Item #48

SEMINOLE COUNTY GOVERNMENT
AGENDA MEMORANDUM

SUBJECT: National Institute of Justice (US Department of Justice / Office of Justice Programs) Grant Application for Electronic Crimes–Research & Development

DEPARTMENT: Sheriff's Office **DIVISION:**

AUTHORIZED BY: Sheriff Eslinger **CONTACT:** Penny Fleming **EXT.** 6617

Agenda Date 1/13/04 **Regular** ☐ **Consent** ☒ **Work Session** ☐ **Briefing** ☐
Public Hearing – 1:30 ☐ **Public Hearing – 7:00** ☐

MOTION/RECOMMENDATION:

Approval by the Board of County Commissioners for the submission of the white paper/grant application by the Sheriff.

BACKGROUND:

The US Department of Justice/Office of Justice Programs, through the National Institute of Justice has made available funds for the research and development of electronic crimes investigative tools. The Seminole County Sheriff's Office would like the opportunity to compete for those funds by making a white paper proposal for about $215,000. This request will cover the cost of an additional investigator, the cost of purchasing the necessary equipment and any training needed to perform the R&D. There is no required match for these funds. The entire grant application is submitted on-line via the Internet. The white paper being submitted is attached.

Reviewed by:
Co Atty:
DFS: C. Hunter
Other:
DCM:
CM:
File No. CSHO01

MEMORANDUM: OFFICE OF THE SHERIFF 1703-04-002

TO: Kevin Grace, County Manager

FROM: Penny J. Fleming, Chief, Administrative Services

DATE: December 30, 2003

SUBJECT: Board of County Commissioners Grant Approval Request

---

The Seminole County Sheriff's Office is requesting the approval to begin an application process for a solicitation from the National Institute of Justice (US Department of Justice/Office of Justice Programs) for a grant for Electronic Crimes – Research and Development. The first part of the process is to submit a white paper to the National Institute of Justice explaining our proposed project. This is the first time we are applying for this funding and we are requesting the Board of County Commissioners to consider the approval for the submission of this white paper to begin the application process. As in some previous Office of Justice applications, the application is only available electronically through their web site.

If awarded this grant, there is no required match. We are seeking about $215,000 to cover the cost of 1 investigative position, the purchase of all the necessary equipment to perform associated research and development, and any required training. This grant will enable advanced technology to be acquired and continue to allow our county to be on the cutting edge of electronic/computer crime investigative technology.

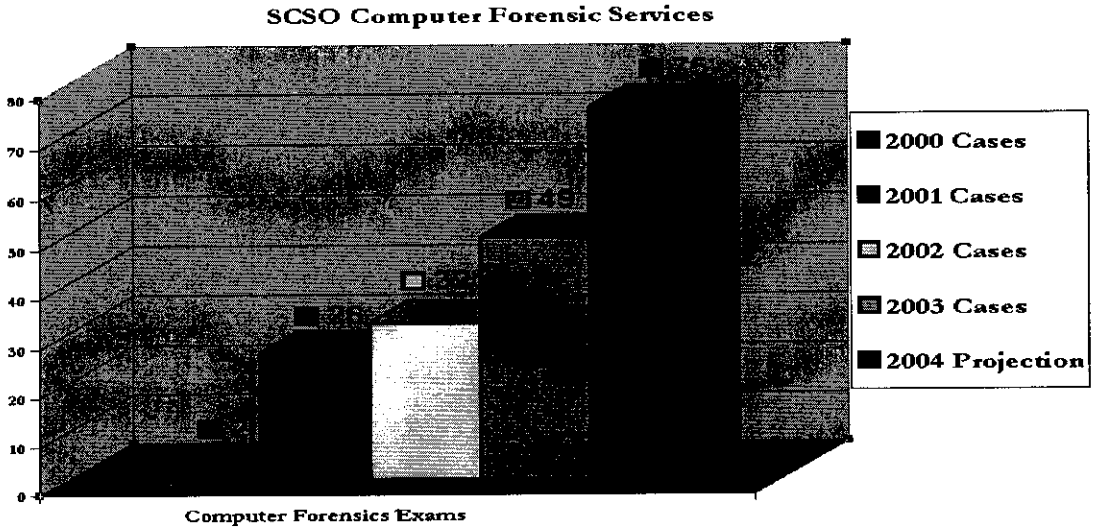
It is respectfully requested that the Electronic Crime Research & Development white paper/application item be placed on the agenda for the Board of County Commissioners meeting on Tuesday, January 13, 2004.

