

Notice of Public Meeting

Nevada Advisory Board for Technological Crime
Nevada Cyber Crime Task Force
10 AM, February 13th

*Office of the Attorney General/Nevada Department of Justice
100 N. Carson Street, Carson City, Nevada
Mock Courtroom Phone: 775.684.1100*

*Via Videoconferencing
Room 3315, Grant Sawyer State Building,
555 East Washington Ave., Las Vegas, Nevada*

AGENDA

1. Call to Order. *
[George Chanos]
 - a. Verification of quorum.
2. Discussion and approval of minutes from December 15, 2005 Advisory Board meeting. *
[George Chanos]
3. Advisory Board changes: Welcome of William Uffelman, President and CEO, Nevada Bankers Association (participating telephonically).
[George Chanos]
4. Report on Student Internet Safety Program in Clark County School District by Ms. Dixie Stephens (invited guest). Discussion, recommendations and action regarding dissemination of related program materials, staff coordination in other school district's activities, and associated potential media involvement.*
[Dixie Stephens, Jim Earl, Tom Pickrell, and Lorrie Adams]
5. Discussion, recommendations and action regarding funding sources and budget for the Advisory Board and activities of the Nevada Cyber Crime Task Force.*
[Jim Earl, Lorrie Adams]
 - a. Attempt to recover funds reverted to General Fund in FY2005 – Lessons learned
 - b. On-going reprogramming attempt from salary account to operating account
 - c. Funding Reduction of Justice Assistance Grant Program (JAG) and its implications for Advisory Board application.
 - d. Cloverdell grant explanation and application window
 - e. Change in administration of Homeland Security grant funds and implications for Advisory Board application
 - f. Action by Board authorizing Executive Director to apply for grants to support Task Force Activities in accordance with governing statute.
6. Discussion, recommendations and action regarding operation of current Nevada forfeiture statutes and comparison with comparable provisions of other states and the federal system.*
[John Colledge]

7. Update on liaison activities.
[Lorrie Adams]
8. Update on InfraGard program and focus
[Eric Vanderstelt]
9. Update on Advisory Board Internet presence
[Jim Earl]
 - a. Executive Branch web site (Attorney General)
 - b. Legislative Branch web site (LCB)
10. Update on training activities anticipated in first half of calendar year 2006.
[Jim Earl and Lorrie Adams]
 - a. "Prosecutorial Responses to Internet Victimization" Training Conference, hosted by National Association of Attorneys General and the National Center for Justice and Rule of Law at the University of Mississippi
11. Discussion, recommendations and action regarding Southern Task Force activities. *
[Michael Sanders, Eric Vanderstelt and Karen Francis]
12. Discussion, recommendations and action on Northern Task Force activities. *
[John Colledge]
 - a. Status of Revised Cooperative Agreement incorporating the Northern Nevada Task Force.
 - b. Update on the laboratory facility in Reno being made available by Immigration and Customs Enforcement.
 - c. POST curriculum preparation
13. Discussion, recommendation and action regarding the State Security Committee.*
[Randy Potts]
 - a. Next phase of State Security Awareness training
 - b. Interface with Nevada Electronic Records Committee regarding Nevada data classification strategy.
14. Discussion, recommendation and action regarding overall strategy and approach.*
[Jim Earl]
 - a. Schools
 - b. Identity Theft
 - c. Expansion of Task Force Membership
 - d. Expand Task Force Response Capabilities
15. Board Comments
16. Public Comments.
17. Scheduling and location of future meetings. *

* Denotes a possible action item. The order of the items is subject to change.

This agenda has been sent to all of the members of the Advisory Board and other interested persons who have requested an agenda.

Unless otherwise stated, items may be taken out of the order presented on the agenda at the discretion of the chairperson. The meeting may be recorded. Some Board members attend meeting via telephone conference.

Members of the public who are disabled and require special accommodations or assistance at the meeting are requested to notify Lorrie Adams at (775) 688-1813, twenty-four hours prior to the meeting.

THIS MEETING HAS BEEN PROPERLY NOTICED AND POSTED AT THE FOLLOWING LOCATIONS:

Office of the Attorney General
5420 Kietzke Lane, Suite 202
Reno, Nevada 89511

Office of the Attorney General
555 East Washington Avenue
Las Vegas, Nevada 89101

Office of the Attorney General
100 North Carson Street
Carson City, Nevada 89701

Reno City Hall
One East First Street
Reno, Nevada

Nevada Advisory Board for Technological Crime
Nevada Cyber Crime Task Force
February 13, 2006
Meeting Minutes

*Office of the Attorney General/Nevada Department of Justice
100 N. Carson Street, Carson City, Nevada
Mock Courtroom Phone: 775.684.1100*

*Via Videoconferencing
Room 3315, Grant Sawyer State Building,
555 East Washington Ave., Las Vegas, Nevada*

1. Call to Order.

George Chanos called the meeting to order at 10:04 AM and requested a roll call of the present board members.

Present:

- Bernie Anderson, Assemblyman
- John Colledge, III, Resident Agent in Charge, Immigrations and Customs Enforcement
- Tom Pickrell, Assistant Director, Facilities, Clark County School District
- William Uffelman, President and CEO, Nevada Bankers Association (via telephone)
- Eric Vanderstelt, Supervisory Special Agent, Federal Bureau of Investigation.

Staff in Attendance:

- Lorrie Adams, Program Coordinator
- James Earl, Executive Director
- Gerald Gardner, Legal Counsel

Others:

- Karen Francis, Detective Sergeant, Las Vegas Metropolitan Police Department
- Matt Goward, Special Agent, US Department of Energy, Inspector General's Office
- Paul Hales, Investigator, Nevada Department of Public Safety
- Mary Haugen, Sergeant, Nevada Department of Public Safety
- Dixie Stephens, Clark County School District

2. Discussion and approval of minutes from December 15, 2005 Advisory Board meeting. George Chanos asked for any revisions or extensions to the meeting minutes of December 15, 2003.

Board Action:

- *Bernie Anderson proposed the minutes to be approved.*
- *Tom Pickrell seconded.*
- *Motion unanimously passed.*

3. Advisory Board changes.

The welcomed William Uffelman, President and CEO, Nevada Bankers Association, to the Advisory Board.

4. Report on Student Internet Safety Program in Clark County School District.

Dixie Stephens presented the i-SAFE pilot program at Clark County School District. i-SAFE provides age-appropriate K-12 curriculum free of charge and is funded by Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. The curriculum is a dynamic interactive program designed to educate and empower the student. Each lesson includes Activity Pages and Discussion for the class. The six modules include: Cyber Citizenship; Personal Safety; Cyber Security; Intellectual Property; Cyber Bullying and; Predator Identification. The program will also include parental outreach and online professional development for continued education credits. One of the objectives includes having one teacher trained from each school. In turn, the teachers would train the other teachers in their respective schools. The pilot program will start with 10 teachers in March 2006. These teachers will be asked to evaluate the overall program.

Tom Pickrell added that this program is more inclusive than the previous program used which focused on middle school students.

Jim Earl asked if the program would be available statewide. Dixie responded that at the moment there was no plan in place to introduce other schools districts. This is a pilot program that will need to be evaluated.

Jim shared that he has been in contact with media regarding television interviews on what school districts are doing to educate students and parents about internet safety. Tom Pickrell noted that this is a pilot program and media coverage now would be too soon.

Bernie Anderson shared that school librarians are concerned with the type of information that should be available to students and how to keep the students safe from online predators. Bernie suggested contacting English and Social Studies teachers to take this training, as they required students to conduct research online for written papers. This may assist teachers in determining if the students have “lifted” papers from the Internet to claim as their own work.

George Chanos asked if the website provided all the informational materials for the Advisory Board to download. Dixie stated the website provides a lot of information, but not course specific information. George asked if i-SAFE was open to private citizens and corporate businesses in order recruit volunteers and conduct fund raising efforts. Dixie stated i-SAFE was funded by Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice and provided a contact name.

George asked if there was anything that the Board could do to assist. Dixie stated a grant from the Las Vegas Metropolitan Police Department pays for the substitute teachers’ salaries. The i-SAFE program is an in-service training for teachers, thus causing a need for substitute teachers

to cover the classrooms. George asked could parents volunteer to be trained in order to further the training program. Dixie stated at this time parents are not being trained, however a parental outreach is one of the objectives once the pilot program is underway.

George stated that the Advisory Board has a statewide focus and i-SAFE program is a Clark County School District program. The Board needs to start thinking about how to broaden this program statewide to include funding from the legislature and private sector. Bernie stated that Curriculum Coordinators are cabinet level positions. Sharing the i-SAFE program with the coordinators is a natural way to introduce i-SAFE and for possible incorporating into the curriculum. Nevada has been successful in placing computers in every class; introducing this type of program is the next natural step to raise the awareness of technological issues.

George asked Tom Pickrell and Dixie if Clark County School District would welcome private sector volunteers to teach the i-SAFE program. Tom and Dixie pointed out that there are a number of concerns about allowing “outsiders” onto the schools for presentations. George stated he was not satisfied with waiting a year until the legislature went into session to address the Internet safety in the schools. George asked Jim to look into possible solutions.

5. Discussion, recommendations and action regarding funding sources and budget for the Advisory Board and activities of the Nevada Cyber Crime Task Force.

- Jim Earl stated that due to a salary savings the advisory board account now has about \$9000. The advisory board statute states the funds will not revert back to the general fund at the end of the fiscal year. However, there is a general fund statute that supersedes the board statute; if the general fund is facing a shortfall; unused funds from all accounts will revert back to the general fund at the end of the each fiscal year. To address this issue, the board may want to consider action at the close of the next legislative session to have the Board account excluded from the general fund reversion statute. Jim identified the areas where the money will be spent, such as travel for rural outreach laboratory supplies.

Bernie Anderson stated that there may be some other areas with available resources that could be used to obtain equipment for the task forces other than the Attorney General’s Office, such as the state computer systems and the central repository. Bernie noted in the beginning, the advisory board was to act in an administrative capacity, relying on the local agencies to use their grant opportunities to fulfill the need for forensic equipment. Jim stated that to date funding sources for the task forces have largely come from federal agencies. The federal agencies are starting to redirect their funding sources to other areas. Bernie asked about the crime labs participation in examinations. Jim stated that the crime labs are limited in their expertise and rely on highly trained officers for full forensic examinations. The regional crime laboratory in northern Nevada relies on the task force for complete forensic analysis of computer harddrives.

George Chanos stated that Bernie raises a good point about the advisory board's role. Does the board concentrate on funding raising, legislation, or equipment purchase? Should the board concentrate on education and coordination?

Tom Pickrell stated that the original capacity of the board was oversight. Bernie added that in the beginning, the board wanted to know which agencies were investigating these types of crimes, what financial institutions were doing and to encourage district attorneys to prosecute.

George stated there are many things the task force could do if funding was available, however the reality is what areas the Board should concentrate on that add value to the State. George reiterated that at the last meeting, the Board agreed that child safety and identity theft were the areas of most importance.

Board action:

- *George Chanos proposed a motion that the executive director produce a report on what the Advisory Board should be doing in the areas of child safety, identity theft and forensics resources that has fundable, realistic and achievable results within this year. Report to be presented at the next meeting.*
- *Bernie Anderson seconded.*
- *Motion passed unanimously.*
- Jim stated the funding reduction of Justice Assistance Grant Program (JAG) will have a negative impact. The funds are more directed toward drug-related problems.
- Jim stated the Cloverdell grant is for forensic sciences; the deadline has not been announced.
- Jim stated there has been a change in administration of Homeland Security grant funds. The intelligence category is the area where cyber crime qualifies for funding. Jim stated he as had difficulty in talking with the Las Vegas Metropolitan Police Department Chief who is in charge of this category.

