7a - District Attorney High Tech Crime Unit Expansion

1. **Program Area:**
   PUBLIC PROTECTION

2. **Agencies and Departments involved:**
   Office of the District Attorney

3. **New or previously identified in earlier Strategic Financial Plans, if previously identified, what has changed and why:**
   The Office of the District Attorney has combined the High Tech Crime Unit and the Identity Theft Strategic Priorities previously approved by the Board of Supervisors since identity theft crimes tend to fall under the category of high tech crimes. As these types of crime continue to rise, there is a growing need to expand this unit.

4. **Description of the project/program - what it is and what it will achieve:**
   With the proliferation of computers, cell phones, PDAs (Personal Digital Assistants) and the growth of the Internet, cyber-crime is on the rise both nationwide and in this county. Many felony cases require police agencies to search computers, cell phones, PDA's or other electronic devices to uncover evidence of crime. It is unfortunate but true that the criminals engaged in sophisticated crimes often have access to better equipment than the agencies that investigate them. The ability to obtain and analyze evidence obtained from electronic devices varies from police agency to police agency. Television programs create an expectation in the minds of jurors that a wide range of technical and electronic testing is available in all criminal cases, the so-called CSI effect. These issues require the Office of the District Attorney to invest in technical advances, trained personnel and equipment to be successful in prosecuting 21st century criminals. The Orange County District Attorney High Tech Crime Unit, established in 2005, is addressing the issues involved in high technology crimes by providing trained personnel and equipment to successfully obtain evidence from the electronic and digital devices commonly used by criminals, to analyze the information and have sufficient expertise to testify in court on these matters. The need for the Office to expand and train attorneys and investigators specializing in the vertical prosecution of high tech crime cases will continue.

   Orange County is a center for high tech entrepreneurial activity of all kinds and is a target for those who seek to profit criminally by using sophisticated means to victimize companies and individuals. Southern California has long been known as the fraud capital of the United States. Demographics in Orange County create a target rich environment for fraud criminals, combining vulnerable populations such

as seniors and recent immigrants with a dense and mobile population base and large numbers and varieties of businesses.

Many types of crimes can fall within the ambit of high tech crime:

Identity Theft:
There is much attention focused on the issue of identity theft, which is the fastest growing area of criminal fraud. The problem is enormous, and is likely to continue to grow larger as our residents continue to become more technology dependent. Identity theft exists at many levels, from unsophisticated persons who steal credit cards and use them all the way to sophisticated criminal rings that harvest personal information from databases for use and sale. This information can translate into fraudulent real estate purchases, theft from merchants and businesses, and destruction of a victim's financial holdings. It can also turn into large dollar losses for credit card companies, banks and businesses that must pass the costs on, increasing the cost of goods and services for county residents. Sophisticated or simple, tracking down these criminals is difficult and requires extensive, time consuming investigation as well as use of high tech tools such as forensic analysis of digital devices and the use of forensic accountants to track the flow of money through bank accounts. In order to keep up with the increased reporting and investigation of identity theft crimes, additional investigative personnel, attorneys, accountants and computer forensic personnel need to be added and countywide law enforcement resources such as databases and investigation groups are contemplated. Paraprofessionals such as paralegals and investigative assistants are valuable in saving time for sworn personnel and prosecutors.

Criminal Fraud:
Each major fraud activity such as investment fraud, real estate fraud, embezzlement, medical insurance fraud, Workers' Compensation fraud and identity theft involves the use of sophisticated technology to perpetrate the fraud. Many cases have hundreds of victims and millions of dollars in loss. In Orange County, the number of cases in which losses exceed $100,000 is growing quickly. In one recent case, $96 million in fraudulent health insurance billings were generated in an eight-month period. Each fraud case requires multiple search warrants of computer and bank accounts as well as sophisticated computer forensic analysis. The common use of computerized accounting systems requires high-level forensic and financial analysis. It is not unusual for an employee embezzlement to involve more than $1 million dollars in loss to the employer. Often, criminals prey on the elderly or vulnerable using schemes to mislead and confuse them into fraudulent investments. In one recent case, there were more than 150 victims defrauded by the same defendant. Funding of forensic computer analysis and forensic accountants, as well as attorneys, investigators, paralegals and investigative assistants provides the

District Attorney a high tech arsenal to even the playing field with sophisticated criminals.