If you have any questions regarding this agenda item, please contact Chief Penny Fleming at 665-6617 or Rob Forlini at 665-6536.

C: Lisa Spriggs
Director of Fiscal Services

Seminole County Sheriff's Office
Electronic Crime Research and Development

Seminole County is located north of Orlando in Central Florida with a total population of approximately 374,000. Although Seminole County has always been a bedroom community to Orlando, we are home to many "high tech" businesses that have sprung up along the Interstate 4 "Technology Corridor" which spans from Tampa, through Seminole County, to Daytona Beach. These businesses have brought residents that are very comfortable using home and business computers in their daily lives. Across the nation, this trend is growing as computer use has become an integral part of many people's daily lives. In 2000, the Seminole County Sheriff's Office began offering computer forensics services to our personnel and all seven municipal agencies in Seminole County. Since then, the demand for computer forensics services has risen to such an extent that we also examine cases for the United States Secret Service, the Drug Enforcement Administration, the Federal Bureau of Investigations, the Florida Department of Corrections, and other Central Florida law enforcement agencies. In 2001, we examined computer systems and storage media from twenty-six criminal investigations. In 2003, we examined 88% more cases than in 2001, and we continue to experience an increasing demand for computer forensic services on a daily basis. Our projections for 2004 clearly show this trend.



The Seminole County Sheriff's Office recognizes that research and development of new and innovative solutions coupled with proper testing and validation is vital to the success of computer forensic services and digital evidence recovery. Our computer forensic examiners earned the Certified Forensic Computer Examiner (CFCE) certification from the International Association of Computer Investigative Specialists (IACIS), and they have obtained additional certifications and/or attended numerous basic and advanced training courses focusing on computer forensic examinations and digital evidence recovery. They are heavily involved with private and public organizations throughout the computer forensic community through various organizations such as IACIS, HTCN, CFTT, and FACCI. Through these organizations and other partnerships, the Sheriff's Office is well informed of new problem areas for examiners and new products that aid as solutions.

With traditional computer forensic procedures, examiners normally power-off computer systems, remove the hard drive or other media, and forensically acquire a bit-stream image or exact copy of the subject media. However, as new operating systems and software applications emerge that support encrypted file systems or the ability to encrypt a volume, the ability to access data is diminished once the computer system is powered off as the data is now in the encrypted state. For example, Jetico, Inc. sells "Best Crypt" which is an encryption application that allows the user to encrypt the contents of a volume (ie: the C: volume) into a container. If the examiner does not have the password to access the volume once powered off, data recovery is nearly impossible. In addition to data encryption, examiners are encountering networked computer systems that cannot be powered off such as file servers, web servers, or other computer systems running server-based operating systems like Microsoft Windows Server family or UNIX. Powering off business servers or critical enterprise systems may not granted by the court

and/or may result in the business's loss of revenue due to the termination of services. In this case, examiners would resort to traditional means of recovering the data such as logical file copies from the subject computer systems. This procedure, although sometimes necessary, is not a forensically sound solution. Examiners must obtain a bit-stream image of the media devices, whether simple or complex, such as disk arrays or dynamic disks, in order to access all areas of the media to ensure that all areas of the media are examined (slack space, unallocated clusters, non-partitioned area, etc.).

Guidance Software, Inc. recently released a software solution called the Encase Field Intelligence Model, or FIM, which is an investigative solution available only to law enforcement, government, and military personnel. Encase is a common application utilized by thousands of law enforcement agencies throughout the world. The Seminole County Sheriff's Office uses Encase Forensic Edition as one of our primary tools for examinations. The Field Intelligence Model (FIM) allows the examiner to connect to the subject computer via a TCP/IP network connection, whether a single computer or numerous computers connected to a network. This connectivity provides the examiner with the ability to triage the media by running keyword searches, file signature analysis, folder/file copies, and other functions that are important at the crime scene without having to power off the computer system. Moreover, the FIM provides the examiner the ability to obtain a bit-stream image or exact copy of physical or logical devices via the network connection. This new and innovative software solution is critical in situations where the computers are powered on, whether networked or not, but the volume is encrypted or the computer cannot be powered off as previously stated in this paper. The FIM also provides the examiner with the ability to capture running processes, obtain a bit-level copy of physical memory, and document open network ports.

