2008 High Technology Crime In California: Annual Report to the Governor & Legislature

Letter from the High Technology Crime Advisory Committee Chairman

Dear Governor Schwarzenegger, Senate President pro Tem Darrell Steinberg, and Speaker of the Assembly Karen Bass:

High technology is one of California's most important industries, yet it stands vulnerable to a dangerous new breed of criminals. California has in place a vital, thin digital line of protection for our citizens and industries. This thin digital line is the California High Tech Task Force and we file this annual report at a critical juncture. The California High Tech Task Force operates under a program administered by the California Emergency Management Agency (CalEMA) with strategic oversight, guidance, and planning provided by the High Technology Crime Advisory Committee (HTCAC), which is composed of state and local government officials and representatives from all segments of the state's high technology industry.

As the financial crisis deepens in our state and country, our representatives are called upon to make difficult choices amongst competing interests. Without protection from cyber crimes, our vital businesses will suffer even more and exacerbate the financial crisis. Cyber-thieves exploit the Internet to strike anonymously at unwary participants in online commerce. Counterfeiters bleed the profits out of our software development, entertainment, and electronic game industries. Intellectual property thieves deprive companies and shareholders of the fruits of millions of dollars spent on research and development. The purveyors of computer "viruses," "worms," "Trojans," and "spy ware" undermine safety and security of our most confidential data. Identity thieves, whose shadowy frauds leave victims with broken finances that may take years to repair and whose cost to industry reaches into the billions of dollars.

Since 1998, California has fought high technology crime with a state-wide network of regional law enforcement and prosecution task forces. Enacted under Penal Code Section 13848 et. seq., the task force program supports five regions covering 31 counties and is funded through the CalEMA. Each task force is a joint operation of local, state, and federal investigators and prosecutors. The California District Attorneys Association (CDAA) and the California Department of Justice support the task force program with specialized enforcement services, training, technical assistance, and the development of a state-wide database to help coordinate statewide operations and investigations.

Inside this report, you will find details on the scope of the challenge and the activities and observations of our state's most experienced cyber investigators and prosecutors. As an entity composed of state and local government officials, as well as representatives from all segments of the state's high technology industry, we are at the forefront of seeing the deleterious impact of high technology crime and we know the value of the California High Tech Task force. We urge the recipients of this report to continue to protect our citizens and infrastructure in this critical and effective program.

Respectfully Submitted,
William E. Eyres
Chairman, High Technology Crime Advisory Committee
Governor's Office of Emergency Services

Executive Summary

California is home to many of the largest and most advanced technology companies in the world. We also have most of our citizens online in ever increasing amounts. In 2008, 75% of Californians reported that they use a computer at home, work, or school, and 70% use the Internet.[1] Accompanying such an explosion in the telecommunication and Internet penetration has been a concomitant rise in technology crime. Our experience has taught us that technology and computers have given stalkers, pedophiles, destructive disgruntled employees, thieves, scam artists and those seeking infamy a new forum in which to ply their trade and cause misery. Fortunately, California has been a leader in cooperative and cost-effective strategies for protecting our infrastructure and citizens. This report documents the results of the work of the High Technology Theft Apprehension and Prosecution Program and makes recommendations to ensure the continued vitality of the defenses we have been building for over a decade.

The California High Technology Crimes Task Force strategy was created through Senate Bill 1734 in 1998 to help combat computer-related crimes such as network intrusions, computer hacking, theft of trade secrets, counterfeiting and piracy, telecommunications fraud, and theft of high tech related equipment and cargo. This legislation established the High Technology Theft Apprehension and Prosecution Program (HTTAP) which is now funded via the California Emergency Management Agency (CalEMA).

Since 1998, the program has expanded to include five regional task forces covering 31 counties within the State of California. The mission of the HTTAP Program is the investigation, apprehension, and prosecution of high technology crimes and to combat identity theft.

Each of the task force comprises multi-agency, multi-jurisdictional high-tech crime teams consisting of local, state, and federal investigators and prosecutors. Each team has the ability to coordinate effective investigation and prosecution of cross-jurisdictional crime. The task forces are able to efficiently pursue, arrest, and prosecute a wide range of criminal offenders in a greater number of jurisdictions than individual agencies can – thereby minimizing duplication of public resources and expense of time and money by victims, witnesses and courts. Each task force provides high technology-oriented public safety resources to the communities collectively served by all the task forces.

In addition to high-tech crime, the HTTAP Program was expanded in 2001 to address the ever-growing problem of identity theft which frequently exploits high technology to affect its goals. Five additional task force teams, specializing in this area, were created to focus on combating identity theft in California. These identity theft task force teams (one in each of the high-tech task force regions) work collaboratively with the five original HTTAP High-tech task force teams. The identity theft teams were modeled similarly to the High-tech task force teams, in that they too are multi-jurisdictional and multi-agency staffed. Additionally, they enjoy the partnerships of various privacy protection organizations that provide referrals and consumer protection information to the public.

The high tech task forces have been heralded as models and are their works assisting

[1] Public Policy Institute: http://www.ppic.org/content/pubs/jtf/JTF_DigitalDivideJTF.pdf

individual and corporate victims is often reported in the media. Examples include The Rapid Enforcement Allied Computer Team launched a probe targeting sellers who list pirated software on Craigslist at the request of Adobe Systems and Microsoft. [2]

In support of the five high technology and five identity theft regional task force teams, the California District Attorneys Association (CDAA) and the California Department of Justice, Office of the Attorney General, were added to promote aggressive prosecution, legal research leading to innovative ideas, training and new legislation, and the development of an intelligence database for use by the task forces

An allocation of nearly $13,300,000 in State funds was awarded to the 12 entities, which were required to provide a 25 percent match to the Program. This funding level has not increased since the inception of the program a decade ago and in fact has suffered from some reductions.

The California High Technology Crimes Task Force continues to be a high effective and cost-efficient approach to handling the investigation and prosecution of high tech and identity theft crimes in California. The coordinated activity of law enforcement in conjunction with a strong private entity partnership has been the hallmark of this successful approach. As leaders of law enforcement and critical industry in this state, we urge the Governor and Legislature to consider this model approach to other systemic crime problems in the state. Despite the unprecedented economic challenges facing our great state, the success and merits of this strategy demands that we support this program. Year after year the results have proven that the California High Technology Crimes Task Force protects our citizens and infrastructure and prevents additional harm.

This report was prepared and submitted pursuant to California Penal Code 13848.6(g) and encomapsses Fiscal Year (FY) 2007-2008.

[2] High Tech Crime Task Force Targets Craigslist Piracy http://www.kcbs.com/pages/4426821.php? Two major software companies have asked a high tech crime task force based in Silicon Valley to crack down on the billions of dollars worth of pirated software being sold online. The Rapid Enforcement Allied Computer Team launched a probe targeting sellers who list pirated software on Craigslist at the request of Adobe Systems and Microsoft.

THE HIGH TECHNOLOGY CRIME PROBLEM

California is under attack. Cyber criminals, including perpetrators of identity theft, are stealthily yet inexorably undermining the financial underpinnings of our state. E.g., High technology and entertainment, two of California's most important industries, continue to suffer staggering losses as the result of digital counterfeiting and piracy. Despite those losses, state and local law enforcement authorities can do little to help because the United States Congress preempted the field of copyright law some thirty years ago. In times of economic downturn the effect of such crime is intensified. Another example from the 2007-2008 fiscal year is an international ring of computer hackers who stole millions of customer records from major retail and dining outlets exposing tens of millions of people to identity theft and other misuse of the data. The victim companies included TJ Maxx, Barnes & Noble, Sports Authority, DSW, Forever 21, BJ's, Dave and Buster's and Boston Market. Many individual victims were in California. The crimes became the largest hacking and identity theft case ever prosecuted; indictments were filed in federal courts in San Diego, CA, New York, NY, and Boston, MA in August of 2008. The crimes were widely reported. See e.g.: http://www.cnn.com/2008/CRIME/08/05/card.fraud.charges/index.html

High technology crime in California also encompasses extensive losses due to counterfeiting and piracy of business, entertainment and consumer software and hardware, theft of computers and components, the continual growth of unauthorized access of computer systems and other criminal conduct. The five task forces have continued to combat high technology crime on all fronts. Where 2007 saw an 8 percent drop from the previous year in high-tech cases investigated by the task forces, 2008 showed a slight increase - just over 1 percent – from the previous year. Nonetheless, in 2008 there was an almost 5 percent decrease from the previous year in financial loss suffered by victims of high technology crime in California. It is possible that the decrease is in part due to the task forces' efforts to minimize losses to California businesses and citizens through the use of education, in conjunction with arrest and prosecution.

The risk of cyber attacks on infrastructure grows exponentially with our increased reliance on technology for transportation, communication, finance, and medicine. Dr. Steven Bucci notes that, "the high-level threats involve the full power of nation-states. These come in two major groups. The first is a full-scale nation-state cyber attack. The closest example of this was the assault made on Estonia in 2007. There, the highly developed network of a small country was temporarily brought to its knees. Portrayed by some as a simple display of public outrage over the moving of a statue, most felt there was more going on and that a government hand was at play. This dispute over the responsibility makes this an imperfect example, but it is a highly troubling harbinger of the future. One former Department of Defense (DoD) leader stated that over 1 million computers were used in this event, coming from over 70 countries." [3]

Highlighting the seriousness of the threat, President Barack Obama created a Cyber-Czar post. In addition, in a recently released Cybserspace Policy Review from the Whitehouse, the report noted that,"the architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these

[3] http://www.heritage.org/Research/NationalSecurity/hl1123.cfm

systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations. Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. Other intrusions threaten to damage portions of our critical infrastructure. These and other risks have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests."4

Internet Related Crimes

Much high technology crime is related to the Internet. While high technology crime encompasses much more, internet crime comprises a significant portion of it. The Internet Crime Complaint Center (IC3) is the only agency who collects data nationally specifically related to Internet crimes.[5] The IC3 annually compiles the information into reports. Useful inferences can be drawn from those reports and used to practical effect - with the caveat that the report is based upon victim complaints. When an internet crime is not reported the statistical information is not considered and the case is not referred to the proper law enforcement agency.

