incident Report

1. How was the incident discovered? (e.g. via an audit trail, or accidental discovery)

2. What applications, systems and/or data were accessed? Did access include any personally identifying information or criminal justice information? Is the hard drive encrypted? Provide a description / list as to who you believe is affected or vulnerable to a similar incident.
3. When did the incident occur? Identify the time-frame and the operational phase (i.e., Was this a one-time occurrence or continuing? Could it occur anytime or do certain events trigger it?)
4. Why did this incident happen? What allowed this incident to occur? Were there policies in place which may be applicable to this incident? Should there be controls in place which may help to prevent this type of incident from reoccurring?
5. What are the vulnerabilities and impacts associated with this incident? Describe what you believe are the vulnerabilities and impacts to other information systems as a result of this incident.