



AGENDA REPORT

Meeting Date: January 22, 2009
Item Number: E-5
To: Honorable Mayor & City Council
From: David L. Snowden
Subject: **RESOLUTION OF THE COUNCIL OF THE CITY OF BEVERLY HILLS
APPLYING FOR THE NATIONAL INSTITUTE OF JUSTICE FY 2009
ELECTRONIC CRIME AND DIGITAL EVIDENCE RECOVERY
TECHNOLOGY GRANT**

Attachments:

1. Resolution
2. Concept Paper for Grant Application

RECOMMENDATION

It is recommended that the City Council adopt the resolution approving the application for the FY 2009 Electronic Crime and Digital Evidence Recovery Technology grant.

INTRODUCTION

The National Institute of Justice (NIJ) is the research, development, and evaluation agency of the U.S. Department of Justice (DOJ) and a component of the Office of Justice Programs (OJP). NIJ provides objective, independent, evidence-based knowledge and tools to enhance the administration of justice and public safety. NIJ solicits applications to inform its search for the knowledge and tools to guide policy and practice.

NIJ is seeking applications for funding to research, develop, and demonstrate emerging digital evidence recovery technology solutions for law enforcement agencies. Specific areas of interest include cell phone forensics tools, digital evidence forensic examination tools, and computer crime investigative tools.

DISCUSSION

In 2008, the Police Department established a Computer Forensic Unit. The purpose of this unit is to provide investigative expertise for high tech crimes and assistance to other

Meeting Date: January 22, 2009

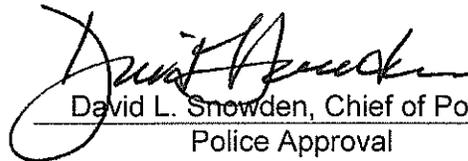
investigators working with digital evidence. The department would like to expand the tools available to law enforcement agencies and its role as a leader in the investigation of technology crimes in the region. If awarded, the grant will assist the Computer Forensics Unit in the creation of a law enforcement database to triage and examine cellular phones and attached storage devices.

FISCAL IMPACT

The proposed concept that is being submitted to NIJ includes the procurement of consulting services to examine cellular phone devices and develop a law enforcement database and purchase related equipment. The proposed project costs total \$535,000 and would be funded by the granting agency.



Scott G. Miller, Director
Finance Approval



David L. Snowden, Chief of Police
Police Approval

RESOLUTION NO. 09-R-

RESOLUTION OF THE COUNCIL OF THE CITY OF BEVERLY HILLS
APPLYING FOR THE NATIONAL INSTITUTE OF JUSTICE FY 2009
ELECTRONIC CRIME AND DIGITAL EVIDENCE RECOVERY
TECHNOLOGY GRANT

The Council of the City of Beverly Hills does hereby resolve as follows:

Section 1. The National Institute of Justice administers the Electronic Crime and Digital Evidence Recovery Technology grant program.

Section 2. The City Council hereby appoints the City Manager or his designee to apply for and, if awarded, accept the FY2009 Electronic Crime and Digital Evidence Recovery Technology grant program to assist with funding purchases for the Police Department's Computer Forensics Unit. Upon award to the City, the City Manager or his designee is also authorized to execute and submit all documents including, but not limited to, applications, agreements, amendments, and payment requests, which may be necessary for administration of the FY2009 Electronic Crime and Digital Evidence Recovery Technology grant.

Section 3. The City Clerk shall certify to the adoption of the Resolution and shall cause the Resolution and his certification to be entered in the Book of Resolutions of the Council of the City.

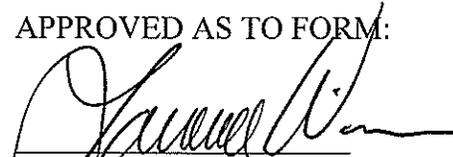
Adopted:

BARRY BRUCKER
Mayor of the City of
Beverly Hills, California

ATTEST:

_____(SEAL)
BYRON POPE
City Clerk

APPROVED AS TO FORM:



LAURENCE S. WIENER
City Attorney

APPROVED AS TO CONTENT:

RODERICK J. WOOD
City Manager



SCOTT G. MILLER
Director of Administrative Services/
Chief Financial Officer



DAVID L. SNOWDEN
Chief of Police

Electronic Crime and Digital Evidence Recovery Grant Concept Paper

Our goal is to improve the quality, efficiency and number of cell phone investigations as well as push some acquisitions to line level officers and detectives; current practices make this difficult. Many devices are easy to use but do not acquire the information needed by investigators. In order to give line level personnel the ability to make a triage-based assessment, they need an easily accessible database which will guide them on the proper procedures for dealing with a specific phone while in the field. This grant could significantly assist law enforcement agencies with identifying the most appropriate forensic course of action based on the nature of the investigation, time & legal constraints, information obtainable, needed forensic application and level of technical expertise required for the acquisition.