George Chanos asked in Detective Sergeant Karen Francis would assist Jim in making this connection. Karen stated she would.

- Jim asked if the Board would authorize the Executive Director to apply for grants to support Task Force Activities in accordance with governing statute.

Board action:

- *Bernie Anderson proposed a motion authorizing the Executive director to apply for grants to support the task force activities.*
- *John Colledge seconded.*

- *Motion passed unanimously.*

6. Discussion, recommendations and action regarding operation of current Nevada forfeiture statutes and comparison with comparable provisions of other states and the federal system.

John Colledge stated that the current Nevada forfeiture statute requires a higher standard of proof than other states. In addition, there is a cap on the amount to be shared to law enforcement. John suggested that the Nevada statute be revised to be comparable to other states. Nevada currently lacks a cohesive mechanism for asset forfeiture. John pointed out that other states obtain significant funding for technology crime investigation through the operation of their forfeiture statute.

Jim Earl described the Nevada racketeering statute and how this statute could be used to create a new technological crimes statute.

George Chanos asked Gerald Gardner to work with Jim on drafting the proposed legislation. Gerald stated he would.

Bernie Anderson stated he would reserve a Bill Draft for this new proposed legislation.

George Chanos asked Bill Uffleman if he could assist, as well. Bill stated he would.

7. Update on liaison activities.

Lorrie Adams discussed her various liaison activities, which include two National Institute of Justice committees.

George Chanos asked Lorrie to supply a one-page summary to the Board on a monthly basis.

8. Update on InfraGard program and focus

Eric Vanderstelt stated InfraGard is a Federal Bureau of Investigation program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United

States. InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

Jim Earl noted that the staff would continue to participate in and support InfraGard activities as a means of fulfilling one of the Board's statutory mandates.

9. Update on Advisory Board Internet presence

Jim Earl stated that a four-page website that has been laid out is waiting to be added to the redesigned Attorney General website.

Jim stated that the Legislative Council Bureau website has some information on the Board and provide link information on meetings, agendas and minutes.

Bernie Anderson asked if a link to the sexual predators registry website would be helpful to parents. Jim stated he was concerned that sexual predators will have access the same public website and therefore be able to view the child safety page.

10. Update on training activities anticipated in first half of calendar year 2006.

Jim Earl stated the National Association of Attorneys General and the National Center for Justice and Rule of Law at the University of Mississippi will be hosting "Prosecutorial Responses to Internet Victimization" Training Conference.

A Deputy Attorney General has already been identified to attend. The attorney will then in turn provide a continuing legal education class for the Attorney General's Office.

11. Discussion, recommendations and action regarding Southern Task Force activities.

Lorrie Adams discussed the Southern Facility 2005 statistics.

Karen Francis shared that a recent case, involved a 20GB harddrive that contained 5 million images.

George Chanos commends Las Vegas Metropolitan Police Department for the efforts.

12. Discussion, recommendations and action on Northern Task Force activities.

- John Colledge stated the Revised Cooperative Agreement incorporating the Northern Nevada Task Force is ready for signature.
- John stated that the Reno Police Department will be placing a computer forensic machine in the laboratory shortly.
- John stated the curriculum is undergoing its first draft for review.

13. Discussion, recommendation and action regarding the State Security Committee.
Randy Potts was not present.

14. Discussion, recommendation and action regarding overall strategy and approach.

Jim Earl stated that as previously discussed he will compile a report on what direction the Board should take in the areas of schools, identity theft, expansion of Task Force membership and determine the forensic examination capabilities of the task force.

15. Board Comments.

16. No Public Comments.

17. Next meeting Friday, April 7, 2006 10:00 AM at the Attorney General's Offices in Carson City and Las Vegas.

Notice of Public Meeting

Nevada Advisory Board for Technological Crime
Nevada Cyber Crime Task Force
April 7, 2006

10:00 am

*Office of the Attorney General/Nevada Department of Justice
100 North Carson Street, Carson City, Nevada
Mock Courtroom Phone 775.684.1100*

*Via Videoconferencing
Room 3315, Grant Sawyer State Building
555 East Washington Ave., Las Vegas, Nevada*

AGENDA

1. Call to Order.*
[George Chanos]
 - a. Verification of quorum
2. Discussion and approval of minutes from February 13, 2006 Advisory Board Meeting.*
[George Chanos]
3. Discussion, recommendations and action regarding funding sources and budget for Advisory Board and activities of the Nevada Cyber Crime Task Force.*
[Jim Earl and Lorrie Adams]
 - a. Homeland Security Grant application
 - b. Justice Assistance Grant Program (JAG) application
 - c. Budget submission for fiscal years 2008 and 2009
4. Discussion, recommendations and action regarding draft technological crime forfeiture statute.*
[Jim Earl]
5. Update on liaison activities.
[Jim Earl and Lorrie Adams]
6. Discussion, recommendations, and action regarding future mission and strategies of the Advisory Board and Nevada Cyber Crime Task Force.*
[Jim Earl]
 - a. Presentation relating to basic missions and strategies

- b. Consideration of statutory changes (to include refining mission and Board enlargement).
- 7. Discussion, recommendations and actions regarding responses to existing and emerging technological threats.*
[Randy Potts, Bill Uffelman, Jim Earl]
 - a. Bank actions to reduce identity theft
 - b. State Security Committee activities
- 8. Discussion, recommendations and actions regarding Southern Task Force activities.*
[Task Force members]
- 9. Discussion, recommendations and actions regarding Northern Task Force activities.*
[John Colledge]
- 10. Board Comments.
- 11. Public Comments.
- 12. Scheduling of future meetings.*

* Denotes a possible action item. The order of the agenda items is subject to change.

This agenda has been sent to all members of the Advisory Board and other interested persons who have requested an agenda.

Unless otherwise stated, items may be taken out of order presented on the agenda at the discretion of the chairperson. The meeting may be recorded. Some Board members may attend the meeting via telephone conference.

Members of the public who are disabled and require special accommodations or assistance at the meeting are requested to notify Lorrie Adams at (775) 688-1813 twenty-four hours prior to the meeting.

THIS MEETING HAS BEEN PROPERLY NOTICED AND POSTED AT THE FOLLOWING LOCATIONS:

Office of the Attorney General
5420 Kietzke Lane, Suite 202
Reno, Nevada 89511

Office of the Attorney General
555 East Washington Avenue
Las Vegas, Nevada 89101

Office of the Attorney General
100 North Carson Street
Carson City, Nevada

Reno City Hall
1 East First Street
Reno, Nevada

Nevada Advisory Board for Technological Crime
Nevada Cyber Crime Task Force
April 7, 2006
Meeting Minutes

*Office of the Attorney General/Nevada Department of Justice
100 N. Carson Street, Carson City, Nevada
Mock Courtroom Phone: 775.684.1100*

*Via Videoconferencing
Room 3315, Grant Sawyer State Building,
555 East Washington Ave., Las Vegas, Nevada*

1. Call to Order.

John Colledge called the meeting to order at 10:05 AM and requested a roll call of the present board members.

Present:

- Chris Finnegan, Information Security Officer, Office of Information Security, Nevada Department of Information Technology (proxy)
- Tom Pickrell, Assistant Director, Facilities, Clark County School District (via telephone)
- Bill Uffelman, President and CEO, Nevada Bankers Association
- Eric Vanderstelt, Supervisory Special Agent, Federal Bureau of Investigation (proxy)
- Valerie Wiener, State Senator

Staff in Attendance:

- Lorrie Adams, Program Manager
- James Earl, Executive Director
- Gerald Gardner, Legal Counsel

Others:

- Karen Francis, Detective Sergeant, Las Vegas Metropolitan Police Department

2. Discussion and approval of minutes from February 13, 2006 Advisory Board meeting.

John Colledge asked for any revisions or extensions to the meeting minutes of February 13, 2006.

Bill Uffelman noted his last name was misspelled and asked the minutes reflect the corrections. Also, on page 4, second line, the word “funding” should be changed to “fund.”

Board Action:

- *Chris Finnegan proposed the minutes to be approved with the correct spelling of Bill Uffelman and the word correction on page 4.*

- *Eric Vanderstelt seconded.*
- *Motion unanimously passed.*

Jim Earl stated that it is his intention to have the meeting minutes completed and submitted to the Board within 10 working days of the meeting. Lorrie Adams stated that is noted as such in the Nevada Open Meeting Law.

3. Discussion, recommendations and action regarding funding sources and budget for Advisory Board.

Homeland Security

Jim Earl stated the he emailed all Board members the electronic version of the Homeland Security grant application on February 22. There was very little time to respond to Nevada's internal application process; the application was completed in about 3 days and submitted on time. Jim attended a briefing by the Nevada Homeland Security Committee. While it was not particularly detailed, it appears as though the grant application was incorporated into the State process. Jim stated he will not know if the Board will receive any money until late May when the federal award is made to states. Money is then allocated through the State process.

Jim stated he is not particularly hopeful. His impression is that the Board is not a favored player in the State – perhaps because the Board is not regarded as integral to traditional homeland security issues. Jim wanted to change that and will take advantage of all opportunities in the future to insert the Board into the homeland security community. Jim stated he will need the assistance of some Board members and some task force members in this process.

Justice Assistance Grant Program (JAG)

Jim submitted this year's application on March 27th, in advance of the April 3rd deadline. As mentioned in the last meeting, the State officials administering the grant informed Jim the funding has been reduced by over a half and the governing board has established guidelines favoring grants to drug enforcement efforts. Jim attempted to bring the application within that favored scope by stressing (1) the connection between methamphetamine use and identity theft, and (2) the expanding use of electronic devices such as computers and cell phones directly or indirectly to aid in the commission of drug crimes. The group that determines grant awards may meet as early as the end of April. Jim stated the Board has repeatedly and unsuccessfully applied for JAG grants in the past. Jim believes it will be difficult to succeed this year. However, the Board cannot realistically ask for money from the Legislature next year without having applied for a JAG grant.

Budget Submission

Jim stated that Lorrie Adams had prepared and submitted an initial budget request as part of the internal AG's Office process last November. Jim anticipates making changes to that submission based, in significant part, on the discussion to be had under Agenda Item 6.

Jim stated he understands in past years, the Board has not been significantly involved in budget preparation and approval and that needs to change. Jim thinks it important that the

Board review the modified budget submission at its next meeting, as the Director's office will seek considerably more money and new positions. Jim will seek high-level concept approval at the very least, but will be very willing to discuss details if the Board feels it appropriate.

Jim reported authorizing an unusual expenditure. As discussed in the last meeting, the Director's Office arranged for Eric Levin, a Deputy Attorney General in the criminal section to attend out of state training, "Prosecution Responses to Internet Victimization." The National Association of Attorneys General and the National Center for Justice and the Rule of Law make this training available on a no-cost basis. However, due to increased airfares and scheduling issues, Eric's actual flight costs exceeded the no-cost ceiling by several hundred dollars. Jim authorized the expenditure of this additional amount in light of Eric's future planned involvement in a Continuing Legal Education program. The money may be reimbursed depending on actual travel expenses of other Attorney General Office personnel.

No Board Action

4. Discussion, recommendations and actions regarding draft technological crime forfeiture statute.

As discussed at the last meeting, Jim drafted statutory language based on the provisions of the Nevada Racketeering law. Within the last several days, Jim has passed the draft text on to the Board's Counsel, Gerald Gardner, for review and redrafting, probably within the Criminal Division. After that is completed, the Director's Office may seek input from some of Nevada's district attorneys. Jim envisions at least a high-level review by the Board at the next meeting. Assemblyman Anderson has reserved a bill draft number for the legislation.