While, there is no global, national or statewide standardized reporting process to collect data for or track computer-related crimes, the IC3 annual report provides a viable basis for evaluating the extent of Internet related crime and developing appropriate methods to mitigate the problem. One thing apparent from the reports is certain - Internet crime is on the rise.

The IC3 received 275,284 reports of internet crime in 2008, a 33% increase over 2007. Of note is the fact that for the United States in 2008, California ranked 10th highest in internet crime perpetrators per 100,000 population. **More significant, California was 1st in the United States in the total number of internet crime perpetrators residing in the state (as it was in 2007)** and accounted for nearly 16% of all internet crime complaints where the perpetrator was identified. There appears to be equilibrium in the numbers of the perpetrators and victims of internet crime in California. **In 2008 California also ranked 10th highest in internet crime victims per 100,000 population and again California was 1st in the United States in the total number of internet crime victims residing in the state and accounted for nearly 15% of all internet crime complaints in the United States.**

---

[4] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[5] The Internet Crime Complaint Center (IC3) was established as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. The IC3 was intended, and continues to emphasize, serving the broader law enforcement community to include federal, as well as state, local, and international agencies, which are combating Internet crime and, in many cases, participating in Cyber Crime Task Forces. About us – www.ic3.gov

In the IC3 2008 ranking of states based on the percentage of reported internet crimes committed in a state where the perpetrator is from the same state, California is number 1 (with 30.6%); and in the top ten states in that ranking, perpetrators from California make up the 2nd highest percentage for each of those states. Thus California not only is significantly victimized with internet crime by resident Californians, but Californians also disproportionately victimize the rest of the country.

In addition to its national report, the IC3 also annually produces state specific reports. The 2008 state specific reports were not available at the time this document was produced. However, the 2007 report for California[6] noted the following:

The IC3 received 25,904 internet crime complaints from California. While the median dollar loss per California internet crime victim was $750.00, the range of loss demonstrates that significantly greater losses are likely.

Percent of California Internet Crime Victims by Monetary Loss:

13.2% $ .01 - $ 99.99
41.8% $ 100.00 - $ 999.99
31% $1,000.00 - $ 4,999.99
6.6% $5,000.00 - $ 9,999.99
6.7% Over $10,000.00

In 2007 the top dollar loss from a single complaint was $750,000.00; but the most alarming statistic is the total loss from reported internet crime throughout California - it was more than $29,000,000.00.

Perhaps not enough attention is paid to the problem due to a misconception that internet crime victims in California are “young kids” who have done foolish things to cause their victimization, thus we should not be concerned because they will grow out of the youthful foolish behavior that led them to be victimized. Such is not the case. The vast majority of victims are over thirty years old with a significant portion (nearly 57%) forty years or older. See the accompanying data:

California Complainant Demographics

Under 20 3.0%
20-29 19.7%
30-39 20.6%
40-49 23.2%
50-59% 23.4%
Over 60 10.1%

THE IDENTITY THEFT CRIME PROBLEM

Identity theft in California has changed very little over the last year, in terms of schemes

[6] Information in this section was obtained from the 2007 Internet Crimes Complaint Center Annual Report.

and those who are victimized. The home foreclosure crisis continues to fuel innovation in identity theft schemes and the use high technology, particularly botnets, has increased the ability to surreptitiously steal and use personal identifying information to facilitate financial fraud and other crimes

The Federal Trade Commission (FTC) provides the most viable and accurate national data related to identity theft that is published on an annual basis. **In 2008, California ranked number 2 in identity theft complaints to the FTC per 100,000 population. As bad as that appears, in terms of sheer numbers California is by far number one in terms of victimization, with 51,140 victim complaints of identity theft to the FTC**. California's next closest competitor for such dubious distinction is Texas with 31,708.[7] Unfortunately, California has maintained its number ranking for number of victims every year since 2001 when the FTC first published such data in its annual identity theft report. The problem has continued to grow in California. In 2007, of the top ten metropolitan areas in the United States for identity theft-related consumer complaints, four were in California. In 2008, six of the top ten were in California.

The 2008 FTC report includes three key findings:

1. Electronic fund transfer-related identity theft continues to be the most frequently reported type of identity theft bank fraud, despite declining since calendar year 2006.

2. Identity theft continues to be the number one reported consumer complaint accounting for 26% of all complaints received.

3. 65% of victims did not report the crime to any law enforcement agency (this percentage has remained steady for the past four years)

The first finding above is significant because it underscores the connection between identity theft and high technology crime and the need for the two areas to continue to be linked in law enforcement investigations.

The latter two findings are significant because they help interpret the decline in some statistics for identity theft for the HTTAP task forces. Clearly identity theft is increasing, particularly in California. However, fiscal year 2007-2008 saw a drop from the previous fiscal year in most categories of identity theft statistics for the task forces. The most dramatic drop, in number of victims, (roughly 71%) may be due to fewer reports to the task forces of database breaches by large businesses. There were also fewer investigations (about 8%) and concomitantly fewer cases filed (about 20%). Fortunately, there was also a decrease in the amount of losses experienced by task force case victims of identity theft (about 6%). Another factor affecting identity theft statistics is the lack of uniformity in defining an identity theft case (similar to the issues involved in defining gang cases for statistical purposes).

[7] FTC 2008 Annual IDTheft Report

The FTC reports that, nationally, complaints of identity theft increased in 2008, thus the decreased number of victims and losses in California as reported by the task forces present an apparent paradox. However, it is difficult determine the true impact of identity theft on our citizens when 65% of victims do not report their victimization to law enforcement. It is likely that many of the victims identified by the FTC are not put in contact with the task forces (especially since the central portion of the state is not served by an HTTAP Program identity theft task force team). These factors may in part explain why California's numbers are not in sync with the FTC data.

Public reluctance to report their complaints of identity theft to law enforcement has remained a problem for some years. Thus, accurate statistics to measure the scope and breadth of the problem have remained elusive at all levels of government.

Another possibility for a decline in task force statistics in fiscal year 2008 may be the beginning of an aggressive crackdown on unauthorized access and control of computers by federal agencies. E.g., during that time an ex-security consultant in Los Angeles, California, surreptitiously took over approximately 150,000 computers and ultimately became the first botnet operator charged under federal wiretap statutes. The defendant's network of "zombied" computers allowed the interception of communications between the victims' computers and financial institutions such as PayPal in order to mine data such as passwords and usernames and to transfer funds directly from victims' accounts. The information was also used to facilitate fraudulent purchases resulting in tens of thousands of dollars in losses. The defendant pleaded guilty (April 2008) in Federal Court in Los Angeles and was sentenced to four years in prison in March 2009. See e.g.,: http://www.wired.com/threatlevel/2009/03/botnet-hacker-g/.

The long standing problem of technology exacerbated ID Theft in ID theft and role of the California Task Forces in helping has been the subject of national news such as MSNBC's: Multiagency task force in California aims to catch thieves[8] as well as many local print and television stories.[9]

[8] http://www.msnbc.msn.com/id/7680843/

[9] http://www.10news.com/investigations/16925214/detail.html; http://www.signonsandiego.com/news/metro/20070408-9999-1m8scam.html; http://www.informationweek.com/news/global-io/showArticle.jhtml?articleID=201300944&cid=RSSfeed_TechWeb; http://sanjose.bizjournals.com/sanjose/stories/2009/05/18/story2.html; http://www.venturacountystar.com/news/2008/sep/21/hacker-grounds-rock-it-radio-ads/ http://www.sacbee.com/static/weblogs/crime/archives/013868.html; http://www.sacbee.com/static/weblogs/crime/archives/021254.html

HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE

The High Technology Crime Advisory Committee was established concurrently with the HTTAP Program. The purpose of the committee is to provide strategic oversight to the program and conduct planning in response to high technology crime in California. This committee includes representatives of the following agencies/organizations:

(1) A designee of the California District Attorneys Association.
(2) A designee of the California State Sheriffs Association.
(3) A designee of the California Police Chiefs Association.
(4) A designee of the Attorney General.
(5) A designee of the California Highway Patrol.
(6) A designee of the High Technology Crime Investigation Association.
(7) A designee of the California Emergency Management Agency.
(8) A designee of the American Electronic Association to represent California computer system manufacturers.
(9) A designee of the American Electronic Association to represent California computer software producers.
(10) A designee of CTIA--The Wireless Association.
(11) A representative of the California Internet industry.
(12) A designee of the Semiconductor Equipment and Materials International.
(13) A designee of the California Cable & Telecommunications Association.
(14) A designee of the Motion Picture Association of America.
(15) A designee of the California Communications Associations (CalCom).
(16) A representative of the California banking industry.
(17) A representative of the Office of Information Security and Privacy Protection.
(18) A representative of the Department of Finance.
(19) A representative of the State Chief Information Officer.
(20) A representative of the Recording Industry of America.
(21) A representative of the Consumers Union.

HTCAC ACTIVITIES

During the reporting period the HTCAC has addressed various areas of public safety concerns for the citizens of California. As noted above, California loses millions of dollars to criminals via counterfeiting and piracy of technical, education, business and entertainment industry software and hard goods. In addition to providing direction and guidance at quarterly HTCAC meetings (which are attended by personnel from the five task forces, general law enforcement, the industries represented by the Committee, educators and the general public), HTCAC members provided insight, technical assistance and practical support for initiatives to stem the tide of technology facilitated lawlessness.

One such area has been the effort to reinstitute concurrent jurisdiction among the states and the federal government in the area of enforcement of copyright law violations. Currently the tide of crime in this area has far outstripped the resources of the federal government to effectively prosecute the breadth of this crime allowing the theft of hundreds of millions of dollars from California corporations to continue with virtual impunity.

The HTCAC consistently reviews the standards and goals of the task forces and evaluates the practicality and applicability of them in light of changing technologies, crime patterns and societal norms. Periodically the HTCAC recommends modifications for the managing state agency (now Cal-EMA) to implement in order to maintain the effectiveness of the task forces.