Table of Contents

Subject	page
Concept	3
Purpose, Goals and Objectives	4
Research Design and Methods	5
Implications for Criminal Justice Policy and Practices in the United States	6
Managing/Staffing Plan and Organization	7
Dissemination Strategy	8
Funding Estimate	9
Research Calendar	10

Concept

The Beverly Hills Police Department began the formation of a local High Technology Crime Unit in 2005 in order to meet the growing needs of our Community and specifically our Detective Bureau. Over the last two years the High Tech Crime Unit has formalized its existence in the Department as well as extended its services to other area agencies in order to enhance inter-agency cooperation.

Additionally, we maintain a formal relationship with the Southern California High Tech Task Force. However, we have our own Digital Forensic Lab, with a new lab currently under construction. This new High Tech lab is being designed to support multiple law enforcement agencies on the Westside of Los Angeles and all infrastructure costs are being absorbed by the City of Beverly Hills. Our agency has worked cases for multiple Law Enforcement agencies to include the City of Beverly Hills, Santa Monica, West Hollywood, Culver City, Los Angeles, University of California at Los Angeles and the Drug Enforcement Agency. Upon completion of our new facility in the spring, we have agreements to house Detectives from Beverly Hills, Santa Monica and Los Angeles County Sheriff's in support of their respective agencies. Additionally, we are pursuing formal agreements to support Culver City and the UCLA Police Department.

In order to improve both the quality and level of service provided to our participating agencies, the Beverly Hills High Technology Crime Unit would like to focus research and development on the most prevalent digital device we encounter, cell phones. One of the biggest challenges for law enforcement in processing cell phones is the lack of a central catalog system that addresses which current hardware or software forensic solutions are best suited in acquiring information for any specific unit. Often times it is difficult to consolidate vendor claims with the reality of the results. By establishing a user-friendly SQL database which incorporates proven methodologies and results, law enforcement personnel at every level would have an unbiased working guide in processing cell phone (and similar) technology.

Our goal is to improve the quality, efficiency and number of cell phone investigations as well as push some acquisitions to line level officers and detectives; current practices make this difficult. Many devices are easy to use but do not acquire the information needed by investigators. In order to give line level personnel the ability to make a triage-based assessment, they need an easily accessible database which will guide them on the proper procedures for dealing with a specific phone while in the field. This grant could significantly assist agencies with identifying the best all around (or multiple) cell phone forensic tool. Additionally, an officer will be able to make a more timely determination as to the most appropriate forensic course of action based on the nature of the investigation, time & legal constraints, information obtainable, needed forensic application and level of expertise required.

In as much, the establishment of the described database catalog system would greatly assist trained forensic units in dealing with the overwhelming number of phone types and technologies that law enforcement currently addresses in attempting to preserve digital evidence.

Purpose

The purpose of this research is to provide local and state law enforcement officers with a detailed technical database which can be accessed and updated in order to both improve and support the investigation of cell phone devices and their attached storage.

Goals

Create a regional cellular telephone forensic acquisition database which can be accessed and provided to all law enforcement personnel. The database will provide appropriate guidance to the officers seizing the device such as how to deal with acquiring the contents, solutions to password protected devices, and what tool should be used based on the information required from the device.

Objectives

Create an SQL database accessible via web interface and available to all law enforcement personnel over a secure network.

Test a large number of commercially available cellular phone forensic tools using real cases and subsequently catalog the acquisition results in the newly created SQL database.

Determine which commercially available cell phone forensic software provides the best combined ease of use and acquisition capability by device.

Train officers and investigators from multiple Los Angeles County agencies to use the cell phone acquisition database and one or two primary cell phone forensic tools.

Determine the productivity improvements based on how many devices are acquired and whether acquisitions and reports are successfully conducted by trained field officers and investigators or High Tech Crime Unit Examiners.

Eventually, allow other Los Angeles area High Tech Crime Units and Digital Forensic Labs to manipulate and improve research data.

Use the results of this research to improve commercially available cell phone acquisition software and hardware by sharing results with the manufacturers on the performance of their equipment.

Improve the acquisition of small device (non cellular) digital devices attached to cell phones, such as mini and micro SD cards.