Jim stated at the last session, Assemblyman Anderson appropriately identified a key sticky issue, "Who will get the cookies?" After considerable thought, Jim's first draft has the cookies going first, to defray expenses of the forfeiture and sale of assets, then into the Board's account. The Board would retain not less than 25% of those forfeiture funds for its use to fund the north and south task forces, and could disperse up to 75% of the funds to federal, State, and local law enforcement agencies based on their participation in the investigation. Further, a fund-sharing arrangement arrived at by the participating law enforcement agencies would be conclusive as to the share ratio determined by the Board.

Jim understands this will be contentious, perhaps before the Board and certainly at the Legislature. Jim suggests this issue be reviewed only after a revised draft is ready and the Board has had the opportunity to go through the Working Paper relating to the mission of the Board and Task Forces.

Jim stated if this does go forward, either Assemblyman Anderson or Senator Wiener might consider asking the Legislative Counsel Bureau Research staff to determine how much money is actually collected under the existing forfeiture statute, for what crimes, and what its disposition is in dollar terms. Obviously, if there is a claim that someone will be

disadvantaged, the Board will want to know if that is true, and by how much.

John Colledge stated a recent Immigration and Customs Enforcement investigation in Reno involved an E-Bay scam that used Moneygram and Western Union to wire-transfer the funds to the Russian Republic. Due to the victims not being Russian, the Russian authorities were hesitant to assist. ICE used the federal forfeiture statute to interdict the funds by serving seizure warrants to both Moneygram and Western Union. The seizure warrants effectively closed down that scam. The scammers have since moved onto other variations of the same scam. The recovered funds were made available for victims to apply for reimbursement. This is a very important tool for law enforcement to use. From what John has seen, the Nevada asset forfeiture law is not as user friendly as the federal law. In effect, law enforcement agencies are being denied the same tools and methodologies, which are available at the federal level, to protect the citizens of Nevada by not allowing intervention of illegal funds.

Jim added as the number of investigations involving electronic devices increase, so will the need for examinations of these devices. Modifying the asset forfeiture statute could assist in the necessary funds needed to support these examinations.

John stated that in no way should the asset forfeiture statute be looked as “money-making venture.” In the case that John discussed, interdicted funds were used to assist victims to come forward and be reimbursed.

No Board Action

5. Update on liaison activities.

Lorrie Adams stated that she attend two National Institute of Justice committee meetings in March. The first meeting was with the National Law Enforcement and Corrections Technology Center-West in Los Angeles. The Los Angeles Police Department and Sheriff’s Office presented their latest technology projects. Due to the nature of the technology, Lorrie cannot share the details; however, Lorrie has shared the information with local law enforcement.

The second meeting was with the Electronic Crime Partnership Initiative in Las Vegas. The group finished their peer review of the guide, Electronic Crime Scene Investigation: A Guide First Responders. Lorrie received permission to use the draft version to create patrol briefings and will continue to work with John Colledge on police academy curriculum. Lorrie cautions that as the task force and Board raise awareness to electronic evidence potential seizure, the need for examination will also rise; causing a flood of technical assistance calls for the task force members.

Lorrie stated that the use of the term “Cyber Crime” is diminishing on a national basis, except when applied to pure Internet fraud. Other states are realizes that a more accurate description is “electronic evidence.”

Jim added that the submitted grant proposals discussed this concern of raised awareness by adding State personnel to both laboratory facilities.

Electronic devices are becoming integrated in most everyone's lives. Handling these devices are everyday law enforcement issues, much like issuing a speeding ticket to a motorist. Today, electronic evidence is what DNA evidence was fifteen to twenty years. At first, DNA science was considered "fuzzy" science until the techniques for handling, examining and presenting became standardized. Electronic evidence collection, handling, examining and presenting must become standardized.

Jim Earl stated that he had been invited to testify before the Legislative Committee on Health Care, Subcommittee to Study Services for the Treatment and Prevention of Substance Abuse. Assemblywoman Shelia Leslie is the chair. This group was established by legislation last session. Its focus has been on methamphetamine use. Jim will explain the relationship between methamphetamine and Internet identity theft. Jim will suggest that as the supply of meth precursor ingredients continues to dry up, the expectation less of manufacture and more importation into Nevada. This will likely mean that information related to meth distribution, and the identity theft that provides funds for meth purchases, will increasingly be found on computer hard drives and in cell phone memory. Jim will address the importance of first responder training, the need for task force funding, and the need to deprive meth distributors of profits and possible new forfeiture legislation.

Jim stated in the Working Paper under Agenda Item 6, the Director's Office has an invitation from the Intellectual Property Section of the Nevada Bar Association regarding the prevention of network penetrations, data theft, and international espionage. The Director's Office also has tentative invitations from the Nevada Association of Sheriffs and Chiefs in May and from the Nevada Prosecution Advisory Council this fall.

6. Discussion, recommendations and action regarding future mission strategies of the Advisory Board and Nevada Cyber Crime Task Force.

Jim Earl led the Board through a discussion on the submitted Working Paper. Jim made note to add ICE to Task 1, Working hypothesis. Also, based on the survey, some rural agencies indicated their electronic evidence was sent to Washoe County Sheriff's Office, Crime Lab for forensic exam. The Crime Lab does not actually conduct computer forensic examinations; the evidence was probably forwarded to other local agencies for examination.

Jim stated that he over summarized the activities of ICE and FBI in Task 2. Jim added ICE investigates trafficking and counterfeit merchandise; identity theft is viewed as part of the much large crime of Internet fraud. The FBI also investigates computer intrusions, homeland security and intellectual property theft, such as copyright infringement and industrial espionage.

Jim reiterated that as the awareness of electronic devices and evidence increases, so will the need for trained personnel to exam the devices. The State will need to address this problem.

John Colledge stated the forensic equipment required is costly. For example, according to a recent advertisement, a Samsung cell phone is able to hold 8MB of data. The necessary forensics equipment to examine that type of phone currently costs about \$20,000. To the best of John's knowledge, there is no law enforcement agency in Nevada that has the money to purchase the equipment. Certainly at the federal level and outside of Nevada, the equipment is available, but is in high demand from other law enforcement agencies. This again raises the concern that Nevada law enforcement must seek outside assistance.

Lorrie Adams added that the SEARCH, the National Consortium for Justice Information and Statistics, in conjunction with an Internet Crimes Against Children (ICAC) grant, recently spent \$10,000 per student in cell phone forensic equipment for a pilot class for 20 students for a total of \$200,000.

John stated that purchasing the equipment is certainly not the end of the process, training computer forensic examiners to use the equipment is essential. In addition, raising the awareness with all levels of law enforcement of what kinds of data and amount of data that can be found on cell phones will impact investigations.

Jim stated that he would like to add a recommendation regarding legislation on Internet safety programs to be taught in schools. Jim referenced an email he sent to the Board on the recent Virginia State Statute.

Chris Finnegan asked if Jim was asking the Board to require Internet safety be taught in schools or asking the Board to recommend that Internet safety be taught in schools.

Jim stated he was asking for Board direction of this issue and if so how. For example, would the Board like to review the Virginia statute and make necessary changes to fit Nevada in the upcoming legislative session?

Bill Uffelman suggested looking at existing curriculum regarding online education and possibly add a line for Internet safety programs. This may avoid the concern of "yet, another thing to teach to students."

Jim stated that Bill made a fair comment. Jim stated he sent a letter to Keith Rheault, Superintendent, Nevada Department of Education regarding Internet safety programs being taught in schools and has received no response. Jim said he would follow up with Superintendent Rheault on this issue as well as any potential legislation based on the Board's recommendation.

Bill stated that given all of the recent mandates placed upon the education system, the Department of Education may be engaging in an equal opportunity and universal push back.

Eric Vanderstelt stated that the FBI continually receives requests for presentations on Internet safety from middle school and high school parents, specifically myspace.com. Eric stated he understood that a more formalized relationship is being sought with Clark County School District.

Jim stated he would like to point out, based on the survey results, there is considerable interest expressed by local law enforcement agencies to present information to schools and parent groups. The second set of CDs to be sent to local law enforcement agencies contains a CD focusing on Internet Safety for parents of elementary-aged children. This CD is independent of i-Safe and Netsmartz programs. Lorrie and Jim looked at a way of being to disseminate Internet safety without endorsing any one specific program. Jim was hoping to be able to work with the Department of Education to provide assistance in providing information on Internet safety. Jim had thought about contacting parent-teachers organizations; however this was considered impracticable due to the number of such organizations and the yearly turnover of officers. Since the idea of top-down presentation is not currently available, Jim would like to provide law enforcement agencies with materials to present to schools in their jurisdictions.

John stated he would like to propose the idea of a speakers bank where we could identify various member agencies that have personnel that are very adept at presenting to schools.

Lorrie asked Tom Pickrell as if the concern about “outsiders” going into schools to make presentations would apply to the suggestion of a speakers bank.

Tom stated yes, that we need to be cautious about whom we send into the schools. In addition, Tom stated that the pilot program discussed in the last meeting is finishing up with the first class with middle school teachers. The program will be expanded to elementary school teachers.

Lorrie stated that the National Institute of Justice is going to hold a “symposium” on Child Internet Safety in the fall of 2006. The Electronic Crime Partnership Initiative held a round table discuss during the last week of March in Las Vegas. The groups of 30 individuals brainstormed about who to invite, as well as who should be asked to be keynote speakers. NIJ and ECPI have purposely planned the symposium to be held in Washington DC in fall in order to draw the attention of Congress and current political candidates for the desperate need for a national awareness on Internet Child Safety. Lorrie stated she suggested the event be held in the month of October, as it is also Cyber Security Awareness Month and Domestic Violence Prevention Month, as well as the month between primary and general elections in most states. Lorrie stated she has volunteered to assist in organizing and coordinating this event. As the round table discussion was just held, she has no further information to share.

John stated that there seems to be a number of approaches to this issue. Perhaps a subcommittee could be established to review the approaches. John asked if Tom would be interested in being a part of that subcommittee.

Tom stated yes he would and reiterated that the Clark County School District is always available for other school districts to use.

Jim would like to establish the speakers bank previously mentioned and provide that list to the schools to be used at their discretion.

John suggested possibly go beyond the educational system to the civic groups, such as rotary, lions or elks or any other group that has concerned parents. These groups may be able to provide assistance to local agencies when presenting schools and parents.

Lorrie asked Chris if she could contact him in regards to recontacting the Department of Education for establishing a relationship.

Chris said he would be willing to use his office's contacts to help in establishing that relationship.

Jim reiterated on Task 4 that the Department of Information Technology has expressed an interest in developing a civil computer forensic center and would like to ensure that the budget proposals are complimentary.

Chris stated for the record that the Office of Information Security is only seeking two additional positions in contrast to the several mentioned in the Working Paper. Also, OIS wholeheartedly supports the task forces in expanding their computer forensic capabilities.

Jim stated that there is no conflict between regarding the expansion of OIS computer forensic positions and that of the task forces. Jim stated that the budget should compliment and support each other.

Jim stated has nothing to add to Tasks 5 and 6 and is open to any comments from the Board.

John asked if there was any further comment on the tasks or recommendations presenting in the Working Paper. Perhaps members could provide their comments to Jim over the next weeks.

Bill asked if a decision could be put off until the next meeting, assuming the next meeting will be held in the next 30 to 60 days due to the short time available to review the Working Paper.

Gerald Gardner stated the Board would do that if it wishes. In addition, Gerald was asked by Attorney General Chanos to commend Jim on the substantive nature of the Working Paper and was looking forward to this meeting unfortunately he missed his flight.

Valerie Wiener pointed out that due to upcoming department budget deadlines, as well as bill draft requests for the upcoming legislative session perhaps voting on the Working Paper would be better today than to wait.