As representatives of the high technology industries, HTCAC members facilitate solutions to and help mange the tension between the industries' interest in protecting their trade secrets and stock value by avoiding public disclosures inherent in the criminal justice process and the need to cooperate with law enforcement for effective policing of those who would do harm to the industry (both from without and within) costing the state and its citizens millions of dollars in losses.

HTCAC committee members also facilitate interaction between law enforcement as represented on the committee and the high technology industry through appearances at key meetings and conferences sponsored by organizations such as TechNet (a bipartisan, political network of CEOs and Senior Executives that promotes the growth of technology and the innovation economy).

HTCAC members committed to facilitating productive exchanges between legislators, the high technology industry and law enforcement to secure means of sustainable funding for the task forces with a view to emphasizing the value, both financial and societal, to the industry and government in keeping the task forces viable.

During the reporting period in order to keep the program viable in light of technological changes and evolving crime patterns, the HTCAC has engaged in a review and revision of the initial HTTAP Strategy which was originally adopted February 17, 1999 and last revised March 11, 2004.

The HTCAC also monitors the development and maintenance of a trust account facilitated by the CDAA for the benefit of the task forces. The account was created to accept monies from settlements in high-tech cases and other sources outside the normal funding pattern.

At most quarterly meetings the HTCAC is given a presentation by one of the task forces on a case and/or shareable intelligence, so that they can pass that information on to industry personnel. This trust relationship fosters interaction between the industry and law enforcement to better protect the public.

The HTCAC meetings also provide a forum for the direct dissemination of information such as the status of production of new training materials and programs and sources for assistance in getting such implemented. Examples are the statewide ID Theft Manual and the California Attorney General's e-mail piracy training CD. Other examples are the development of regional secure wide-area networks that allow case investigators and prosecutors to search duplicate copies of seized digital evidence themselves, thereby reducing the demands being made on forensic examiners. These programs allow the examiners to concentrate on higher level functions and will reduce backlogs that would otherwise occur in the forensic labs.

The HTCAC monitors and reviews pending legislation each quarter through the auspices of the CDAA member and provides suggestions, support for and opposition to various bills in an effort to keep California on a track that encourages continuation of its leading status in the fight against cyber crime and identity theft.

Finally, the HTCAC has provided the forum through which the task forces have been able to work out the details of and finally adopt a functional crime database system to maintain compliance with their legislative mandate.

2008 TASK FORCE HIGH TECHNOLOGY CRIME DATA

The HTTAP Program, through grants from the California Emergency Management Agency (Cal-EMA), currently funds five regional task forces that comprise the focus of California's efforts to combat the continual growth of high technology crime and identity theft.

During the 2007-2008 fiscal year, the five High Technology Crime Task Forces collectively reported the following information:

- 549 criminal cases were filed involving high technology crimes;
- 905 cases were investigated involving high technology crimes;
- 1,145 victims were involved in the cases with criminal filings;
- 181 arrests;
- 399 convictions were obtained; and
- $102,876,736 in total aggregated monetary losses was suffered by the victims.

A total of $12,172,880 was collectively awarded to the five High Technology Crime Task Forces during this period. This amount includes a 25 percent match provided individually by each of the Task Forces.

This money was utilized collectively as follows:

- Personnel $7,625,729
- Operating Expenses $4,446,749
- Equipment $100,402

For detailed information on statistics and funding by each individual High Technology Task Force, please refer to each Task Force's section of this report.

2008 TASK FORCE IDENTITY THEFT DATA

The HTTAP Program also funds five regional identity theft teams, each comprising a part of one of the five high technology crime task forces, to combat the inexorable increase of identity theft crime.

Collectively, during the 2007-2087 fiscal year, the five Identity Theft teams collectively reported the following information.

- 378 cases were filed involving identity theft;
- 1,252 cases were investigated involving identity theft;
- 4,747 victims were involved in the cases with criminal filings;
- 395 arrests;
- 207 convictions were obtained; and
- $115,356,910 in total aggregated monetary losses was suffered by the victims.

A total of $3,511,895 was collectively awarded to the five Identity Theft Task Forces during this period. This amount includes a 25 percent match provided individually by each of the Task Forces.

This money was utilized collectively as follows:

- Personnel $2,127,857
- Operating Expenses $1,357,488
- Equipment $26,550

For detailed information on statistics and funding by each individual Identity Theft team, refer to each Task Force's section of this report.

CALIFORNIA DISTRICT ATTORNEY'S ASSOCIATION ACTIVITIES

As part of the HTTAP Program, funds were allocated to the California District Attorney's Association (CDAA) for the development and implementation of a statewide education and training program. This program assists local prosecutors in the efficient and effective prosecution of identity theft and crimes perpetrated with the use of high technology.

The CDAA High Technology Theft Prosecution Education Program provides training to prosecutors, investigators, and law enforcement officers from all 58 counties in California. This training targets the successful investigation, apprehension, and prosecution of criminal organizations, networks, and groups of individuals involved in high technology and computer-based crimes. These cases involve computer-related and/or advanced technology issues, including white-collar crimes and identity theft.

In addition to providing training seminars, the program supports:

- Development and publication of the high technology crimes newsletter, Firewall, and the distribution of "Investigation and Prosecutions of High Tech Crimes" prosecution manual;

- Development and maintenance of online resources, including creation of a PowerPoint and audio library, a brief bank, expert witness database; and

- Provision of legal research services and other assistance as needed to California prosecutors and investigators.

A total of $310,448 was awarded to CDAA in furtherance of these activities. This amount includes a 25 percent match of $110,956.

CALIFORNIA DEPARTMENT OF JUSTICE (DOJ) ACTIVITIES

The Department of Justice (DOJ) is actively involved in the HTTAP Program through two separate projects:

Department of Justice – Deputy Attorney General (DAG) Identity Theft Support
Department of Justice – Advanced Training Center

DOJ Deputy Attorney General – Identity Theft Support

There are five Deputy Attorneys General (DAGs) and one Special Agent assigned to support the High Technology Identity Theft Program which is administered through the OES. One DAG is assigned to support each of the five task forces.

The DAGs duties include: (1) Prosecution support to the five task forces; (2) Development and delivery of training programs to law enforcement and the public; (3) Legal and prosecution support to rural counties; (4) Coordination of out-of-state investigation request; and (5) State agency legal and prosecution support.

During the 2008 fiscal year the DAGs initiated 11 investigations, filed 22 criminal complaints, convicted 41 defendants, and sentenced 31 defendants. The DAGs also provided 40 trainings on identify theft issues for law enforcement and the public. As part of the training program the DAGs assisted in the publication of the *2007 E-Evidence & Internet Crimes Against Children California Case Digest and Commentary*, and the *High-technology Crime: Email and Internet Chat Prosecutor/Investigator Resource CD*.

Funds have been allocated to DOJ to create the HTTAP-Identity Theft Support Project, which is part of the Special Crimes Unit in the Office of the Attorney General. A total of $554,779 was awarded to DOJ in furtherance of the DAG Identity Theft Support Project. This amount includes a 25 percent match of $110,956.

DOJ Advanced Training Center

The DOJ Advanced Training Center (ATC) has in place an interagency agreement with the OES. The goals of this agreement are:

- To provide additional high technology investigation training classes to California peace officers, especially personnel assigned to the five regional task forces;
- To provide advanced training in the area of computer forensics; and
- To provide equipment to personnel who conduct computer forensic examinations.

The primary objectives are:

- To create a program that would continuously update the curriculum for teaching high technology investigation techniques and computer forensics;
- To base the changes on trends in crime, law and technology;

- To create a program (a series of classes) that would train an investigator from a 'basic introduction' to high technology crimes, to an advanced level of computer forensic investigation competency;
- To develop the classes necessary to complete this series; and
- To test the students on learned skills and knowledge of computer crime investigations.

DOJ Database:

An additional aspect of the DOJ portion of the HTTAP Program is the development and maintenance of a statewide database on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies (required by Penal Code section 13848.4). Over the past year and a half the HTCAC discussed the trends of high technology and identity theft-related crime vis-à-vis advances in the technological sophistication of existing information management systems. That led the HTCAC to ask the DOJ to explore adapting an existing statewide system so that the task forces could take advantage of the all the existing statewide information in conjunction with their own crime data and information management systems. The rationale was that it would be more efficient, less expensive and very practical. During the period covered by this report the DOJ facilitated and completed a transition for the task forces from their prior system to the California Justice Regional Information Exchange System (Cal-JRIES). This database solution, provided by the DOJ, provides both an intelligence database and electronic bulletin board for law enforcement agencies to collaborate and exchange information, and thus complies with legislative mandate.

Classroom training begins in February 2009 and will be completed in May 2009. By the time of publication of this report, at least eleven classes will have been held and 90 officers and support staff trained. Two additional classes are scheduled which will complete the circuit for the High Tech Task Forces. Make-up classes will be offered on an as-needed basis. A good sign of the efficacy of the database is its increasing usage and the regular entry of new cases by high technology task force staff.

A total of $75,000 was allocated to the DOJ for the development, maintenance, backup and archiving of this database. This amount includes a 25 percent match of $15,000. The DOJ will continue to support the program, however, due to recent funding cuts, that support will be restricted to ensuring database availability.

CONCLUSION

High technology is the wave of the future and is becoming inextricably bound to nearly every aspect of crime. It is the hallmark of terrorist who use satellite communication, web-based messaging, electronic intrusion, remote controlled botnets and other means to steal money to fund violent attacks, to recruit supporters, and wreak havoc on civilization. These are also the tool of low level miscreants to commit everyday crime. Every entity that measures computer related crime and identity theft produces data that demonstrates that California is at the forefront in terms of victimization and perpetration of crime via high technology.