The Seminole County Sheriff's Office recognizes the Encase Field Intelligence Model as necessary solution to address complex crime scenes that law enforcement computer forensic examiners will encounter as new technologies arise and are used by victims or suspects. Therefore, we propose the following goals and objectives in researching this new product.

1. Validate the components of the FIM will integrate into a wide area network, local area network, or standalone computer system and establish network communication with the examiner's computer system.

2. Validate the FIM will "preview" or "triage" computer media at the bit level, via the network connection, and will view specific areas of the physical media such as slack, system area, unallocated space, etc.

3. Validate the FIM will acquire removable media, fixed disks, or other complex disk arrays (RAID volumes or dynamic disks), whether physical or logical, under common operating systems.

4. Test common retail or commercial encryption software suites on computer systems with different operating systems and different disk configurations with the FIM software in a network environment or standalone computer.

5. Deploy the FIM during testing or at actual crime scenes as an available computer forensics tool and document "real world" use of the product with other computer forensics hardware and software.

Presently, there are two computer forensic examiners employed by the Seminole County Sheriff's Office who have the training and technical expertise to perform examinations and fulfill the goals of this program. One is a sergeant who supervises the Economic & Computer Crimes Unit while the second works fulltime on computer forensic examinations and internet frauds. As evidenced with our rising caseload and current backlog, it is impossible for him to work on the goals and objectives of this program. To ensure the program requirements are met and achieve maximum results for the testing of the FIM, the Sheriff's Office requests funding for one fulltime investigator/computer forensic examiner at approximately $60,500 (salary and benefits).

In addition to funding one computer forensics examiner, the Sheriff's Office requests funding for equipment, software, and operating expenses. We will purchase two licenses of the Encase Field Intelligence Model with all available modules for Encase. This will ensure simultaneous testing of target computer systems and cross-validation between the examination systems as well. The Sheriff's Office will purchase a server rack populated with various modules to include high capacity RAID arrays, various hard drives for different operating systems, and components to forensically examine each testing phase. The server will provide an ideal platform to test and validate various operating systems and basic to advanced disk configurations while serving as the central repository for test sessions. In addition, we will purchase desktop and laptop computers as test machines. A portable forensics computer will facilitate field testing of the FIM and will be accompanied with a large storage array for examining and acquiring test computers via our local or wide area networks and the internet as well. Finally, we will purchase forensic, encryption, utility, and general software titles for test and examination computers. To minimize grant expenditures, we will utilize the existing computer forensics laboratory and equipment located at the Seminole County Sheriff's Office.

Programmatic Activities, Tasks, and Estimate of Funding

ACTIVITY	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Cost Estimate
Funding for one Investigator / Computer Forensic Examiner	X	X	X	X	X	X	X	X	X	X	X	X	**$60,500**
Purchase Equipment and installation/configure software	X	X											**$149,340**
Attend FIM software 5-day training course	X												**$3,500**
Test FIM integration into TCP/IP networks		X	X	X									**N/A**
Test and validate acquisition of computer systems with FIM			X	X	X	X	X	X	X	X	X	X	**N/A**
Test and validate preview features of live media with FIM				X	X	X	X	X	X	X	X	X	**N/A**
Test and validate preview / acquisition of RAID & dynamic disk arrays with FIM					X	X	X	X	X	X	X	X	**N/A**
Test and validate preview / acquisition of encrypted volumes with FIM							X	X	X	X	X	X	**N/A**
Field testing and crime scene deployment		X	X	X	X	X	X	X	X	X	X	X	**N/A**

The Seminole County Sheriff's Office believes our technical expertise in the area of computer forensics and related solutions will greatly enhance the overall results of this project. We believe the goals and objectives as outlined represent key concerns for the computer forensics community by addressing digital crime scenes in a networked environment or encrypted volumes. Testing the FIM on standalone or networked computer systems, computers utilizing certain levels of volume encryption, and advanced file servers with complex disk arrays is key to ensuring the capabilities of this product are validated for practitioners in computer forensics. This is the only forensic solution available to examiners at this time which has the ability to address complex crime scenes such as those we have outlined above. However, without proper testing and validation of the FIM, the criminal justice community must rely upon Guidance Software's claims regarding this software. We propose to thoroughly test and validate the capabilities and potential deficiencies of the FIM in a real-world environment. Finally, we will report our findings to the computer forensics community so that they may benefit from our research.