Gerald stated that Valerie is correct in her remark. The deadline for bill draft requests for the Attorney General's Office is within the next few days. Gerald cautioned the Board about providing comments that might be interpreted as a vote, thus violating the Open Meeting Law. Perhaps the Board could propose a motion to accept the Working Paper as a whole, unless a member has any grave concerns.

Lorrie stated she has already submitted a budget request within the Attorney General's Office for the expansion of computer forensics capabilities with the addition of computer forensic examiners, investigators, a data analyst and a prosecutor, as well as the funds needed for training and travel funds.

Jim stated that he and Lorrie are planning on revising the budget request to include two addition computer forensic examiners.

Board action:

- *Valerie Wiener proposed accepting the Working Paper as presented.*
- *Bill Uffelman seconded.*
- *Motion unanimously passed.*

7. Discussion, recommendations and actions regarding responses to existing and emerging technological threats.

- a. Bill Uffelman stated a "two step" security requirement will undoubtedly become fairly common in the not too distant future. For example some banks now allow you to look at your account with a single password, but to not move money without a second security step. The difficulty is consumer push-back on remembering another password or having a key fob and or other mechanical device. If access is made too difficult, consumers will not want to use electronic banking despite the possible advantages. Of course many of these are the same consumers who don't update their security software in the first place and insist on opening suspect/labeled virus laden emails.

Bill also stated that identity theft insurance is on the rise. This type policy reimburses victims for the cost of restoring their identity and repairing credit reports

Jim Earl stated there is a challenging trade-off when addressing technology changes and ease of use for customers.

- b. State Security Committee activities update was tabled, to be discussed at a future meeting.

8. Discussion, recommendations and actions regarding Southern Task Force activities.

Eric Vanderstelt stated that the southern laboratory expansion is complete. Eric and Karen Francis, Detective Sergeant, Interne Crimes Against Children unit, Las Vegas Metropolitan Police Department, are onsite full-time.

In addition, Eric stated the lab recently held an advanced network intrusion analysis training class with eighteen students.

Karen stated that Sheriff Young hosts a “First Tuesday” monthly meeting. The most recent meeting was on Internet Crime and Child Safety and was attended by hundreds of citizens.

Karen stated that Craig Ronzone, Department of Public Safety, is now in Elko. Las Vegas Metro already has a forensic machine in already place that is shared by both Elko Police Department and Elko Sheriff’s Office, in order to establish another Internet Crimes Against Children task force. Craig will be able to assist both agencies with forensic examinations.

Karen stated she is working Nevada Child Seekers to provide grant money in order to provide professional development training materials for Clark County School District teachers and child safety materials for parents. The materials are well established however one challenge is getting teachers and parents in the classroom to receive the materials. Karen is looking forward to getting this outreach going.

9. Discussion, recommendations and actions regarding Northern Task Force activities.

John Colledge stated that Reno Police Department has moved a forensic machine into the northern laboratory. Chuck Lovitt, Detective Sergeant, Reno Police Department, has devised a rotation schedule for his detectives. One detective will spend one day per week in the lab working with Melissa McDonald, Special Agent, Immigration and Customs Enforcement, to receive on the job training and conduct peer reviews.

In addition, John stated Paul Hales, Department of Public Safety, is working part-time in the lab working with Melissa.

John stated that the working relationships with RPD and DPS will enhance the forensic capability of the northern task force. This will enable a quicker turn around for service requests.

John stated ICE was the lead agency in an international child porn chat room case leading to the arrest of a Reno resident. ICE worked with RPD, US Secret Service and LVMPD. This case is a great example of the kinds of resources Nevada has when a pressing investigation emerges. One of the main reasons for asking for assistance from the other agencies, is ICE anticipated the need to seize and exam up to four terabytes of child porn.

John reiterated that Lorrie is working with the northern task force first responders training. This training will be pushed out to the south, as well rural areas.

Lastly, John noted that Sylvia Redmond, Detective Sergeant, Internet Crimes Against Children, Washoe County Sheriff’s Office, is onboard, replacing Dave Nikoley, who has been promoted. Sylvia will start working Melissa on forensic examinations.

10. Board Comments

No Board comments.

11. Public Comments

No Public comments.

12. Scheduling of next meeting.

The next meeting is scheduled for Monday, July 10, 2006, 10:00 AM, location to be determined.

Notice of Public Meeting

Nevada Advisory Board for Nevada Task Force for Technological Crime
July 10, 2006

10:00 am

*Room 2134 of the Legislative Building
401 South Carson Street, Carson City, Nevada*

Via Videoconferencing

*Room 4412 of the Grant Sawyer State Building
555 East Washington Avenue, Las Vegas, Nevada*

AGENDA

1. Call to Order.*
[George Chanos]
 - a. Verification of quorum
2. Annual election of Board Chairman and Vice Chairman.*
3. Discussion and approval of minutes from April 7, 2006 Advisory Board Meeting.*
[Chairman]
4. Introduction of new Board Member, Special Agent in Charge Steve Martinez, Federal Bureau of Investigation.
 - a. Remarks by Steve Martinez on existing and emerging threats.
5. Report, discussion, recommendations and actions regarding Northern Task Force activities.*
[Concerned Agencies]
6. Report, discussion, recommendations and actions regarding Southern Task Force activities.*
[Concerned Agencies]
7. Report, discussion, recommendations and action regarding funding sources and budget for Advisory Board and Task Force activities.*
[Jim Earl and Lorrie Adams]
 - a. Homeland Security Grant application
 - b. Justice Assistance Grant Program (JAG) application
 - c. Budget submission for fiscal years 2008 and 2009

8. Report, discussion, recommendations and action regarding changes to NRS Chapter 205A, the Board's underlying statute.*
[Jim Earl]
9. Update on liaison activities.
[Lorrie Adams]
10. Discussion, recommendations, and action regarding data compromise at the Department of Veterans Affairs.*
[Jim Earl]
11. Board Comments.
12. Public Comments.
13. Scheduling of future meetings.*

* Denotes a possible action item. The order of the agenda items is subject to change.

This agenda has been sent to all members of the Advisory Board and other interested persons who have requested an agenda.

Unless otherwise stated, items may be taken out of order presented on the agenda at the discretion of the chairperson. The meeting may be recorded. Some Board members may attend the meeting via telephone conference.

Members of the public who are disabled and require special accommodations or assistance at the meeting are requested to notify Lorrie Adams at (775) 688-1813 twenty-four hours prior to the meeting.

THIS MEETING HAS BEEN PROPERLY NOTICED AND POSTED AT THE FOLLOWING LOCATIONS:

Office of the Attorney General
5420 Kietzke Lane, Suite 202
Reno, Nevada 89511

Office of the Attorney General
555 East Washington Avenue
Las Vegas, Nevada 89101

Office of the Attorney General
100 North Carson Street
Carson City, Nevada 89701

Reno City Hall
1 East First Street
Reno, Nevada 89501

Nevada Advisory Board for Nevada Task Force for Technological Crime
Nevada Cyber Crime Task Force
July 10, 2006
Meeting Minutes

*Room 2134 of the Legislative Building
401 South Carson Street, Carson City, Nevada*

*Via Videoconferencing:
Room 4412 of the Grant Sawyer State Building
555 East Washington Avenue, Las Vegas, Nevada*

1. Call to Order.

Attorney General Chanos called the meeting to order at 10:04 AM and requested a roll call of the present Board members.

Present:

George Chanos, Nevada Attorney General (AG)

John W. Colledge, III, Resident Agent in Charge (RAC), Immigration and
Customs Enforcement

Don L. Means, Commander, Forensic Science Division, Washoe County
Sheriff's Office

Steve Martinez, Special Agent in Charge (SAC), Federal Bureau of Investigation
Senator Valerie Wiener

Staff in Attendance:

Lorrie Adams, Secretary

James Earl, Executive Director

Gerald Gardner, Legal Counsel

Others:

David Atkinson, Assistant Crime Lab Director, Washoe County Sheriff's Office

Karen Francis, Detective Sergeant, Internet Crimes Against Children, Las Vegas
Metropolitan Police Department

Matt Goward, Special Agent (SA), Department of Energy, Inspector General

Gwen Hadd, Deputy Homeland Security Administrator, State of Nevada

Paul Masto, Supervisory Special Agent (SSA), US Secret Service

2. Annual election of Board Chairman and Vice Chairman.

AG Chanos asked RAC Colledge, as Vice-Chair, to handle the election of the
Chair.

Board Action:

RAC Colledge proposed Attorney General Chanos be elected Chair.

Commander Means seconded.

Motion unanimously passed.

Board Action:

Commander Means proposed RAC Colledge be elected Vice-Chair

Attorney General Chanos seconded.

Motion unanimously passed.

3. Discussion and approval of minutes from April 7, 2006 Advisory Board Meeting.

Board Action:

RAC Colledge proposed the minutes to be accepted with no corrections.

Senator Wiener seconded.

Motion unanimously passed.

4. Introduction of new Board Member, SAC Steve Martinez, Federal Bureau of Investigation.

AG Chanos welcomed SAC Martinez.

SAC Martinez commended Special Agent Eric Vanderstelt for his work to keep the cyber unit going. The FBI has been involved with the cyber crime world since mid-1990s. Following the 9-11 terrorist attacks in 2002, the FBI Director recognized that cyber crime is an area that needed to be addressed. He pooled the existing resources, which included child exploitation in the Violent Crime Program, computer fraud in the White Collar Crime Program and criminal and national security computer intrusion in the National Infrastructure and Protection Center (NIPC), together into a cyber program. SAC Martinez's most recent position before coming to Nevada was Deputy Assistant Director of the cyber program; many times he was Acting Director. Cyber is the third of ten priorities of the FBI; counterterrorism and counterintelligence are first and second. The cyber program has the following priorities: national security related intrusions, criminal intrusions, child exploitation, intellectual property, economic espionage and fraud, such as ID theft. "We are working very hard to establish cyber issues as one of the four operational programs in the FBI. The others are counter terrorism, counter intelligence and traditional criminal work."

The threat picture, as viewed by the FBI, includes the convergence of hackers and fraudsters. "We now have hackers working for hire. They are facilitating internet frauds. The 'Mytob' and 'Zotob' worm investigations are examples of this convergence, 'a perfect storm that is brewing.' Our national security issues are by far our highest priority." SAC Martinez continued by saying that "Nevada has a disproportionate number of national assets between Department of Energy Department of Defense and other projects that are target rich for our enemies. We are addressing this aggressively." Data theft is a national and congressional concern. Congress is looking into mandating reporting requirements. The greatest concern is the threat of hackers working for terrorists. "We will be looking hard for this."

SAC Martinez is excited to be a part of this Board. He recently visited the off-site lab and feels the environment encourages collaboration, technique and information sharing. "We are ahead of others in Las Vegas and Nevada by being able to leverage combined agency resources."

AG Chanos thanked SAC Martinez for his comments.

AG Chanos thanked SSA Masto for attending on behalf of if the US Secret Service. AG Chanos extended an invitation, through SSA Masto, to Attorney General candidate Catherine Cortez-Masto to attend future Advisory Board meetings.

SSA Masto thanked AG Chanos for the acknowledgement. He is grateful for the opportunity to introduce himself and learn more about the task force. Referencing SAC Martinez' remarks, SSA Masto stated US Secret Service, by working with other agencies, can leverage their assets; it is "us against them, not us against us."