We reiterate a concern from our last report's conclusion: each year, technology improves, challenging law enforcement's ability to stay current with the myriad trainings required to maintain functional standards in the high tech world. In a community regularly affected by injuries, transfers, rotation, and promotion, in order to maintain continuity and not waste expensive training and valuable experience, stability of law enforcement personnel who specialize in identity theft or high technology investigations is essential. The average cyber criminal will use technology to advance his/her schemes and will devote much of his/her time committed to improving his/her potential for financial gains. That financial gain enables criminals to "re-invest" their time and resources back into themselves for the purpose of perfecting their illegal crafts. Law enforcement must have the commitment available to counter the criminal.

We the citizens, businesses, educational institutions and government of California have a huge stake in securing California from future crime. There is a consensus among those in the cyber security arena that criminals are consistently leveraging new technologies to facilitate new types of crime and reinventing old crime in the face of new technology. Law enforcement has to do the same. The learning curve for high technology crime fighting is steep and time consuming. We can't afford to sit on our laurels or wait for the next development to respond to. We have to be in front of it. The best way to do so is to redouble our efforts in innovative approaches to fighting high technology crime. This requires putting resources into our existing systems which have been recognized as leading edge by the rest of the country. Our failure to keep our task forces up to date through adequate funding has jeopardized our future. Our recommendations are few and simple:

RECOMMENDATIONS

- Increase funding available to the five existing task forces
- Provide resources to produce a task force to serve the central California region
- Continue public awareness programs
- Seek Federal Homeland Security funding based on the terrorism threat posed by cyber criminals

TASK FORCE SUMMARIES

Computer and Technology Crime High-Tech Response Team (CATCH)

Lead Agency: ***San Diego County District Attorney's Office***

CATCH is represented by the following three counties:

- Imperial
- Riverside
- San Diego

Through a common memorandum of understanding, CATCH is comprised of participants from the following agencies:

- California Department of Justice
- California State Parole
- California Department of Motor Vehicles
- Carlsbad Police Department
- Federal Bureau of Investigations
- Imperial County District Attorney's Office
- Riverside County District Attorney's Office
- Riverside County Sheriff's Department
- San Diego County District Attorney's Office
- San Diego County Probation
- San Diego County Sheriff's Department
- San Diego Police Department
- United States Postal Inspector

CATCH - HIGH TECHNOLOGY CRIMES

During fiscal year 2007-08, CATCH received $1,947,661 in State funds for high technology crimes. CATCH provided a 25 percent match of $486,915. Total grant award funds to further the investigation of high technology crimes was $2,434,576.

During the grant period, CATCH budgeted approximately 64.2 percent of its high technology grant budget on personnel costs; 35.8 percent on operational costs. No grant funds were used for equipment.
CATCH reported the following for cases involving high technology crimes during this grant period:

- **19** cases filed
- **126** cases investigated
- **71** victims involved in the cases filed
- **26** convictions obtained
- **32** arrests

- **$237,859** in total aggregate monetary loss was suffered by the victims

CATCH - IDENTITY THEFT CRIMES

During fiscal year 2007-08, CATCH received $561,903 in State funds for identity theft crimes. CATCH provided a 25 percent match of $140,476. Total grant award funds to further the investigation of identity theft crimes was $702,379.

During the grant period, CATCH budgeted approximately 43.2 percent of its identity theft grant budget on personnel costs; 56.8 percent on operational costs. No grant funds were used for equipment.

CATCH reported the following regarding Identity Theft team:

- **28** cases filed
- **54** cases investigated
- **55** victims involved in the cases filed
- **25** convictions obtained
- **34** arrests
- **$279,772** in total aggregate monetary loss was suffered by the victims

CATCH - STEERING COMMITTEE MEMBERS

CATCH receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with CATCH. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the CATCH Steering Committee:

- AEA
- Border Research & Technology Center
- California Attorney General
- California Department of Motor Vehicles
- California Department of Justice
- California State Parole
- Café Soft
- Carlsbad Police Department
- San Diego City Attorney's Office
- Computer Conversion
- Cox Communications
- Evident Data, Inc
- Federal Bureau of Investigations
- High Technology Crime Investigation Association
- ICE
- Imperial County
- Internal Revenue Service
- Linksys
- MedImpact Healthcare Systems, Inc
- Open Doors Software
- Peterbuilt

- Practical Security
- Qualcomm
- Ranger Online Corporation
- RCFL Forensic Lab
- Riverside Adult Probation Department
- Riverside County Sheriff's Department
- Riverside County Probation Department
- SAIC
- SBC
- San Diego Sheriff's Department
- San Diego County Probation Department
- San Diego District Attorney's Office
- San Diego Police Department
- SDRIW
- Software Design Assoc
- Sony
- Sony Computer Entertainment
- Source 4, Inc
- SPAWAR
- Time Warner Cable
- Time Warner ISP
- U.S. Encode Corporation
- U.S. Department of Justice
- U.S. Postal Inspection
- U.S. Secret Service
- Volonet/Redwire, ISP
- Voyager Systems, Inc
- Websense

Northern California Computer Crimes Task Force (NC3TF)

Lead Agency: ***Marin County District Attorney's Office***

NC3TF is represented by the following thirteen counties:

- Contra Costa
- Del Norte
- Humboldt
- Lake
- Napa
- Marin
- Mendocino
- Shasta
- Siskiyou
- Solano
- Sonoma
- Tehama
- Trinity

Through a common memorandum of understanding, NC3TF is comprised of participants from the following agencies:

- California Department of Justice
- California Department of Motor Vehicles
- Concord Police Department
- Contra Costa County District Attorney's Office
- Del Norte County District Attorney's Office
- Federal Bureau of Investigation
- Humboldt County District Attorney's Office
- Lake County District Attorney's Office
- Marin County District Attorney's Office
- Marin County Sheriff's Department
- Mendocino County District Attorney's Office
- Napa County District Attorney's Office
- Napa County Sheriff's Department
- Novato Police Department
- Redding Police Department
- San Pablo Police Department
- Shasta County District Attorney's Office
- Shasta County Sheriff's Department
- Solano County District Attorney's Office
- Sonoma County District Attorney's Office
- Tehama County District Attorney's Office
- Trinity County District Attorney's Office
- United States Postal Service
- United States Secret Service
- Vacaville Police Department
- Vallejo Police Department

NC3TF - HIGH TECHNOLOGY CRIMES

During fiscal year 2007-08, NC3TF received $1,947,661 in State funds for high technology crimes. NC3TF provided a 25 percent match of $486,915. Total grant award funds to further the investigation of high technology crimes was $2,434,576.

During the grant period, NC3TF budgeted approximately 79.2 percent of its high technology grant budget on personnel costs; 20.8 percent on operational costs. No grant funds were used for equipment.

NC3TF reported the following for cases involving high technology crimes during this grant period:

- **175** cases filed
- **351** cases investigated
- **317** victims involved in the cases filed
- **117** convictions obtained
- **106** arrests
- **$1,051,257** in total aggregate monetary loss was suffered by the victims

NC3TF - IDENTITY THEFT CRIMES

During fiscal year 2007-08, NC³TF received $561,903 in State funds for identity theft crimes. NC³3F provided a 25 percent match of $140,476. Total grant award funds to further the investigation of identity theft crimes was $702,379.

During the grant period, NC3TF budgeted approximately 86.8 percent of its identity theft grant budget on personnel costs; 13.2 percent on operational costs. No grant funds were used for equipment.

NC3TF reported the following on behalf of the Identity Theft team during this grant period:

- **13** cases filed
- **24** cases investigated
- **27** victims involved in the cases filed
- **13** convictions obtained
- **6** arrests
- **$99,615** in total aggregate monetary loss was suffered by the victims

NC3TF - STEERING COMMITTEE MEMBERS

NC3TF receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with NC3TF. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the NC3TF Steering Committee:

- Lucas Films Ltd.
- Marin County District Attorney's Office
- Napa County District Attorney's Office

- Napa County Sheriff's Office's Office
- Sechrest of Systems Integration Solutions
- Solano County District Attorney's Office
- Sonoma County District Attorney's Office
- Vallejo Police Department

Rapid Enforcement Allied Computer Team (REACT)

Lead Agency: ***Santa Clara County District Attorney's Office***

REACT is represented by the following five counties:

- Alameda
- San Francisco
- San Mateo
- Santa Clara
- Santa Cruz

Through a common memorandum of understanding, REACT is comprised of participants from the following agencies:

- Atherton Police Department
- California Highway Patrol
- Federal Bureau of Investigations
- Freemont Police Department
- Mountain View Police Department
- Pacifica Police Department
- San Francisco County District Attorney's Office
- San Jose Police Department
- San Mateo County Sheriff's Department
- Santa Clara County District Attorney's Office
- Santa Clara County Sheriff's Department
- United States Secret Service
- Department of Motor Vehicles
- Millbrae Police Department

REACT - HIGH TECHNOLOGY CRIMES

During fiscal year 2007-08, REACT received $ 1,947,661 in State funds for high technology crimes. REACT provided a 25 percent match of $ 486,915. Total grant award funds to further the investigations of high technology crimes was $2,434,576.

During the grant period, REACT budgeted approximately 36 percent of its high technology grant budget on personnel costs and 64 percent on operational costs. Grant funds of $ 8,376 were spent on equipment.

REACT reported the following for cases involving high technology crimes during this grant period:

- **2** cases filed
- **117** cases investigated
- **128** victims involved in the cases filed
- **10** convictions obtained
- **7** arrests
- **$93,703,921.00** in total aggregate monetary loss was suffered by the victims

REACT - IDENTITY THEFT CRIMES

During fiscal year 2007-08, REACT received $ 561,903 in State funds for identity theft crimes. REACT provided a 25 percent match of $ 140,476. Total grant award funds to further the investigations of identity theft crimes was $ 702,379.

During the grant period, REACT budgeted approximately 31 percent of its identity theft grant budget on personnel costs; 69 percent on operational costs. Grant funds of $ 0 were used for equipment.