Large-scale fraud has actually become easier with the widespread use of electronic communications and computerized accounting. The use of computerized information in businesses ensures that identity thieves will target them as rich sources of victim information. In one recent case, 70,000 names with identifying information were downloaded from the records of a large Orange County business by an IT employee. Fraudulent transfers of funds, counterfeit checks, investment fraud, theft of confidential information, intellectual property and trade secrets, laundering of illegal profits through computer networks and electronic banking transfers are a few examples of crimes that have become easier to commit in our digital society. Computers have also made it easier to hide, cover up, or detect the crimes.

Gang Crime:
Computers, PDA's and cell phones have become common communication devices for criminal street gangs. Some gangs have become deeply involved in identity theft, while others use communication devices to identify potential rivals or to identify targets for theft or robbery. Many street gang members who are apprehended have digital or electronic devices that need to be searched for evidentiary information. In some cases, photos from cell phones have been used to prove gang-related crimes. The increased use of technology by street gang members requires additional personnel for the analysis of this type of evidence.

Child Pornography/Sexual Assault:
Forensic analysis of computers has been the most important tool in identifying those who traffic in the exploitation of children through child pornography. Pedophiles frequently use the Internet, including instant messaging features to troll for victims, often misrepresenting themselves as children or computer game enthusiasts. The process of analyzing computers to uncover this evidence is extremely complex and time consuming. The proliferation of child pornography among sexual predators will require more specifically trained investigators and computer forensic analysts. Pending legislation increasing the penalties for possession of child pornography will increase the number of cases referred to the District Attorney for prosecution.

Serious and Violent Crimes:
When search warrants are executed in all kinds of crimes, including homicide, drug trafficking and domestic violence, it is common to search for materials on home computers, PDA's, cell phones and other electronic devices. This material can be critical in providing evidence necessary for successful prosecution. The number of these types of searches has increased dramatically in the past few years to the point that nearly every serious felony has some warrant activity related to technological

devices. Even non-theft cases can require sophisticated accounting or computer analysis to prove an element of the case such as identity or intent. As an example, the notorious BTK killer in the Midwest was identified based on computer forensic analysis of coding recovered from a CD that he had mailed to a news agency. The coding led to identification of the killer from library computer passwords.

Criminals of all kinds seek out vulnerable victims using the Internet and capitalizing on the relative anonymity of the cyber-world. Web sites exist to mislead people about investments, to "phish" (illegally obtaining identifying data over the Internet), and to prey on children. Stalkers use the Internet to locate and track their victims and then to threaten their victims at their homes and workplaces. Because these criminals are faceless, proving the crimes requires resources to pay for updated equipment, hardware, software and personnel who have computer forensic, accounting and prosecution skills beyond that of the typical police investigator or prosecutor.

Criminal Trials:
There is an increased need for sophisticated investigative tools in criminal trials and a high cost associated with hiring outside expert witnesses to perform these tasks. Some examples of work that can be done internally in a high tech unit without hiring outside experts would be reviewing and enhancing video/audio footage, analyzing and preserving information in digital devices, seizing and reviewing financial data and bank records as well as testifying in court as persuasive witnesses in these areas. Many outside experts charge in excess of $300 per hour, so maintaining an adequate staff of forensic accountants and forensic computer analysts to do these tasks is cost effective and provides prosecutors with a quality and timely source of analysis and information. Quick access to this type of evidence will result in a greater ability to successfully prosecute these crimes, bring the criminals to justice, seize assets from them and hold them to repay the victims, and in some cases recoup the cost of investigation.

5. Personnel - will the program/project require additional staffing? If so, estimate number of positions:

In the last two years, the District Attorney High Tech crime staff has experienced an enormous workload increase of over 290%.

High Tech Crimes Unit - Data Processed

Year	Amount of Data
2000	845.97 gigabytes
2001	2.198 terabytes*
2002	3.488 terabytes
2003	8.60 terabytes

* A terabyte is 1,000 gigabytes

The High Tech Crime workload is anticipated to continue growing.