5. Report, discussion, recommendations and actions regarding Northern Task Force activities.

RAC Colledge stated the work environment continues to improve with participating agencies either donating or supplying equipment and supplies. He acknowledged Reno Police, Washoe County Sheriff, FBI and Attorney General for their contributions. Storey County Sheriff's Office would like to start participating. A new deputy with a computer science background has been helping out; his participation will increase, as will that from DPS. RAC Colledge wanted to highlight some of the non-tradition cyber crime cases that have been investigated. Most people related cyber crime to ID theft or child exploitation. The Northern Task Force certainly continues to investigate these types of cases. RAC Colledge provided an update on their most recent case involving a large international child porn operation, in which US Secret Service and Reno Police Department assisted. The accused person pled guilty and must serve ten years in prison; other defendants are facing 25 year prison terms. The task force has recently assisted in investigating cases for Nevada gaming, DPS and a Reno Police Department homicide. Because these cases are not ICE cases, RAC Colledge did not provide more detail. RAC Colledge wanted to report to the Board the diverse agencies and crimes that the Northern Task Force is facing. It is important that the Board, Nevada Legislature, State government and the general public are made aware that "High Tech Crime" involves every type of traditional crime faced by law enforcement.

RAC stated that due to diligent work, the first responder training program is progressing. Secret Service has agreed to assist in providing roll call, patrol briefings for a number of local northern agencies. These briefings are designed to provide officers and troopers fundamental information on electronic evidence at crime scenes, not just fingerprints, blood samples and weapons. "We want to ensure they have a basic knowledge of what to look for." A contact list from the task force will be distributed to agencies to assist when handling electronic

evidence to ensure proper handling and examination. "We will supply telephonic support and will dispatch people to assist the officer, if necessary. This assistance will help ensure that digital devices are treated as evidence, rather than being booked as property when a crook is jailed; only to be returned when he is released on bond. We do not want digital evidence to leave with the crook." In addition, POST is looking at integrating electronic evidence into the tradition coursework.

6. Report, discussion, recommendations and actions regarding Southern Task Force activities.

SA Goward discussed a recent case involving the US Secret Service Los Angeles Electronic Crime Task Force's Clean Room Lab and agents specializing in harddrive recovery. In a last ditch effort, he sent the drive this lab. The harddrive was considered "dead" and irreparable. Unfortunately, this case was dependent upon the evidence contained on the harddrive. After five weeks and three different controller boards, the detectives were able to get the harddrive working long enough to create an image. "This case is great example of how leveraging resources and expertise will allow complex cases to be investigated and prosecuted. Once the evidence was presented to the defense, the defendant immediately requested a plea agreement." SA Goward thanked the Secret Service for its assistance.

SAC Martinez joined in complementing the Secret Service Los Angeles Lab. He stated that the FBI has special agents assigned full-time to the Secret Service Los Angeles Electronic Crime Task Force largely because of the size and quality of the facility. This is a rare situation to have an entire FBI squad within a Secret Service Task Force. He is proud of this arrangement; it has been working very well and is available to us in Nevada. This further emphasizes the advantage of leveraging agency resources and expertise for investigations. He said that his career has involved task force participation, noting that virtually every case he was worked has been within a task force setting.

Mr. Earl reported he and Mr. Gardner visited the Southern Task Force recently. They were impressed with the methodology demonstrated by the Internet Crimes Against Children unit.

Detective Sergeant Francis discussed a case where a 51-year old male, a Reno lawyer from a prominent family, admitted to using his work computer at the law firm to commit his crimes. He must serve five years in prison and pay a \$10,000 fine for receiving hundreds of child porn images via the Internet. This case was jointly investigated by Las Vegas Metropolitan's Internet Crimes Against Children and FBI's Innocent Images Initiative, both participating as part of the Southern Nevada Cyber Crime Task Force.

7. Report, discussion, recommendations and action regarding funding sources and budget for Advisory Board and Task Force activities.

a. Homeland Security Grant application

Mr. Earl stated the Nevada Homeland Security Commission is continuing its progress reviewing the grant applications within Nevada now that the Federal Awards have been made to the individual states. Mr. Earl acknowledged Gwen Hadd from the commission is attending today's meeting. Gwen works closely with the commission members. He pointed out that SAC Martinez is now a member of that commission. Mr. Earl has been attending Nevada Homeland Security meetings. Mr. Earl hopes that the joint staff coordination will assist meeting the challenges identified by SAC Martinez. It may be several months yet before a decision is made on the Board's application in support of the task forces.

b. Justice Assistance Grant Program (JAG) application

Although not unexpected, the Advisory Board's application was denied funding. Overall, the available grants funds have been reduced by about 60% and only existing programs were funded.

c. Budget submission for fiscal years 2008 and 2009

The proposed budget, which was initially created by Ms. Adams when she was Interim Director, has been slightly increased. Copies of the revised budget request have been supplied to the Board and the Chief Finance Officer, Attorney General's Office. "We have modified the budget to reflect the recent review of the Board's mission. Most importantly, additional personnel, forensic examiners and information security officers, have been requested along with the associated necessary equipment, training and travel costs." Based on types of cases that have been presented today, Mr. Earl anticipates the requests for service will increase quickly. "Presently, to the best of our knowledge, forensic service requests are handled by a single, full-time State employee associated with the Southern Task Force and computer forensic examiners from ICE, US Secret Service and FBI. We are anticipating asking the legislature for a dramatic increase in the number of State forensic examiners and investigators. This is driven both by the threat identified by SAC Martinez and training of First Responders explained by RAC Colledge. Clearly, as Nevada's First Responders become aware of the importance of digital evidence in the solution of all crimes, demand for forensic services will increase."

At present, State demands for digital evidence examinations are met by employees of the three federal agencies, FBI, ICE and USSS. With Board approval, he will press as firmly as possible for the increase in State personnel dedicated to technological crime. He invited the Board members to question and discuss the budget request. Ideally and Board request will flow through the AG's Office to the Governors' Office, will be addressed by the new elected officials and transmitted to the next Legislature. He again invited Board involvement in the budget process.

Ms. Adams clarified the budget request. Local and federal agencies work on a rotation basis. A detective or special agent is trained in computer forensics, remains in the position for two to three years and then either is promoted or transfers. These agencies will continue to have this “gap” of training personnel. “The Attorney General’s Office and other State agencies are in a strategic position to provide an infrastructure for processing electronic evidence, as well as investigation.”

AG Chanos asked the federal agencies whether their resources should be supplemented by the AG’s Office for the reasons outlined by Ms. Adams. AG Chanos stated he would like to hear from the legislative members of the Board on how they feel about the probability of success with the legislature.

SAC Martinez stated the likely impact will be for the FBI to refocus its limited resources. An increase in State forensic examiners would be particularly important. Any assistance the Attorney General’s Office can provide is greatly appreciated. The FBI has a hard time even now keeping up with the amount of digital evidence it receives. Digital evidence is appropriately seized in almost any crime regardless of who investigates it. “The volume will only get larger and larger. Harddrives continue to get larger. This also vastly increases the amount of evidence that must be examined.” Again, FBI has a national security focus, counterterrorism and counter intelligence, which is ahead of cyber crime. By the Attorney General’s Office providing resources, the FBI will be able to maintain its resources for high priority cases involving national security. The addition of computer forensic examiners will assist in meeting the forensic load.

RAC Colledge stated that his law enforcement career started in Arizona with a Phoenix area Sheriff’s Office and then onto Customs in Southern Arizona. The local and federal agencies work very closely with Arizona Attorney General’s Office in investigations. It was not uncommon for Customs and the Drug Enforcement Agency to present cases to the Attorney General for prosecution, many times using the racketeering statute. Arizona has recently completed several long term investigations, which involved complex ponzi schemes, without federal assistance. Nevada is a rapidly growing state where federal law enforcement personnel are citizens who pay taxes. Collectively, the officers of the federal agencies owe themselves and other citizens a safe environment for children to access the Internet. “We also have a collective responsibility to provide a safe environment for existing, expanding and new businesses to operate. We in Nevada need to provide adequate law enforcement resources at every level. All federal agencies have priority areas and limited resources; FBI with national security and ICE with immigration. An incident can occur, at any time, where the federal agencies must

respond, leaving Nevada citizens grossly lacking adequate resources to address forensic examinations now done by the federal agencies.”

SSA Masto stated Ms. Adams’ observation accurately describes what needs to be done. Federal personnel come and go, but Nevada personnel remain. More are definitely needed. SSA Masto would like to see more participation from the Attorney General’s Office in each others task forces. “The Secret Service task force has deputized, through the US Marshal’s Service, their entire local and State participants. This gives State and local law enforcement personnel federal authority when chasing criminals across state lines; it is integral to making arrests where the crime spans several states. Training is expensive and must be ongoing. Technology is constantly changing. Forensic examiners must go to classes constantly to remain updated. This week the US Secret Service is having a conference for all of their task forces.” SSA Masto invited everyone to attend. In summary, more analysts must be trained and the US Secret Service can help facilitate the training.

AG Chanos would like to have Mr. Earl attend the conference, if possible. He then observed there is broad support for more State personnel. “Our decision will ultimately rest with the Legislature. How can we get this done, what do we need to do as a Board? What can the Board do to make this happen in the Legislature?”

Senator Wiener said she spoke as a bit of an outsider, since she did not sit on the Senate Finance Committee. Senator Wiener noted getting this budget proposal incorporated into the Attorney General’s budget and then into the Governor’s budget is pivotal. “Things have changed since I became a legislator. Now, items must be in the budget in order to get a hearing before the money committees. Typically, budget proposal that are not part of the Governor’s budget are viewed as special projects and only receive one-time funding. This proposal is not a special project and needs to receive ongoing funding. Ensuring this budget request is included in the Governor’s budget is crucial.” She will support the proposal. In addition, having ICE, FBI and Secret Service testify on behalf of the budget will go a long way in the legislative session. “This is a profound message of need.”

AG Chanos noted he will do his best to keep this proposal part of the Attorney General’s budget and work with the Governor’s Office to have included in the overall State budget. He asked for additional comments on the budget.

SAC Martinez noted the inclusion of Information Security Officers in the budget. “This type of position is important. Other states are having difficulty with data retention issues. From a liability standpoint, there is

enormous exposure for state governments to operate day-to-day with large databases of personnel information. Articulating this issue to the legislature is important.”

AG Chanos observed a consensus had emerged from the discussion to move forward with the proposed budget.

Board Action:

Senator Valerie proposed the budget proposal be approved, incorporated into the Attorney General’s budget and that the Attorney General’s Office work with the Governor’s Office to obtain the necessary funding to implement the Board’s proposed budget.

SAC Martinez seconded.

Motion unanimously passed.

8. Report, discussion, recommendations and action regarding changes to NRS Chapter 205A, the Board’s underlying statute.

Mr. Earl had put together proposed changes based on the Mission review and previous Board discussion.

Mr. Earl suggested shortening the name of the Advisory Board.

Attorney General Chanos suggested the Board be called Technological Crime Advisory Board.

Mr. Earl addressed the title of section .080. “When Ms. Adams initially formulated the budget, she quite appropriately made arrangements with AG staff that any forensic examiners and investigators in the Board budget actually be employed in the AG’s Office. The question is, whether these people should be employed by the Board directly or work for supervisors within the AG Office. I do not know the Board’s preference, but thought it appropriate to put forward the language patterned on that in the Private Investigators Board statute, allowing the Board to staff itself.”

AG Chanos stated for practical and logistical purposes having staff supervised by the Executive Director is perhaps better than by the AG’s Chief Investigator and IT staff. He said that “While this made sense from a mission perspective, it would raise the issue of whether that was consistent with the name ‘Advisory Board.’ We would be doing more than advising.”

Mr. Gardner stated that the Advisory Board is quasi-related to the Attorney General’s Office, not a subdivision, and having the ability to supervise staff may be beneficial. In the past, cross-supervision has been problematic in other areas.