REACT reported the following on behalf of the Identity Theft team during this grant period:

- **2** cases filed
- **80** cases investigated
- **224** victims involved in the cases filed
- **13** convictions obtained
- **9** arrests
- **$99,831,700.00** in total aggregate monetary loss was suffered by the victims

REACT – STEERING COMMITTEE MEMBERS

REACT receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with REACT. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the REACT Steering Committee:

- Network Appliance
- Google
- KLA-Tencor
- Applied Materials
- eBay
- Adobe Systems Incorporated
- Prosper
- Symantec

- Creative Security Company
- Cadence Design Systems, Inc.
- Apple
- Hitachi
- Palm
- American Express
- National Semiconductor
- BayTSP
- PG&E
- Sony Computer Entertainment
- Synopsys
- Oracle
- Netapp
- Visa
- Seagate
- Bechtel
- Cisco

Southern California High Tech Task Force (SCHTTF)

Lead Agency: ***Los Angeles County Sheriff's Department***

SCHTTF is represented by the following three counties:

- Los Angeles
- Orange
- Ventura

Through a common memorandum of understanding, SCHTTF is comprised of participants from the following agencies:

- Bureau of Immigration and Customs Enforcement (ICE)
- California Department of Motor Vehicles
- California Department of Social Security
- California Highway Patrol
- Culver City Police Department
- Federal Bureau of Investigations
- Glendale Police Department
- Los Angeles City Attorney's Office
- Los Angeles County District Attorney's Office
- Los Angeles County Sheriff's Department
- Los Angeles Police Department
- Orange County Sheriff's Department
- Oxnard Police Department
- Simi Valley Police Department
- United States Postal Service
- United States Secret Service
- Ventura County District Attorney's Office
- Ventura County Sheriff's Department
- Ventura Police Department

SCHTTF - HIGH TECHNOLOGY CRIMES

During fiscal year 2007-08, SCHTTF received $1,947,661 in State funds for high technology crimes. SCHTTF provided a 25 percent match of $486,915. Total grant award funds to further the investigation of high technology crimes was $2,434,576.

During the grant period, SCHTTF budgeted approximately 52.95 percent of its high technology grant budget on personnel costs; 43.27 percent on operational costs; and 3.78 percent on equipment.

SCHTTF reported the following for cases involving high technology crimes during this grant period:

- **31** cases filed
- **75** cases investigated
- **354** victims involved in the cases filed
- **23** convictions obtained
- **6** arrests
- **$6,958,583** in total aggregate monetary loss was suffered by the victims

SCHTTF - IDENTITY THEFT CRIMES

During fiscal year 2007-08, SCHTTF received $561,903 in State funds for identity theft crimes. SCHTTF provided a 25 percent match of $140,476. Total grant award funds to further the investigation of identity theft crimes was $702,379.

During the grant period, SCHTTF budgeted 53.01 percent of its identity theft grant budget on personnel costs; 41.91 percent on operational costs; and 5.08 percent on equipment.

SCHTTF reported the following on behalf of the Identity Theft team during this grant period:

- **163** cases filed
- **751** cases investigated
- **3,042** victims involved in the cases filed
- **62** convictions obtained
- **139** arrests
- **$10,596,699** in total aggregate monetary loss was suffered by the victims

Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)

Lead Agency: ***Sacramento County Sheriff's Department***

SVHTCTF is represented by the following seven counties:

- El Dorado
- Merced
- Placer
- Plumas County
- Sacramento
- San Joaquin
- Stanislaus
- Yolo
- Yuba County

Through a common memorandum of understanding, SVHTCTF is comprised of participants from the following agencies:

- Bureau of Immigration and Customs Enforcement (ICE)
- California Department of Insurance
- California Department of Justice
- California Department of Motor Vehicles
- California Highway Patrol
- California State Attorney General's Office
- California State Controller's Office
- Ceres Police Department
- Citrus Heights Police Department
- Crescent City Police Department
- Davis Police Department
- El Dorado County Sheriff's Department
- Elk Grove Police Department
- Escalon Police Department
- Federal Bureau of Investigation
- Folsom Police Department
- Lodi Police Department
- Manteca Police Department
- Marysville Police Department
- Merced Police Department
- Merced County Sheriff's Department
- Modesto Police Department
- Placer County District Attorney's Office
- Placer County Sheriff's Department
- Plumas County Sheriff's Department
- Rocklin Police Department
- Roseville Police Department
- Sacramento County Probation Department
- Sacramento County District Attorney's Office
- Sacramento Police Department
- Sacramento County Sheriff's Department
- San Joaquin County Sheriff's Department

- Solano County Sheriff's Department
- Stanislaus County District Attorney's Department
- Stanislaus County Sheriff's Department
- Tracy Police Department
- Turlock Police Department
- United States Attorney's Office
- United States Postal Inspection Services
- United States Secret Service
- USDA Forest Service
- Woodland Police Department
- Yolo County Sheriff's Department
- Yolo County District Attorney's Office

SVHTCTF - HIGH TECHNOLOGY CRIMES

During fiscal year 2007-08, SVHTCTF received $1,947,661 in State funds for high technology crimes. SVHTCF provided a 25 percent match of $486,915. Total grant award funds to further the investigation of high technology crimes was $2,434,576.
During the grant period, SVHTCTF budgeted approximately 81 percent of its high technology grant budget on personnel costs; 19 percent on operational costs. No grant funds were used for equipment.

SVHTCTF reported the following for cases involving high technology crimes during this grant period:

- **196** cases filed
- **236** cases investigated
- **275** victims involved in the cases filed
- **223** convictions obtained
- **30** arrests
- **$925,116** in total aggregate monetary loss was suffered by the victims

SVHTCTF - IDENTITY THEFT CRIMES

During fiscal year 2007-08, SVHTCTF received $561,903 in State funds for identity theft crimes. SVHTCTF provided a 25 percent match of $140,476. Total grant award funds to further the investigation of identity theft crimes was $702,379.

During the grant period, SVHTCTF budgeted approximately 89 percent of its identity theft grant budget on personnel costs; 11 percent on operational costs. No grant funds were used for equipment.

SVHTCTF reported the following on behalf of the Identity Theft team this grant period:

- **162** cases filed
- **293** cases investigated
- **1,353** victims involved in the cases filed
- **88** convictions obtained
- **204** arrests
- **$4,479,447** in total aggregate monetary loss was suffered by the victims

SVHTCTF – STEERING COMMITTEE MEMBERS

SVHTCTF receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with SVHTCTF. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the SVHTCTF Steering Committee:

- American Express
- American Network Services
- Apple Computer
- Best Buy
- Blue Shield of California
- Cache Creek Casino Resort
- California Department of Corporations
- California Department of Corrections
- California Department of Insurance
- California Department of Justice
- California Department of Motor Vehicles
- California District Attorneys Association
- California Highway Patrol
- California State Controller's Office
- Ceres Police Department
- Citi
- Citrus Heights Police Department
- Comcast
- Davis Police Department
- DHL/Airborne Express
- DirecTV
- E Trade Financial
- El Dorado County Sheriff's Department
- Elk Grove Police Department
- Escalon Police Department
- Esurance
- Federal Bureau of Investigation
- FedEx
- Folsom Police Department
- Hewlett Packard
- Home Depot
- Immigration & Customs Enforcement
- Intel Corporation
- Lodi Police Department
- Long's Drugs
- Macy's West
- Manteca Police Department
- Merced Police Department
- Merced Sheriff's Department
- Modesto Police Department
- Motion Picture Association of America (MPAA)
- NEC Electronics

- Nordstrom Investigations
- Oracle
- Placer County District Attorney's Office
- Placer County Sheriff's Department
- Plumas County Sheriff's Department
- Raley's
- Recording Industry Association of America (RIAA)
- Rite Aid
- Roseville Police Department
- Rumsey Tribal Gaming Agency
- Sacramento County Department of Human Assistance
- Sacramento County District Attorney's Office
- Sacramento Police Department
- Sacramento County Probation Department
- Sacramento County Sheriff's Department
- SAFE Credit Union
- San Joaquin County Sheriff's Department
- SBC
- Sears Loss Prevention
- Security Solutions LLC
- Stanislaus District Attorney's Office
- Stanislaus County Sheriff's Department
- State Farm Insurance
- Stockton Police Department
- Target
- Tracy Police Department
- Turlock Police Services
- UPS
- United States Attorney's Office
- Unite States Postal Inspection
- United States Secret Service
- US Bank
- USDA – Forest Service
- Verizon Wireless
- Walgreens
- Washington Mutual
- Wal-Mart Stores, Inc.
- Wells Fargo Bank
- Williams-Sonoma/Pottery Barn
- Woodland Police
- Yolo County District Attorney's Office

APPENDIX A

California Penal Code Sections 13848-13848.6

Penal Code 13848 Legislative intent; prevention of technology-related crimes

(a) It is the intent of the Legislature in enacting this chapter to provide local law enforcement and district attorneys with the tools necessary to successfully interdict the promulgation of high technology crime. According to the federal Law Enforcement Training Center, it is expected that states will see a tremendous growth in high technology crimes over the next few years as computers become more available and computer users more skilled in utilizing technology to commit these faceless crimes. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which is the target of a criminal act.

(b) Funds provided under this program are intended to ensure that law enforcement is equipped with the necessary personnel and equipment to successfully combat high technology crime which includes, but is not limited to, the following offenses:

(1) White-collar crime, such as check, automated teller machine, and credit card fraud, committed by means of electronic or computer-related media.
(2) Unlawful access, destruction of or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, or unauthorized disclosure of data stored within those computers and networks.
(3) Money laundering accomplished with the aid of computer networks or electronic banking transfers.
(4) Theft and resale of telephone calling codes, theft of telecommunications service, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.
(5) Software piracy and other unlawful duplication of information.
(6) Theft and resale of computer components and other high technology products produced by the high technology industry.
(7) Remarking and counterfeiting of computer hardware and software.
(8) Theft of trade secrets.

(c) This program is also intended to provide support to law enforcement agencies by providing technical assistance to those agencies with respect to the seizure and analysis of computer systems used to commit high technology crimes or store evidence relating to those crimes.