We propose to add the following staff in each year:

FY 2006/2007: 2- Senior Deputy District Attorneys, 2- Investigators, 2- Paralegals, 2- Investigative Assistants, 2- Computer Forensic Technical System Specialists, 1- Forensic Accountant, 1- Office Services Staff

FY 2007/2008: 1- Senior Deputy District Attorney, 2- Investigators, 1- Supervising Attorney's Investigator, 1- Paralegal, 1- Investigate Assistant, 2- Computer Forensic Technical System Specialists, 1- Forensic Accountant, 1- Office Services Staff

FY 2008/2009: 1- Senior Deputy District Attorney, 2- Investigators, 1- Paralegal, 1- Investigative Assistant, 2- Computer Forensic Technical System Specialists, 1- Forensic Accountant, 1- Office Services Staff

6. Cost - estimate and identify costs:
Please refer to the attached spreadsheet for cost information.

7. Potential Funding Sources:
We continue to explore a variety of public funding sources, at the State and Federal level. To date we have received a one-time $100,000 state grant for equipment. In addition, the Board of Supervisors approved earmarking Federal Southwest Border Prosecution Initiative Funds associated with the prosecution of federally referred/declined cases to fund this initiative. The private sector would likely assist, but legally we are prohibited by conflict of interest provisions which would prevent us from accepting funding from a private source such as a victim or business group. Funding of that nature would result in recusals of the District Attorney's Office.

Please refer to the attached spreadsheet for funding information.

8. Community Awareness (stakeholders):
Orange County residents and local law enforcement agencies.

9. Mandated or discretionary:
Prosecution of fraud is mandated by the California Penal Code.

10. Implementation period if funding were available:
Program has already been implemented.

7a - District Attorney High Tech Crime Unit Expansion											
	FY 05-06	FY 06-07	FY 07-08	FY 08-09	FY 09-10	FY 10-11	FY 11-12	FY 12-13	FY 13-14	FY 14-15	FY 15-16
I. Cost											
One-Time Costs											
Network Forensic Storage	0	80,000	20,000	50,000	60,000	20,000	0	20,000	0	20,000	0
Agency One-Time Cost Total	**0**	**80,000**	**20,000**	**50,000**	**60,000**	**20,000**	**0**	**20,000**	**0**	**20,000**	**0**
Total Cost											
Salaries & Benefits	0	1,275,872	2,453,277	3,470,336	3,521,428	3,549,076	3,549,076	3,549,076	3,549,076	3,549,076	3,549,076
Services & Supplies	0	262,096	321,996	495,500	358,500	368,500	261,500	368,500	261,500	368,500	261,500
Fixed Assets	461,200	80,000	20,000	50,000	60,000	20,000	0	20,000	0	20,000	0
Agency Ongoing Cost Total	**461,200**	**1,617,968**	**2,795,273**	**4,015,836**	**3,939,928**	**3,937,576**	**3,810,576**	**3,937,576**	**3,810,576**	**3,937,576**	**3,810,576**
Agency Cost Total	**0**	**1,617,968**	**2,795,273**	**4,015,836**	**3,939,928**	**3,937,576**	**3,810,576**	**3,937,576**	**3,810,576**	**3,937,576**	**3,810,576**
II. Non-General Fund Revenue											
No Revenue	0	0	0	0	0	0	0	0	0	0	0
Agency Revenue Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
III. General Fund Requirement	**461,200**	**1,617,968**	**2,795,273**	**4,015,836**	**3,939,928**	**3,937,576**	**3,810,576**	**3,937,576**	**3,810,576**	**3,937,576**	**3,810,576**
IV. Staffing											
Investigative Assistant, DA	0	2	3	4	4	4	4	4	4	4	4
Investigative Auditor, DA	0	1	2	3	3	3	3	3	3	3	3
Investigator	0	2	4	6	6	6	6	6	6	6	6
Office Assistant	0	1	2	3	3	3	3	3	3	3	3
Paralegal	0	2	3	4	4	4	4	4	4	4	4
Senior Deputy Attorney	0	2	3	4	4	4	4	4	4	4	4
Supervising Attorney's Investigator	0	0	1	1	1	1	1	1	1	1	1
Technical Systems Specialist	0	2	4	6	6	6	6	6	6	6	6
Agency Position Total	**0**	**12**	**22**	**31**	**31**	**31**	**31**	**31**	**31**	**31**	**31**