Mr. Earl stated the current Attorney General employee who is assigned to the task force is supervised on a day-to-day basis by the Task Force. “By having the

Attorney General staff located within the labs, the staff are given practical exposure and included in ongoing training. The peer review provided by more experience forensic examiners is a very important component of the task force organization. Regardless of whether employees work for the AG's Office or the Advisory Board, in fact their day-to-day work will likely continue to be supervised by the Task Force members on-site. The language proposed is permissive in that it allows the Board to hire, but does not require the Board to do so. There are, of course, advantages to being within the AG's Office, depending on how active the Office is in moving aggressively on technological crime."

AG Chanos said "The real question was what would be in the best interests of the State regarding management of these activities." There are several possibilities: (1) the Board drops "Advisory" from its name and becomes a more stand alone operation; actually managing the assets the legislature commits; (2) the assets are managed by some apparatus within the AG's Office, "while we have an IT staff, some future examiners will quickly eclipse the knowledge of that IT staff" and (3) the management could come from a Deputy Attorney General. "I want to do what is best for the State."

SAC Martinez stated if the Board moves beyond advisory, he would need to an internal FBI legal review to determine if he could continue since federal agencies are not generally permitted to direct State or local financial assets. However, the driving factor is the tasks of new employees. If the staff is for investigative and computer forensic purposes, it should fall under the Attorney General's Office because there is an existing framework to supervise people with those job skills.

Mr. Earl clarified any misunderstanding regarding the terms "forensic examiner" and "information security officer." These are the same thing within the Board's budget because the State Personnel system does not yet have a classification for "computer forensic examiner." New investigator positions would augment the forensic examiners now identified as ISOs in the budget.

AG Chanos acknowledged the staff clarification. "However, who supervises the staff has not been made clear. I understand it may be problematic."

Mr. Gardner stated he saw no statutory or constitutional problem with Mr. Earl serving as Executive Director of the Advisory Board in an Ex-Officio, unpaid capacity. "There is a practical problem in asking the Legislature to create a new Senior Deputy Attorney General position and simultaneously defund the Executive Director position, but that does not mean it cannot be done."

AG Chanos stated that we now need to figure out how to accomplish this logistically within budget constraints. The Department of Personnel probably should be consulted.

RAC Colledge suggested that the investigators, particularly if they were peace officers should be supervised within the structure of the Attorney General's Office. "This is also true of forensic examiners. In order to avoid problems observed in the past, it is probably best to have staff under the Investigative Unit within the AG's Office."

AG Chanos stated under the current structure of the Attorney General's Office maybe Mr. Earl is better suited to supervise the staff. "Perhaps Mr. Earl's position needs to be reclassified as a Senior Deputy Attorney General. He could then manage these new assets."

Mr. Gardner stated that his concern regarding the Board managing Executive Branch employees. Senator Wiener, as a member of the Legislature, would be unable to serve on any Board with executive powers. This would likely be problematic if examiners were managed by the Board. Currently, Chris DeFonseka, the AG employee, is supervised by the Investigation Division. He believes that the proposed staff should be supervised by the investigative unit. Reclassifying Mr. Earl's position is not necessarily a problem. "His salary would have to be provided differently and structured outside the Board's budget. We should consider how to restructure, so he could oversee new executive positions."

Mr. Earl stated that make-up of the Advisory Board on Nevada Criminal justice Information Sharing provided an analog. The Executive Director of that Board is a full-time employee of the Department of Public Safety.

AG Chanos observed that was the most logical approach considering all of today's discussion.

AG Chanos noted that the Executive Director salary in the presented budget is commensurate with a Senior Deputy Attorney General. "It makes the most sense for Mr. Earl to be hired as a Senior DAG. The Board could then determine he would act as Executive Director, much as Mr. Gardner acts as Legal Counsel. Doesn't this solve the problem of asset management? Otherwise, we would have duplicative salaries. One for the Executive Director and one for the person the AG's Office hires to supervise new employees. We do not have that supervisory capacity now."

AG Chanos confirmed that the Board was in consensus to have Mr. Earl's position reclassified into the AG's Office and for him to serve in an uncompensated Executive Director of the Board.

In addition, AG Chanos stated NRS 205A.080 will change to "employment of administrative staff personnel." As a consequence of this decision, to ensure only administrative personnel were hired by the Board.

Mr. Earl suggested adding “forfeiture” to the title line of NRS 205A.100. The substantive provision will be addressed later in the statute’s review.

Board had no objections.

Mr. Earl suggested adding “attempt to commit any crime, or conspiracy to commit any crime” to NRS 205A.030.

Board had no objections.

Mr. Earl outlined two options for increasing the size of the Board based in the Mission review and the Board’s interest in including a representative from Las Vegas Metropolitan Police Department. The two options are distinguished by the number of members the Governor would appoint in the categories described in the current statute. The first option would expand the Governor’s discretionary appointments from five to eight; the second option would expand the Governor’s appointments from five to eleven.

As an illustration only, if the Board membership were to be expanded under option one, then the total number of Board members would expand to twelve. Mr. Earl recommended use of the Board expansion to include representatives of the three federal agencies most involved in electronic forensic investigations in Nevada: FBI, ICE, and USSS. The economic sector representation might be expanded to include a representative from the gaming community, in addition to the present banking representative. A representative from LVMPD could be added to the current local law enforcement representative from Northern Nevada.

If the Board membership were to be further increased under option 2 to a total of fifteen, then three additional Board members could be added. In addition to the Option 1 recommendations, Mr. Earl suggested another representative from the technological community, such as Intuit. He also suggested another local law enforcement representative, specifically the head of the Nevada Sheriffs and Chiefs Association. Lastly, another educational institution representative could be added such as, the Superintendent of a middle-sized school district.

Mr. Earl stressed the illustrations were only an illustration. The new governor would have complete discretion regarding whom to appoint, if the statute were modified.

AG Chanos asked the Board which area, federal law enforcement, local law enforcement, technology or education, would be most important to augment when considering Board expansion. “Are new members in any of these areas sufficiently important to offset the competing disadvantage of having a larger and perhaps more unwieldy Board?”

After determining the Board was in agreement to recommend expansion to eight discretionary appointments (adding for example USSS, LVMPD and a gaming industry representative), AG Chanos asked for Board input on the next most important addition.

RAC Colledge would like to see someone from technology due to its rapid growth. “This person could provide an important perspective for the Board and the task forces. This sector is greatly impacted by technology crimes and information privacy issues.”

AG Chanos, while he would agree, asked if any Board member thought a representative from the Sheriffs and Chiefs or from a mid-sized school district would be more important.

Senator Weiner noted that the Attorney General was also included as a Board member, so she was comfortable with law enforcement representation. She noted the importance of having an odd number of total members to help avoid a voting deadlock.

RAC Colledge suggested some type of rotation in the category of “educational institution.”

AG Chanos responded that the present wording of the statute would allow for the Governor to appoint someone other than from Clark County School District. This option would continue to be open.

SA Goward asked if the industry trade representative, as well as corporate employees could be considered in the technical sector.

AG Chanos stated that would be in the discretion of the Governor.

AG Chanos confirmed the Board had reached consensus regarding nine gubernatorial discretionary appointments: a technology representative (economic sector representative), another local law enforcement agency, and three federal government appointees (allowing for representation from FBI, ICE and USSS). The total Board would thereby be increased to thirteen members. Quorum would be seven present members.

Mr. Earl suggested “in the event it is impracticable for the member to attend” be added to NRS 205A.050, item 2.

Board had no objections.

Mr. Earl suggested adding “support and oversee the activities of” to expand the role of the Board beyond simply “creating” the task forces in NRS 205A.060, item 2. Mr. Earl recommended that the words “for Northern Nevada” and “for

Southern Nevada” be deleted since the questionnaire sent to all law enforcement agencies indicated that both task forces received and processed evidence from sources throughout the State. The Reno group, for example was not just “for Northern Nevada.” This geographical distinction would become even less meaningful in the future as task force work was assigned in order of make best use of available personnel.

Mr. Earl then addressed paragraph 2(a) of NRS 205A.060. Prosecutors have never been involved in the task force activities. This was dealt within the Mission review. The task forces have evolved into bodies with an investigative mission. Only forensic examiners and investigators have been involved.

Turning to paragraph 2(b), Mr. Earl stated that this section was implicated by some of AG Chanos’s earlier remarks; private sector personnel have not participated in the task forces. That is what this section is about. “Because the task forces investigate crimes, it is inappropriate to include private sector individuals in the process. All of the text of the paragraph 2(b) can be struck without affecting the abilities of the Board to get private sector advice either through its membership or as invited speakers. The question is whether text should be retained that would put private sector individuals into task force criminal investigations.”

AG Chanos, returning to the beginning of the section 2 of NRS 205A.060, asked if SAC Martinez was comfortable with the word “oversee” in describing the Board’s Mission with respect to the task forces in light of his earlier expressed concerns.

SAC Martinez stated the word “oversee” does seem to imply some operational control over the task forces. “Presently, the agencies pretty much tend to make their own operational decisions.” The agencies “collaborate;” perhaps there is a more descriptive word than “oversees.”

RAC Colledge suggested the word “coordinate” instead of “oversee,” as better reflecting the original intent and the philosophy of the Board. “The Board would act as the honest broker in investigations.”

Mr. Earl stated that he took the word “oversee” from the existing Cooperative Agreement signed by the Southern Task Force members. However, he is comfortable without the word “oversee.”

SAC Martinez said he did not want to preclude the Board from performing a coordination function. “Adding the word ‘coordination’ would be fine.”

AG Chanos suggested “Establish, support and assist in the coordination...” be used.

The Board concurred with this resolution of the text.

Mr. Earl had suggested “and investigate” be added to NRS 205A.060, item 4.

Board had no objections.

Turning to NRS 205A.060, item 4, AG Chanos expressed concern with the proposed deletion of the text “Administer with the assistance of members of private industry, a program to secure governmental information systems against illegal intrusions and other criminal activities” to “Administer the equitable distribution of forfeiture funds in accordance with NRS XXX.XXX.” AG Chanos stated “there was an original desire by the State to have this Board pay some attention to the safeguarding of the State systems, even if it only makes suggestions. This seems to be a fundamental reason for the Board to not delete this language, which would strike at the core of why the Board was probably created.’ He expressed concern to replace this language with text relating to forfeiture funds.

Mr. Earl stated the Attorney General Chanos had correctly read the change he had proposed. Mr. Earl expressed regret Board member Terry Savage, Director, Department of Information Technology was unable to attend and had not sent a proxy. Mr. Earl explained the reason for the deletion was the Board statute was passed in 1999 before the legislature placed increasing responsibility on the Department of Information Technology to safeguard governmental information systems. His impression is that the Legislature looks to DOIT rather than the Advisory Board to fulfill this function.

AG Chanos stated that was a very meaningful explanation. “It would not be necessary for safeguarding to remain part of the Board’s Mission if it is being picked up someone else.”

Senator Weiner said she did not recall the original testimony on this point. DOIT should be at the table on this issue. “However, it may not be an ‘all or nothing’ situation. Perhaps the Board could work with DOIT in a shared capacity.”

AG Chanos suggested item 4 be changed to “assist the Department of Information Technology in their effort to secure governmental information systems against illegal intrusion and other criminal activities.” He noted that complete deletion of this mission would be a red flag to the legislators who would not see that text of the proceeding section as an adequate substitute.

The Board reached consensus on the language proposed by AG Chanos, and as a consequence, added a new provision with the appropriate renumbering, “Administer the equitable distribution of forfeiture funds in the accordance with NRS XXX.XXX.”

Board reached consensus.

Mr. Earl suggested NRS 205A.080, item 1 change from “unanimous approval” to “two-thirds approval.”