Penal Code 13848.2 High Technology Theft Apprehension and Prosecution Program; establishment; funding

(a) There is hereby established in the California Emergency Management Agency a program of financial and technical assistance for law enforcement and district attorneys' offices, designated the High Technology Theft Apprehension and Prosecution Program. All funds allocated to the California Emergency Management Agency for the purposes of this chapter shall be administered and disbursed by the Secretary of Emergency Management in consultation with the High Technology Crime Advisory Committee as established in Section 13848.6 and shall to the extent feasible be coordinated with federal funds and private grants or private donations that are made available for these purposes.

(b) The Secretary of California Emergency Management is authorized to allocate and award funds to regional high technology crime programs which are established in compliance with Section 13848.4.

(c) The allocation and award of funds under this chapter shall be made on application executed by the district attorney, county sheriff, or chief of police and approved by the board of supervisors for each county that is a participant of a high technology theft apprehension and prosecution unit.

Penal Code 13848.4 Expenditure of allocated funds

(a) Moneys allocated for the High Technology Theft Apprehension and Prosecution Program pursuant to subdivision (b) of section 13821 shall be expended to fund programs to enhance the capacity of local law enforcement and prosecutors to deter, investigate, and prosecute high technology related crimes. After deduction of the actual and necessary administrative costs referred to in subdivision (f), the funds shall be expended to fund programs to enhance the capacity of local law enforcement, state police, and local prosecutors to deter, investigate, and prosecute high technology related crimes. Any funds distributed under this chapter shall be expended for the exclusive purpose of deterring, investigating, and prosecuting high technology related crimes.

(b) Up to 10 percent of the funds shall be used for developing and maintaining a statewide database on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies. In addition, the Secretary of California Emergency Management may allocate and award up to 5 percent of the funds available to public agencies or private nonprofit organizations for the purposes of establishing statewide programs of education, training, and research for public prosecutors, investigators, and law enforcement officers relating to deterring, investigating, and prosecuting high technology related crimes. Any funds not expended in a fiscal year for these purposes shall be distributed to regional high technology theft task forces pursuant to subdivision (b).

(c) Any regional task force receiving funds under this section may elect to have the Department of Justice administer the regional task force program. The department may be reimbursed for any expenditures incurred for administering a regional task force from funds given to local law enforcement pursuant to subdivision (b).

(d) The California Emergency Management Agency shall distribute funds to eligible agencies pursuant to subdivision (b) in consultation with the High Technology Crime Advisory Committee established pursuant to Section 13848.6.

(e) Administration of the overall program and the evaluation and monitoring of all grants made pursuant to this chapter shall be performed by the California Emergency Management Agency.

Penal Code 13848.6. High Technology Crime Advisory Committee; disbursing funds

(a) The High Technology Crime Advisory Committee is hereby established for the purpose of formulating a comprehensive written strategy for addressing high technology crime throughout the state, with the exception of crimes that occur on state property or are committed against state employees, and to advise the California Emergency Management Agency on the

appropriate disbursement of funds to regional task forces.

(b) This strategy shall be designed to be implemented through regional task forces. In formulating that strategy, the committee shall identify various priorities for law enforcement attention, including the following goals:

(1) To apprehend and prosecute criminal organizations, networks, and groups of individuals engaged in the following activities:

(A) Theft of computer components and other high technology products.

(B) Violations of Penal Code Sections 211, 350, 351a, 459, 496, 537e, 593d, 593e, 653h, 653s, and 635w.

(C) Theft of telecommunications services and other violations of Penal Code Sections 502.7 and 502.8.

(D) Counterfeiting of negotiable instruments and other valuable items through the use of computer technology.

(E) Creation and distribution of counterfeit software and other digital information, including the use of counterfeit trademarks to misrepresent the origin of that software or digital information.

(F) Creation and distribution of pirated sound recordings or audiovisual works or the failure to disclose the origin of a recording or audiovisual work.

(2) To apprehend and prosecute individuals and groups engaged in the unlawful access, destruction, or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wire line communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, and unauthorized disclosure of data stored within those computers.

(3) To apprehend and prosecute individuals and groups engaged in the theft of trade secrets.

(4) To investigate and prosecute high technology crime cases requiring coordination and cooperation between regional task forces and local, state, federal, and international law enforcement agencies.

(c) The Secretary of California Emergency Management shall appoint the following members to the committee:

(1) A designee of the California District Attorneys Association.
(2) A designee of the California State Sheriffs Association.
(3) A designee of the California Police Chiefs Association.
(4) A designee of the Attorney General.
(5) A designee of the California Highway Patrol.
(6) A designee of the High Technology Crime Investigation Association.

(7) A designee of the California Emergency Management Agency.
(8) A designee of the American Electronic Association to represent California computer system manufacturers.
(9) A designee of the American Electronic Association to represent California computer software producers.
(10) A designee of CTIA--The Wireless Association.
(11) A representative of the California Internet industry.
(12) A designee of the Semiconductor Equipment and Materials International.
(13) A designee of the California Cable & Telecommunications Association.
(14) A designee of the Motion Picture Association of America.
(15) A designee of the California Communications Associations (CalCom).
(16) A representative of the California banking industry.
(17) A representative of the Office of Information Security and Privacy Protection.
(18) A representative of the Department of Finance.
(19) A representative of the State Chief Information Officer.
(20) A representative of the Recording Industry of America.
(21) A representative of the Consumers Union.

(d) The Secretary of California Emergency Management shall designate the Chair of the High Technology Crime Advisory Committee from the appointed members.

(e) The advisory committee shall not be required to meet more than 12 times per year. The advisory committee may create subcommittees of its own membership, and each subcommittee shall meet as often as the subcommittee members find necessary. It is the intent of the Legislature that all advisory committee members shall actively participate in all advisory committee deliberations required by this chapter.
Any member who, without advance notice to the Secretary of California Emergency Management and without designating an alternative representative, misses three scheduled meetings in any calendar year for any reason other than severe temporary illness or injury (as determined by the secretary) shall automatically be removed from the advisory committee. If a member wishes to send an alternative representative in his or her place, advance written notification of this substitution shall be presented to the executive director. This notification shall be required for each meeting the appointed member elects not to attend.
Members of the advisory committee shall receive no compensation for their services, but shall be reimbursed for travel and per diem expenses incurred as a result of attending meetings sponsored by the California Emergency Management Agency.

(f) The Secretary of California Emergency Management, in consultation with the High Technology Crime Advisory Committee, shall develop specific guidelines and administrative procedures for the selection of projects to be funded by the High Technology Theft Apprehension and Prosecution Program, which guidelines shall include the following selection criteria:

(1) Each regional task force that seeks funds shall submit a written application to the committee setting forth in detail the proposed use of the funds.

(2) In order to qualify for the receipt of funds, each proposed regional task force submitting an application shall provide written evidence that the agency meets either of the following conditions:

(A) The regional task force devoted to the investigation and prosecution of high technology-related crimes is comprised of local law enforcement and prosecutors, and has been in existence for at least one year prior to the application date.

(B) At least one member of the task force has at least three years of experience in investigating or prosecuting cases of suspected high technology crime.

(3) Each regional task force shall be identified by a name that is appropriate to the area that it serves. In order to qualify for funds, a regional task force shall be comprised of local law enforcement and prosecutors from at least two counties. At the time of funding, the proposed task force shall also have at least one investigator assigned to it from a state law enforcement agency. Each task force shall be directed by a local steering committee composed of representatives of participating agencies and members of the local high technology industry.

(4) The California High Technology Crimes Task Force shall be comprised of each regional task force developed pursuant to this subdivision.

(5) Additional criteria that shall be considered by the advisory committee in awarding grant funds shall include, but not be limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

(B) The number of high technology crime cases investigated in the prior year.

(C) The number of victims involved in the cases filed.

(D) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, or corporations, as a result of the high technology crime cases filed, and those under active investigation by that task force.

(6) Each regional task force that has been awarded funds authorized under the High Technology Theft Apprehension and Prosecution Program during the previous grant-funding cycle, upon reapplication for funds to the committee in each successive year, shall be required to submit a detailed accounting of funds received and expended in the prior year in addition to any information required by this section. The accounting shall include all of the following information:

(A) The amount of funds received and expended.

(B) The use to which those funds were put, including payment of salaries and expenses, purchase of equipment and supplies, and other expenditures by type.

(C) The number of filed complaints, investigations, arrests, and convictions that resulted from the expenditure of the funds.

(g) The committee shall annually review the effectiveness of the California High Technology Crimes Task Force in deterring, investigating, and prosecuting high technology crimes and provide its findings in a report to the Legislature and the Governor. This report shall be based on information provided by the regional task forces in an annual report to the committee which

shall detail the following:

(1) Facts based upon, but not limited to, the following:
(A) The number of high technology crime cases filed in the prior year.
(B) The number of high technology crime cases investigated in the prior year.
(C) The number of victims involved in the cases filed.
(D) The number of convictions obtained in the prior year.
(E) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations, and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained.

(2) An accounting of funds received and expended in the prior year, which shall include all of the following:
(A) The amount of funds received and expended.
(B) The uses to which those funds were put, including payment of salaries and expenses, purchase of supplies, and other expenditures of funds.
(C) Any other relevant information requested.