Specifically catalog those existing acquisition tools which will conduct physical acquisition of cellular phones, and on what phones, in an attempt to improve the recovery of deleted items.

Research Design and Methods

This requires a disciplined multi-phase approach beginning with database development.

Phase I: This will include the research and use of existing private cell phone forensic databases and interview of law enforcement personnel to determine the best database structure to meet their needs (line and investigatory). Additionally, include comments and suggestions from other area High Tech Units, Digital Forensic Labs, and High Tech Task Forces.

Phase II: Development and testing of the web based cell phone acquisition database. Purchase and testing of commercially available cell phone forensic software. In addition, work out data connectivity issues between other county law enforcement agencies either through the use of existing memorandums of understanding or by creating new agreements and new data connections.

Phase III: Many of these tools are currently available in our High Tech Crime Unit and will be supplemented for research purposes. This is a prolonged phase driven by the case load of multiple area agencies requiring cell phone forensics. During this phase, two assigned High Tech Examiners will receive and acquire cell phones on multiple devices and test the results. These results will be cataloged and recorded for entry into database entry.

Phase IV: Fielding and implementation of appropriate cell phone forensic equipment for use by law enforcement personnel. During this phase a selection will be made on what tools to assign non-forensic lab personnel. Training will be conducted on how to acquire devices and access and search the cell phone forensic database.

Phase V: Evaluation and remediation will be conducted based on the fielding data that could either change the makeup of the database or perhaps the tools available to law enforcement personnel.

Implications for Criminal Justice Policy and Practice in the United States

The proper collection and dissemination of cell phone forensic tool data can be used to help law enforcement agencies determine the best tools to use for a specific cell phone. As new devices are introduced to the market, they would be evaluated, added to the database and if Forensic Tool manufacturers wanted to improve capabilities, their specific results could be provided to improve product performance.

The end result would be a detailed comprehensive database available primarily to law enforcement. This database would then point investigators and examiners to the best forensic tool, saving time and improving the quality of acquisitions. In addition, more investigations could be conducted at the line level relieving the burden on a centralized High Tech Crime Lab. High Tech Crime Labs would consequently be able to focus on more complex situations and devices.

Management/Staffing Plan and Organization

The current High Tech Crime Unit and lab organization would remain unchanged. We currently have three sworn Investigators/Examiners, one sworn supervisor. To support the program, the City of Beverly Hills would additionally hire consultants to conduct cellular phone examinations and data entry. Additionally, the Police Department is exploring the feasibility of hiring an additional civilian Computer Forensic Examiner to support the High Tech Crime Unit. Furthermore, the Police Department is aggressively encouraging other regional law enforcement agencies to join our High Tech Crime Unit.

An outside contractor would be hired to assist with design, development and refinement of the database. Additional equipment costs would be required such as a dedicated server, a network infrastructure related to the database and additional cell phone forensic tools not currently in our inventory.

The assigned High Tech Crime Unit Supervisor will be the primary manager of the grant and be responsible for effective development and implementation at all phases.

Dissemination Strategy

The dissemination process is foreseen as being a secure, web-based interface that is accessible to all authorized law enforcement personnel. In this manner, the required updates and database improvements can be administered centrally while providing users the most current forensic solutions.

Funding Estimate

Funding will be based on a two year program and include the following costs:

Federal Funding Request

Year One

Contract Forensic Examiners	\$140,000
Cell Phone Forensic Solutions	\$80,000
Database Development Costs	\$80,000
Total Year One Costs:	\$300,000

Year Two

Contract Forensic Examiners	\$140,000
Deployable Forensic Cell Phone Equipment	\$65,000
Database Refinement Costs	\$30,000
Total Year Two Costs:	\$235,000

Total Federal Funding Requested to Support Program: \$535,000

Research Calendar

Phase One (4 month period)

- Includes hiring of contract forensic examiners
- Research into existing cell phone forensic databases
- Research of available cell phone forensic tools
- Concept of database design

Phase Two (6 month period)

- Development and testing of web-based cell phone acquisition database
- Purchase cell phone forensic solutions
- Manual collection of datum related to cell phone acquisitions
- Research data connectivity solutions to allow partnering agencies access

Phase Three (6 month period)

- Data entry of pre-existing collected data
- Direct data entry into established database (multi-agency)
- Deployment of field mobile solutions (single agency for testing)

Phase Four (4 month period)

- Deployment of field mobile solutions (multi-agency)
- Training of field personnel

Phase Five (4 months)

- Evaluation and remediation period
- Database redesign as required
- Mass distribution of deliverable