AG Chanos supported this change in light of the Board’s recent experience where a deadlock might have emerged had one of the Executive Director candidates not withdrawn.

Board had no objections this change.

Mr. Earl asked, based upon the Board’s previous discussion of staff, how the Board would like to handle the proposed changes to NRS 205A.080, in light of the discussion regarding relocating the person currently Executive Director within the Attorney General’s Office. The proposed change had read “shall appoint a full-time secretary, who is in the unclassified service...” to “employ investigators, forensics examiners and other personnel necessary to carry out the provisions of this chapter.” Mr. Earl stated “If the Executive Director is a Senior Deputy Attorney General and also manages Board personnel, then his authority over staff hired by the Board needs to be clear.”

AG Chanos suggested NRS 205A.080 remain mostly the same with the following changes: “Upon two-thirds approval...” from “Upon unanimous approval...” and “shall appoint a full-time secretary who is in the unclassified service...” to “shall appoint an administrative assistant who is in the unclassified service...and reports to the Executive Director.” “This would be consistent with a Senior DAG who also serves as the Board’s Ex-Officio, unpaid Executive Director and a single Board employee who reports to the Executive Director.”

Mr. Earl returned to the budget proposal, pointing out that it contained a recommendation that the position of secretary be reclassified to Administrative Services Officer, a recognized position in the classified service. He acknowledged that hiring someone in the classified service might present another set of issue for the Board. AG Chanos suggested retaining the secretary/administrative assistant position in the unclassified service.

The Board’s consensus was to move forward with the text as suggested by the Attorney General.

Mr. Earl suggested NRS 205A.100, item 1 change from “...accept gifts, grants, appropriations and donations...” to “accept gifts, grants, appropriations, donations and forfeitures...” “This is in line with the draft forfeiture statute approved in concept at an earlier Board meeting.”

RAC Colledge suggested “shared forfeitures and assets” be added to NRS 205A.100, item 1 to read “...accept gifts, grants, appropriations, donations, and

shared assets and forfeitures...” “This would clearly enable the Board to accept any shared assets that might come to it through federal forfeiture programs, where task force members participated in support of a federal prosecution.”

Board had no objections.

Board Action:

Senator Wiener proposed the Board change its name to Technological Crime Advisory Board and approve the proposed statute changes as discussed.

Commander Means seconded.

Board unanimously approve, noting it would like to confirm the changes at its next meeting.

9. Update on liaison activities.

Ms. Adams stated has not had much time to work with the agencies due to her training schedule and participation on a National Institute of Justice grant panel. She had a recent conversation with Dick Clark, Nevada POST. Mr. Clark has agreed to add electronic evidence handling and collection to the existing curriculum. Ms. Adams will supply a detailed list of potential items of interest and a few scenarios for instructors to use in their courses. POST will be expanding its curriculum to include a portal into Vermont’s POST for web-based training, as well Texas’ POST.

10. Discussion, recommendations, and action regarding data compromise at the Department of Veterans Affairs

Mr. Earl stated he has been very concerned about the data compromise. He has been in contact with a number of veteran organizations. Following the public press reports and proposed legislation, Mr. Earl felt it appropriate to draft a letter for the Board to consider sending to the Nevada Congressional Delegation. The letter suggests that the burden not be placed on active duty personnel and veterans, but on the federal government to adopt some addition techniques that go beyond fraud alerts and credit freezes. Mr. Earl originally drafted this letter before the laptop and external drive were recovered. He has updated the letter to reflect this change. “The real question for the Board is whether to suggest to the Nevada Congressional Delegation that steps be considered beyond those proposed by the Department of Veterans Affairs.”

SAC Martinez stated due to his position he probably must abstain because the letter implies expenditures of appropriated funds. “There are some good points in the letter. However, this is a sensitive matter, particularly as it involves another federal agency.”

Ms. Adams stated she met with both the Northern and Southern groups last week to discuss this letter. Both groups recommend the tone of the letter be changed and submitted to the State Legislature. “This is an example of what law enforcement agencies face on a daily basis; increased funding and continued

support for the task force is essential. This letter should be sent to the State legislature, not the Congressional leadership.”

AG Chanos inquired what the State Legislators would be asked to do what.

Ms. Adams explained that this data compromise could be used as example to demonstrate the urgency of the concern of ID theft.

AG Chanos acknowledged SAC Martinez’s comments, which might be generally applicable to federal agencies. Since he is unencumbered by these limitations, AG Chanos suggested he send the letter in his capacity as Attorney General

AG Chanos is not completely satisfied with the letter in that there is no specific call to action. He will have Mr. Earl redraft the letter, placed on the Attorney General letterhead and then decide if he wants to send it.

SAC Martinez stated that by having the letter come from the Attorney General it eases his concern considerably even if the letter states it comes from the Board’s recommendations. “That places the Board one step away; otherwise the letter would be a tantamount to my trying to influence the federal budget. I am absolutely precluded from doing that.”

AG Chanos stated he could sign the letter as Nevada Attorney General or Chairman of the Board or both. He does not want to create a situation where the federal agencies are uncomfortable, but a Board reference would explain his interest in the subject matter.

SSA Masto stated if US Secret Service were on the Board, it would not be uncomfortable with AG Chanos signing the letter as Chairman of the Board.

Ms. Adams suggested contacting the National Association of Attorneys General or the Western Association of Attorneys General and find out what other Attorneys General are doing, have done or are going to do. “This would provide more influence for this type of letter.”

AG Chanos concurred with Ms. Adams. He may pursue that option of submitting the letter through NAAG to see if it is interested in circulating the letter as a “sign-on” to have it sent beyond Nevada’s Congressional Delegation. He will explore those possibilities and report back to the Board, “but we will not be sending it as a Board.”

11. Board Comments.

SSA Masto thanked the Board for allow him to speak. He will work with Mr. Gardner about Mr. Earl visiting and speaking to the group of Secret Service Officers. The Secret Service has partnered with private industry, such as Cisco,

and academic representatives because they have resources that US Secret Service does not. By doing so, the Secret Service has strengthened its whole operation. Secret Service has deputized local and State officials that work with it. Senator Wiener and SSA Masto were discussing how to finance the operation. In SSA Masto's opinion, the State's forensic services will be able to become self-financing. This is based on his experience with Secret Service. US Secret Service will be happy to testify in front of the legislature to demonstrate the importance of an asset forfeiture program.

The forensic software, EnCase, is used by most law enforcement. It is expensive and a new version is released each year. SSA Masto stated that the worst scenario that could happen is for a computer forensic examiner to be grilled on the witness stand by the defense attorney about which version of EnCase software he is trained on. By using forfeiture funds, Secret Service is able to keep personnel training up-to-date.

SSA Masto discussed the recent Nevada DMV case as an egregious instance of identity theft. It took about 120 days to recover the equipment from the thieves. The Southwest ID theft and Fraud Task Force (SWIFT), which concentrates on ID theft and methamphetamine users, was "key" to the equipment recovery. They focused their investigation on the end user of the equipment. "We raised the temperature sufficiently, so that the equipment was left on the rooftop of a construction site. This is classic example of how the Secret Service works with local agencies to bring a quick resolution to a very serious problem."

SSA Masto stated new legislation and asset forfeiture are very important. Senator Wiener has already been a leader in passing legislation. More needs to be done. "We are never going to get the point where, like last year, the DEA gave Las Vegas Metropolitan Police \$12.5 million because of its involvement in task forces, such as HIDTA. The Secret Service Las Vegas Electronic Crime Task Force is number one in asset forfeiture, beating out our offices in New York, Miami, Detroit, LA, Chicago and Atlanta. All of those assets have been shared with our partners to support training and operations."

SSA Masto would like to see a stand-alone operation, run by the Attorney General's Office, where all the law enforcement agencies work together sharing assets, resources and information. The Attorney General's Office would act as the honest broker to facilitate cooperation among federal agencies. All of the forensic examiners would be sworn law enforcement officers. This helps to eliminate the potential of evidence being over looked by someone who is not familiar with investigating crime.

The Secret Service has a very simple three-paged Memorandum of Agreement and requires a bank account set-up to receive asset forfeiture funds via direct deposit. The Secret Service will be placing an ECSAP agent (Electronic Crimes Special Agent Program) in Reno. SSA Masto thanked RAC College and SA

McDonald and her police partners for all of their work in providing forensics services. "Secret Service is trying to be more proactive rather than waiting for something to happen, as was the case for much of the last 25 years." The DEFCON convention, a hackers' convention, will be in Las Vegas soon. A 24-hour command post will be set-up. The Secret Service will be educating local businesses about the convention and what can happen, as well as providing a phone number for a rapid response.

SSA Masto again invited everyone to visit their lab.

Attorney General Chanos thanked all of the federal agencies for participating on the Board and assisting law enforcement throughout the State and safeguarding Nevada. It is encouraging and gratifying that the federal agencies have the confidence in the Attorney General's Office to act as a partner in this effort.

12. Public Comments.

No public comment.

13. Scheduling of future meetings.

Mr. Earl will circulate dates for an October 2006 meeting in order to enable a meeting before the end of the year, if the Board deems it necessary

Approved with corrections by the Board at its subsequent meeting on October 11, 2006.

Notice of Public Meeting

Advisory Board for Nevada Task Force for Technological Crime
October 11, 2006

10:00 am

*Room 2134 of the Legislative Building
401 South Carson Street, Carson City, Nevada*

*Via Videoconferencing
Room 4412, Grant Sawyer State Building
555 East Washington Ave., Las Vegas, Nevada*

AGENDA

1. Call to Order.*
[AG Chanos]
 - a. Verification of quorum
2. Discussion and approval of minutes from July 10, 2006 Advisory Board Meeting.*
[AG Chanos]
3. Report, discussion, recommendations and actions regarding Northern Task Force activities.*
[Concerned Agencies]
4. Report, discussion, recommendations and actions regarding Southern Task Force activities.*
[Concerned Agencies]
5. Customer Identification and Information Security in an Internet Banking Environment: a presentation by Joe Palmarozzo, Vice President, Web Site Administrator, Nevada State Bank.*
[Mr. Uffelman and Mr. Palmarozzo]
6. Update on the implementation of the student Internet safety program in the Clark County School District by Ms. Dixie Stephens, Clark County School District.*
[Mr. Pickrell and Ms. Stephens]
7. Overview of Department of Information Technology mission to secure governmental information systems of the State of Nevada.*
[Mr. Savage and Mr. Elste]
8. Report, discussion, recommendations and actions regarding budget submission and legislative proposals.*
[Mr. Earl]

9. Report on action regarding data compromise at the Department of Veterans Affairs.*

[Mr. Earl]

10. Board Comments.

11. Public Comments.

12. Scheduling of future meetings.*

* Denotes a possible action item. The order of the agenda items is subject to change.

This agenda has been sent to all members of the Advisory Board and other interested persons who have requested an agenda.

Unless otherwise stated, items may be taken out of order presented on the agenda at the discretion of the Chair. The meeting may be recorded. Some Board members may attend the meeting via telephone conference. The Chair may limit public comments.

Members of the public who are disabled and require special accommodations or assistance at the meeting are requested to notify James D. Earl at (775) 688-1869 twenty-four hours prior to the meeting.