APPENDIX B

RELEVANT LEGISLATION

California High Technology Related Legislation – 2009/2010 Legislative Session as of 2/27/09

Bill	No.	Author/Sponsor	Subject	Status	Description/Amendments
AB	**5**	**Evans**	**Civil discovery: Electronic Discovery Act**	Referred to Assembly Judiciary Committee.	Establishes procedures in the Civil Discovery Act for a person to obtain discovery of electronically stored information, as defined.
AB	**22**	**Torres**	**Computer hacking: financial institutions**	Referred to Assembly Public Safety Committee.	Provides that in the case of a computer hacking violation involving the computer, computer system, or computer network of a financial institution, the fine for felony conviction would be increased, not to exceed $50,000.
AB	**130**	**Jeffries**	**ID Theft**	Referred to Assembly Judiciary Committee.	Makes the 2nd or subsequent commission of identified offenses related to the unlawful acquisition or use of personal identifying information a felony.
AB	**255**	**Anderson**	**Internet security: virtual globe technology**	Introduced February 11, 2009.	The introduced version Makes it a crime for an operator, as defined, of a commercial Internet website or online service that makes a virtual globe browser available to the public to provide aerial or satellite photographs or imagery or street view photographs of specified places in this state.
AB	**568**	**Lieu**	**Counterfeit goods: unlawful detainer**	Introduced February 25, 2009.	Provides that every building or place used for the purpose of willfully manufacturing, intentionally selling, or knowingly possessing for sale any counterfeit of a registered trademark is a nuisance that shall be enjoined, abated, and prevented.
AB	**575**	**Torres**	**Sex offenders: restrictions**	Introduced February 25, 2009.	Makes it a misdemeanor for a sex offender, except in limited instances, to be physically present and delay, linger, or idle about within 300 feet of a sensitive use site, as defined. Sensitive use site includes cyber cafes frequented by children.
AB	**819**	**Calderon**	**Intellectual property piracy**	Introduced February 26, 2009.	Establishes the Intellectual Property Piracy Prevention and Prosecution Program to fund grants for local law enforcement district attorneys for purposes of preventing and prosecuting intellectual property piracy, as specified. Also establishes the Intellectual Property Piracy Prevention and Prosecution Fund.
AB	**984**	**Nava**	**Cyber Piracy**	Introduced February 27, 2009.	Makes a technical, nonsubstantive change to the provision that makes it unlawful for a person to register, traffic in, or use an Internet domain name that is identical or confusingly similar to the personal name of another living person or deceased personality, with specified exceptions.

SB	**203**	**Harman**	**Child pornography: separate offenses, Internet distribution**	Referred to Senate Public Safety Committee.	Revises child pornography statutes, making the depiction or involvement of each individual minor a distinct and separate offense and includes within the definition of *distribute* making available for access or possession over the Internet.
SB	**226**	**Alquist**	**ID Theft**	Introduced February 23, 2009.	Provides that when multiple offenses occur in multiple jurisdictions and all of the offenses involve the same defendant(s) and the same scheme or substantially similar activity, then jurisdiction for all offenses is proper in any one of the counties where one of the offenses occurred.
SB	**324**	**Cedillo**	**Counterfeit Marks**	Introduced February 25, 2009.	Authorizes the court to consider a motion to have goods, with counterfeit trademarks that would otherwise be destroyed, donated to a nonprofit organization for distribution to persons living in poverty at no charge to the persons served by the organization.
SB	**584**	**Hollingsworth**	**Sex offenders: Internet access**	Introduced February 27, 2009.	Requires any person who is required to register under the Sex Offender Registration Act for committing a crime where the trier of fact has made a finding that a computer was used to facilitate the commission of the crime, to inform the registering agent whether he or she has access to a device with Internet capability. Imposes additional conditions on sex offenders who are on parole or probation if they used a computer to facilitate the commission of the crime.

CHAPTERED BILLS

Bill	No.	Author/Sponsor	Subject	Status	Description/Amendments
SB	**X3 8**	**Ducheny**	**Misc. - High Technology Crime Advisory Committee**	**Chapter 4, Statutes of 2009**	In regard to who the High Technology Crime Advisory Committee advises, replaces OES and Director of OES with California Emergency Management Agency and Secretary of California Emergency Management.

These bills deal with high technology crimes and identity theft and were recently introduced. A summary and the author of each, is shown. For details on any pending California high technology legislation, please visit the web site for the California District Attorneys' Association at www.cdaa.org.

APPENDIX C

HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE MEMBERS

MEMBER / ADDRESS/TELEPHONE	ORGANIZATION REPRESENTED
William E. Eyres – Chair 8831 Berta Ridge Court Prunedale, CA 93907 831-663-3695 eyres@montereybay.com	**Governor's Office of Emergency Services**
Saul Arnold – Vice Chair Corporate Counsel, Legal Services Law Department Applied Materials, Inc. 3050 Bowers Ave. M/S 2062 P.O. Box 58039 Santa Clara, CA 95054 408-563-4590 408-986-2836 (fax) saul_arnold@amat.com	**Semiconductor Equipment and Materials International**
Craig Beuhler Bureau Chief California Department of Justice Bureau of Investigation and Intelligence 1102 Q Street, Room 6050 Sacramento, CA 95814 916-319-9282 916-319-9440 (fax) Craig.buehler@doj.ca.gov	**California Department of Justice**
Joe Camicia Chief of Staff Office of the Chief Information Officer 1325 J Street, Suite #1600 Sacramento, CA 95814 916-319-9223 Joe.camicia@cio.ca.gov	**State Chief Information Officer**
Todd Chadd Assistant Chief Information Management Division California Highway Patrol 2555 First Avenue Sacramento, CA 95818 916-647-7171 TChadd@chp.ca.gov	**California Highway Patrol**

Jack Christin, Jr.
Trust & Safety Counsel
eBay, Inc.
2145 Hamilton Avenue
San Jose, CA 95125
408-376-5145
408-376-7517 (fax)
jchristin@ebay.com

California Internet Industry
E-Bay/PayPal

Mark Domnauer
Director, Global Safety and Security
Adobe Systems Incorporated
345 Park Avenue, MS A09-406
San Jose, CA 95110
408-536-4049
408-536-6616 (fax)
domnauer@adobe.com

American Electronic Association
(Calif. Computer Software Producers)

Donald Duggan
Senior Executive Vice President & CIO
Bank of the West
180 Montgomery Street, 25th Floor
San Francisco, CA 94104
415-765-4883
415-765-4858 (fax)
donald.duggan@bankofthewest.com

California Banking Industry

Merle (Bud) Frank
Deputy District Attorney
County of Santa Clara
County Government Center, West Wing
70 West Hedding Street
San Jose, CA 95110
408-792-2469
408-279-8742 (fax)
Bfrank@da.sccgov.org

California District Attorneys Assoc.

Margaret Felts
President, California Communications Association
1321 Howe Avenue, Suite 201
Sacramento, CA 95825
916-567-6702
916-922-3648
mcf@calcom.ws

California Communications Assoc.

Brian Gurwitz — **Recording Indust. Assoc. of America**
Regional Counsel
Anti-Piracy Legal Affairs
Recording Industry Association of America
10842 Noel Street, #106
Los Alamitos, CA 90720
714-236-0830
714-236-0930 (fax)
bgurwitz@riaa.com

Jim Cooper, Captain — **California State Sheriff's Assoc.**
Sacramento County Sheriff's Department
3720 Dudley Boulevard
McClellan, CA 95652
916-874-3007
916-874-3006 (fax)
jcooper@sacsheriff.com

Steven Lund — **American Electronic Association**
Director, Corporate Security — (Calif. Computer Syst. Manufacturers)
Intel Corporation
4500 S. Dobson Road, OC4-35
Chandler, AZ 85248
480-715-5036
Steven.j.lund@intel.com

Rocky P. McCants — **Calif. Cable & Telecommunications Association**
Regional Security Director
Comcast Cable
12647 Alcosta Blvd., Suite 200
San Ramon, CA 94583
925-973-7074
925-901-0231 (fax)
Rocky_mccants@cable.comcast.com

John McMullen, Lt. — **High Tech Crime Investigation Association**
Santa Clara Co. Dist. Attorney's Office
Bureau of Investigation
High Technology Crime Unit
70 West Hedding Street, West Wing
San Jose, CA 95110
408-210-9508 (cell)
jmcmullen@da.sccgov.org

Joanne McNabb — **Calif. Office of Information & Privacy Protection**
Chief, Office of Privacy Protection
California Office of Information & Privacy Protection
1325 J Street, Suite 1650
Sacramento, CA 95814
916-323-7301
916-323-7299 (fax)
Joanne.McNabb@OISPP.ca.gov

Bruce Muramoto — **California Police Chiefs Association**
Chief of Police
City of Winters
318-A First Street
Winters, CA 95694
530-795-2261 (ext. 121)
530-795-3921 (fax)
Bruce.muramoto@winterspolice.org

Jennifer Osborn — **California Department of Finance**
Principal Program Budget Analyst
Corrections/General Government Unit
Department of Finance
915 L Street, 8th Floor
Sacramento, CA 95814
916-45-8913
Jennifer.osborn@dof.ca.gov

Kevin Suh — **Motion Picture Assoc. of America**
Deputy Director
15301 Ventura Blvd., Building E
Sherman Oaks, CA 91403
818-995-6600
818-285-4408 (fax)
kevin_suh@mpaa.org

Mark Yamane (Northern California rep.) — **Calif. Communications Assoc. (CalCom)**
Buck Carter (Southern California rep.)
Area Manager-Asset Protection
(Appointment pending approval)
(858) 320-5520 or (619) 518-7990

Vacant — **Consumers Union**

APPENDIX D

HIGH TECHNOLOGY THEFT APPREHENSION & PROSECUTION PROGRAM

PROJECT DIRECTORS

Gil VanAttenhoven — **Interagency Agreement No. 6050-8**
Special Agent in Charge
Advanced Training Center
Department of Justice
11181 Sun Center Drive
Rancho Cordova, CA 95670
916-464-5591
FAX 916-464-5577
Gil.vanattenhoven@doj.ca.gov

Edward Berberian — **OES Grants Nos. HD08080210 and HT08080210**
District Attorney
Marin County
3501 Civic Center Drive, #130
San Rafael, CA 94903
415-499-6450
707-253-4664
eberberian@co.marin.ca.us

Craig Buehler — **OES Grant No. HT08089504**
Bureau Chief
California Department of Justice
Bureau of Investigation and Intelligence
1102 Q Street, Room 6050
Sacramento, CA 95814
916-319-9282
FAX 916-319-9440
craig.buehler@doj.ca.gov

Michael Groch — **OES Grants Nos. HD08080370 and HT08080370**
Deputy District Attorney
Chief, Economic Crimes Division
San Diego County District Attorney's Office
330 W. Broadway, Suite 700
San Diego, CA 92101
619-531-3102
FAX 619-531-4481
Michael.groch@sdcda.org

James Cooper, Capt. **OES Grants Nos. HD08080340 & HT08090340**
Sacramento County Sheriff's Department
3720 Dudley Blvd.
McClellan, CA 95652
916-874-3030
FAX 916-874-3006
jcooper@sacsheriff.com

Robert J. Costa, Lt. **OES Grant No. HT08090190**
Los Angeles County Sheriff's Department
11515 S. Colima Rd., #M-104
Whittier, CA 90604
562-347-2602
FAX 323-415-3421
rjcosta@lasd.org

David Hendrickson, Lt. **OES Grants Nos. HD08080430 and HT08090430**
County of Santa Clara District Attorney's Office
Bureau of Investigation
High Technology Crime Unit
70 West Hedding Street, West Wing
San Jose, CA 95110
408-792-2879
FAX 408-947-0692
dhenrickson@da.sccgov.org

Ron Smetana **OES Grant No. HD08089504**
Senior Assistant Attorney General
Special Crimes Unit
Office of the Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
415-703-5856
Ron.smetana@doj.ca.gov

W. Scott Thorpe **OES Grant No. HT08081059**
Chief Executive Officer
California District Attorneys Association
731 K Street, Third Floor
Sacramento, CA 95814
916-443-2017
sthorpe@cdaa.org

Ronald D. Williams, Lt. **OES Grant No. HD08080190**
Los Angeles County Sheriff's Department
9900 Norwalk Blvd., Suite 150A
Santa Fe Springs, CA 90670
562-347-2661
FAX 323-415-3818
rdwillia@lasd.org

APPENDIX E

HTCAC BYLAWS

STATE OF CALIFORNIA
BYLAWS, RULES AND PROCEDURES
OF THE
HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE

Adopted: June 2005
Revised: December 2008

ARTICLE I: NAME AND AUTHORITY

This organization, created in the State government by statutory authority, shall be known as the High Technology Crime Advisory committee – hereinafter referred to as the "Committee."

ARTICLE II: MEMBERSHIP AND CHAIRPERSON SELECTION

Section 1.
The Committee shall include the following twenty one representatives:

(1) A designee of the California District Attorneys Association;
(2) A designee of the California State Sheriff's Association;
(3) A designee of the California Police Chief's Association;
(4) A designee of the California Attorney General;
(5) A designee of the California Highway Patrol;
(6) A designee of the High Technology Crime Investigation Association;
(7) A designee of the California Office of Emergency Services;
(8) A designee of the American Electronic Association to represent California computer system manufacturers;
(9) A designee of the American Electronic Association to represent California software producers;
(10) A designee of the CTIA – The Wireless Association;
(11) A designee of the California Internet Industry;
(12) A designee of the Semiconductor Equipment and Materials International (SEMI);
(13) A designee of the California Cable Television Association;
(14) A designee of the Motion Picture Association of America;
(15) A designee of the California Communications Association (CalCom);
(16) A representative of the California Banking Industry;
(17) A representative of the California Office of Information Security and Privacy Protection;
(18) A representative of the California Department of Finance;
(19) A representative of the State Chief Information Officer;
(20) A designee of the Recording Industry of America; and
(21) A designee of the Consumers Union.

Section 2.
The chairperson of the Committee shall be selected by the Executive Director of the Office of Emergency Services from among the members of the Committee [Penal Code Section 13848.6(d)].

ARTICLE III: POWERS AND DUTIES

Section 1.

The Committee is empowered to act as the advisory board of the Office of Emergency Services in accordance with the mandates of the pertinent state acts and programs. The Committee may develop and/or modify and recommend to the Office of Emergency Services a high technology plan.

Section 2.

The Committee may develop policy recommendations for the Governor, the Legislature, the Office of Emergency Services and the local units of government on major criminal justice issues where a high technology nexus exists. To that end, the Committee understands itself to be the primary advisory board on technology-related criminal justice issues. Its goals include:

1. Identifying current, developing and future issues involving high technology crime and criminal justice policy and procedures relevant to such issues;
2. Developing an understanding of the issues attendant to high technology crime and making conclusions that provide the foundation for recommendations to the Office of Emergency Services, the Governor and the Legislature concerning high technology crime, criminal identification, apprehension and prosecution;
3. Issuing analysis of current or pending high technology criminal justice-related legislation;
4. Assisting California's criminal justice agencies and practitioners in the effective use of resources regarding high technology crime;
5. Coordinating studies and recommendations with the Office of Emergency Services and other criminal justice agencies with a view toward isolating issues common to high technology crime and justice.

ARTICLE IV: COMMITTEE MEETINGS

Section 1.

The Committee shall meet at such intervals as necessary to carry out its duties, but no more than twelve meetings shall be held annually. Regular meetings of the Committee shall be held at least quarterly unless, in the opinion of the Committee Chair and Vice Chair, there are insufficient items of business or insufficient funds to call such quarterly or regular meetings. The Executive Secretary of the Committee shall give a minimum of ten days written advance notice to the membership of the Committee of the time and place of a regular meeting.

Section 2.

Special meetings of the Committee may be called at any time by the Committee Chair. Forty-eight hours prior notice of the time and place of such special meetings shall be given by the Chair to the members, where permitted by law.

Section 3.

Meetings shall be conducted in accordance with these bylaws and Robert's Rules of Order.

ARTICLE V: SUBCOMMITTEES AND SUBCOMMITTEE MEETINGS

Section 1.

The Committee shall have the following subcommittees:

--Strategy Subcommittee
--Bylaws Subcommittee

ARTICLE V: *(continued)*

Section 2.

The Committee may recommend the creation of such subcommittees of its own membership as it deems necessary.

Section 3.

By a majority decision, the Committee may request the review of any subcommittee's decisions or activities.

Section 4.

Each subcommittee of the Committee shall meet as often as the subcommittee members find to be necessary.

Section 5.

All subcommittees shall be ad hoc in nature, and sit at the pleasure of the Committee Chair and a majority vote of the membership present at the time of the subcommittee creation.

ARTICLE VI: OFFICERS AND DUTIES

Section 1.

The officers of the Committee shall be the Chairperson (Chair) and the Vice Chairperson (Vice Chair).

Section 2.

The Chairperson shall be chosen by the Executive Director of the Office of Emergency Services from among members of the Committee, and shall serve at the pleasure of the Director. The Vice Chair shall be chosen by the membership of the Committee from among members of the Committee.

Section 3.

The Chair shall preside over all meetings of the Committee, and perform such additional duties as requested by the Committee and normally executed by a chairperson. The Chair shall create such standing and ad hoc committees as are deemed necessary to carry out the powers, duties and mission of the Committee. The Chair also shall appoint all members to both standing and ad hoc committees. All such subcommittee members shall serve at the pleasure of the Chair.

Section 4.

In the absence of the Chair, the Vice Chair shall preside at meetings and perform such additional duties as are required by the Committee and necessitated by the absence of the Chair.

Section 5.

In the event a vacancy occurs in the office of the Chairperson, the Director shall designate a successor prior to the next regular or special meeting. In the event a vacancy occurs in the office of the Vice Chairperson, the membership of the Committee shall designate a successor at the next regular or special meeting (Penal Code 13810).

ARTICLE VII: QUORUM, VOTING AND ATTENDANCE

Section 1.

A quorum of the Committee for any meeting shall consist of a majority of the members designated or appointed at the time of the meeting. If a quorum is present, a majority vote of the members present is necessary for Committee action, except for the suspension of these bylaws pursuant to Article XII.

Section 2.

No vote by an alternate will be honored except as provided for in this section.

a) An alternate designation letter is required from any absent Committee member, and shall be presented to the Committee prior to the start of the next regular or special meeting.

b) An alternate will have full voting rights, floor rights, and be included in quorum determinations.

c) Alternated attendance for a Committee member will negate provision of Section 3 below.

Section 3.

Any member of the Committee who misses three consecutive meetings or who attends less than fifty percent of the Committee's regularly called meetings during one calendar year shall be automatically removed from the Committee, except in situations in which the Chair finds that such deficiency is the result of illness or injury.

ARTICLE VIII: REIMBURSEMENT OF EXPENSES

Section 1.

Members of the Committee shall not receive compensation for their services but will be reimbursed for those actual and necessary expenses incurred which relate to their duties as Committee members.

Section 2.

Members of continuing task forces, review committees or of any other Committee-established auxiliary bodies who are not Committee members shall not receive compensation for expenses, unless prior approval has been obtained from the Office of Emergency Services. However, individuals who appear before the Committee at its request in order to review specific topics on one or more occasions shall be reimbursed for their necessary travel expenses.

ARTICLE IX: EXECUTIVE SECRETARY

Section 1.

The Executive Secretary of the Committee shall be appointed by the Director of the Office of Emergency Services

Section 2.

The duties of the Executive Secretary to the Committee shall be to provide staff support to the Committee including keeping all records, preparing agendas for each meeting, keeping minutes and approving all Committee expenditures.

Section 3.

The Executive Secretary shall, in accordance with applicable law, be responsible for any additional staffing, planning, organizing, coordinating, and directing to those activities necessary to assure the fulfillment of the powers, duties, and mission of the Committee.

ARTICLE X: CONFLICT OF INTEREST

Section 1.

No member of the Committee shall participate personally through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise in any proceeding, application, request for a ruling or other determination, contract, grant claim controversy, or other particular matter
in which funds under jurisdiction of the Committee are used, where to his or her knowledge he or she or his or her immediate family, partners, organization other than a public agency in which he or she is serving is an officer, director, trustee, partner, or employee or any person or organization with who he or she is negotiating or has any arrangement concerning prospective employment, has a financial interest.

Section 2.

In the review of proposals under appeal before the Committee, members of the Committee shall avoid any action which might result in, or create the appearance of:

a) Using his or her official position for private gain;
b) Giving preferential treatment to any person'
c) Losing complete independence or impartiality;
d) Making an official decision outside official channels; or
e) Affecting adversely the confidence of the public in the integrity of the Government or the program.

ARTICLE XI: AMENDMENTS TO THE BYLAWS

Section 1.

Amendments