THIS MEETING HAS BEEN PROPERLY NOTICED AND POSTED AT THE FOLLOWING LOCATIONS:

Office of the Attorney General
5420 Kietzke Lane, Suite 202
Reno, Nevada 89511

Office of the Attorney General
555 East Washington Avenue
Las Vegas, Nevada 89101

Office of the Attorney General
100 North Carson Street
Carson City, Nevada

Reno City Hall
1 East First Street
Reno, Nevada

Minutes of the Advisory Board for the Nevada Task Force for Technological Crime

October 11, 2006

The Advisory Board for the Nevada Task Force for Technological Crime was called to order at 10:07 a.m. on Wednesday, October 11, 2006. Resident Agent in Charge John W. Colledge III, Vice Chairman, presided in Room 2134 of the Legislative Building, Carson City, Nevada and via videoconference in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Resident Agent in Charge John W. Colledge III, Vice Chairman
Mr. Patrick A. Ferguson, proxy for Attorney General George Chanos
Special Agent in Charge Steve Martinez
Commander Don L. Means
Mr. Tom Pickrell
Mr. Terry Savage
Mr. William Uffelman

ADVISORY BOARD MEMBERS ABSENT:

Attorney General George Chanos, Chairman
Assemblyman Bernie Anderson
Senator Valerie Wiener

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director

OTHERS PRESENT:

James R. Elste, Department of Information Technology
Nicole Moon, Office of the Attorney General
Jim Lemaire, Department of Public Safety
Dave Atkinson, Washoe County Sheriff's Department
Joe Palmarozzo, Nevada State Bank
Dixie Stephens, Clark County School District
Leonard Marshall, Las Vegas Metropolitan Police Department
Brian Evans, Las Vegas Metropolitan Police Department
Paul Mastro, United States Secret Service

Agenda Item 1 – Verification of quorum

A roll call verified the presence of a quorum.

Agenda Item 2 – Discussion and approval of minutes from July 10, 2006 Advisory Board Meeting

RAC COLLEDGE:

Has everyone had an opportunity to review the minutes?

MR. EARL:

Are there any additions or corrections to the minutes?

SAC MARTINEZ:

I have a minor correction on page 2. I made reference to the Mytob and Zotob worm investigations. The spellings are "Mytob" and "Zotob."

A motion to approve the minutes as corrected was made, seconded, and approved.

Agenda Item 3 – Report, discussion, and recommendations regarding Northern Task Force Activities.

RAC COLLEDGE:

Due to several different cases, participation from other agencies has not been as great as we would have liked. Hopefully that will change in the new year. The Immigration and Customs Enforcement (ICE) computer forensic examiner, Senior Special Agent Melissa McDonald, conducted 11 examinations in the last 90 days for various agencies including ICE, the Department of Public Safety (DPS), Washoe County Sheriff's Department, Reno Police Department, and Storey County, among others.

We have had the task force office space repainted. Special Agent McDonald has done a very good job organizing the operation. It has been rather strenuous. We only have one person full time dealing with computer forensics in the northern part of the state. Hopefully we will be able to rectify that in the future and spread the workload.

There have been reassignments in some of the northern agencies. That has caused some difficulties. However, Storey County now has a deputy sheriff who has a background in computer science. He is beginning to participate in task force activities. He is taking the initial steps to learn computer forensics. Hopefully we will be able to get him to some formal training in the coming year.

Agenda Item 4 – Report discussion, recommendations and actions regarding Southern Task Force activities.

MR. EARL:

Yesterday, I spoke briefly with Sergeant Leonard Marshall of the Las Vegas Metropolitan Police Department (LVMPD). He replaces Sergeant Karen Francis on the Internet Crimes Against Children (ICAC) team in the Las Vegas. There is also a new supervising lieutenant, Lieutenant Brian Evans, LVMPD. He deals with the special victims section.

SERGEANT MARSHALL:

Lieutenant Evans has not yet arrived.

I would like to summarize a case we opened in May, 2006. Two children disclosed that they were being molested by a live-in family friend. Subsequent investigation revealed not only the molestation of these two children, but the subject was also taking sexually explicit pictures of them. The pictures were archived to computers. We executed several search warrants. We discovered large amounts of digital evidence. I understand from the detectives that this is the

largest collection of evidence they have ever found. There must be several hundred thousand, if not a million, photos of child pornography. The subject is currently incarcerated for the sexual abuse of two minors. We are still in the process of forensically examining the digital evidence.

I started this detail about a month ago. I have a lot to learn, but look forward to working with all involved in the task forces.

RAC COLLEDGE:

Are there other reports from the southern task force?

SAC MARTINEZ:

I would like to give an indication of the work of the FBI during the last several months. We initiated a case involving the unauthorized switch of DNS numbers of a significant commercial web site maintained in Las Vegas. This web site was hijacked and placed on another server. This was completely unauthorized, and was a denial of service type of attack. We have been working this case aggressively. We have good leads. We have some subjects within the United States. This makes it much easier for us to reach them. We remain in the information gathering stage, but I wanted to provide an example of the type of work currently underway.

In the past two months, Steve Schmidt, the FBI section chief of Special Technologies and Applications, and David Thomas, Deputy Assistant Director of the FBI Cyber Division, have visited the task force. Both talked to task force members and interacted with representatives of the monitoring facility of the Department of Defense (IARC). We are in discussions about how we might leverage some of the information obtained by the IARC to look at potential national security threats to the systems monitored by the IARC.

There is quite a bit of activity in these areas, and I wanted to give Board Members some indication of the FBI's ongoing activities.

MR. EARL:

I would like to highlight one issue Mr. Martinez addressed. Hijacking a web site represents a threat not only to commercial web sites, but also to State web sites. It is a matter of concern to banks. Several presenters this morning are likely to address topics related to the investigation reported by Mr. Martinez.

Agenda Item 5 – Customer Identification and Information Security in an Internet Banking Environment

RAC COLLEDGE:

We have with us this morning Mr. Joe Palmarozzo, Vice President and Web Site Administrator at Nevada State Bank.

MR. EARL:

Board Members may recall expressing a concern about banking security at our February meeting. Mr. Uffelman distributed some general information thereafter.

Mr. Palmarozzo will provide his bank's perspective on information security, and, importantly, the tradeoffs that have to be made by commercial organizations to comply with laws and regulations while also ensuring customer acceptance.

MR. PALMAROZZO:

I am very pleased to address you this morning. I am going to provide a high level overview of the challenges facing financial institutions with regard to customer authentication and security regarding Internet banking, the relevant federal guidelines, and the decision process at Nevada State Bank to comply proactively with recent federal guidance.

As the Internet grows as a channel for banking and commerce, threats to technology-based transactions have grown considerably. Details of phishing, pharmings, spy ware and the associated identity theft and fraud have been widely reported in the media. One needs only to open the newspaper or watch the news to see such stories.

Federal Guidance on Authentication of Customers in an Internet Banking Environment

- The Federal Financial Institutions Examination Council (FFIEC) prescribes uniform principles, standards and report forms for the federal examination of financial institutions by the Federal Reserve, FDIC, NCUA, OCC, and OTS.
- On Oct. 12, 2005, the FFIEC issued updated guidance for authentication of customers in an Internet banking environment.
 - This updates the guidance they issued on Aug. 8, 2001.
- Additional FAQs on the Oct. 12th guidance were released on Aug. 15, 2006.

Our customers are rightfully concerned. These threats are very real. Federal regulatory agencies have taken steps to guide financial institutions to address these threats. One such agency is the Federal Financial Institutions Examination Council (FFIEC). The FFIEC is a federal interagency body that prescribes uniform principles, standards, and report forms for the federal examination of financial institutions by the Federal Reserve Board, FDIC, NCUA, OCC and OTS.

On October 12th of last year, the FFIEC issued updated guidance for financial institutions on

authentication of customers in an Internet banking environment. This updated guidance issued on August, 8. 2001. Most recently, the FFIEC has released additional FAQs.

FFIEC Guidance Summarized

Financial institutions are directed to:

- Ensure that their Information Security Program:
 - Identifies and assess the associated risks with Internet Banking products and services
 - Identifies risk mitigation actions, including appropriate authentication strength
 - Measures and evaluates customer awareness efforts
- Adjust, as appropriate, their information security program in light of changes in:
 - technology
 - sensitivity of it @ customer information
 - internal/external threats to information
- Implement appropriate risk mitigation strategies

I would like to summarize this guidance. Financial institutions are directed to ensure that their information security program identifies and assesses the associated risks with Internet banking products and services, to conduct internal evaluations in order to identify risk mitigation actions including appropriate authentication strength, and to measure and evaluate customer awareness efforts. Additionally, banks must adjust their information security program in light of changes in technology, the sensitivity of the customer information being accessed, and internal and external threats to that information. Finally,

banks must implement appropriate risk mitigation strategies.

Regarding authentication of customers, the guidance applies to both retail and commercial customers.

FFIEC Stance on Authentication of Customers

- The guidance applies to authentication of retail and commercial customers.
- ~~N~~The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.~~O~~
- ~~N~~Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to meet those risks.~~O~~
- Note, no single authentication solution is endorsed.
- Conformance is required by year-end 2006.

The FFIEC agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

Single-factor authentication is the predominant method used currently by most financial institutions. That is changing.

Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor

authentication, layered security, or other controls reasonably calculated to meet those risks.

It is important to note that the FFIEC endorses no single authentication method as a cure-all. This leaves financial institutions some latitude to conduct their own evaluations on the security of their Internet banking applications and to determine the best solution to mitigate those risks.

Banks must conform to these guidelines by the end of this year.

Multi Factor Authentication Defined

Multi factor authentication is a process that uses at least two of the following factors to authenticate clients for access to a given service:

- ☐ Something the client knows (a shared secret)
 - ☐ For example, a password or pin
- ☐ Something the client has (a physical device)
 - ☐ For example, a card or token
- ☐ Something the client is (biometrics)
 - ☐ For example, retinal, finger print or facial scanning

I would like to take a moment to define multi-factor authentication, one of the solutions mentioned in the guidance. Multi-factor authentication is a process that uses at least two of the factors to authenticate clients for access to a given service: something the client knows (a shared secret like a password or PIN), something the client has (a physical device like a card or token), or something the client is (a biometric measure like a retinal, fingerprint, or facial scan).

A good example of two-factor authentication already in use by financial institutions is the procedure involving ATM cards. Customers use something they have (a physical card) as well as something they know (their PIN) in order to withdraw money from an ATM machine.

NSB Evaluation of Authentication Enhancement Solutions

- ☐ At the Bancorp level risk assessments were completed for our Internet Banking applications.
- ☐ Evaluations of authentication enhancement solutions were conducted based on:
 - ☐ The level of security offered relative to the risk of the application
 - ☐ Costs
 - ☐ Ease of use for customers
 - ☐ Portability
 - ☐ Cross-channel Utility
 - ☐ Vendor Financial Strength
 - ☐ Industry Reference

Given the FFIEC guidance, Nevada State Bank, at the corporate level, completed risk assessments for all of our Internet banking applications. We then began to evaluate authentication enhancement solutions for those services. We based these evaluations on the level of security offered by a given solution relative to risk of the application, and the costs involved with that solution (acquisition, licensing, maintenance, integration, infrastructure, and customer rollout costs).

We included the ease of use for customers. Although the Internet is an ever-changing environment, our customers do not like change. They are used to a certain way of logging in. We wanted to make change as easy as possible for them.

We were concerned about the portability of the solution. This goes to the ability to authenticate from different computers, operating systems, and platforms, as well as the ability of customers to login from multiple computers at work, home, or a public kiosk.

Authentication Enhancement Solutions Evaluated

- ☐ Static Password
- ☐ One-Time Password Token
- ☐ Grid Based One Time Password
- ☐ PKI (Public Key Infrastructure) § Software Based
- ☐ PKI (Public Key Infrastructure) § Token Based
- ☐ User/Device Site Authentication Systems
- ☐ Out of Band Authentication

We also considered cross-channel utility, by which I mean the ability to use a solution not only on the Internet but through our voice response unit (VRU) and our call center.

We considered the financial strength and longevity of a potential vendor. Finally we considered industry references; we looked at research reports on different solutions and the level of adoption both in the United States and Europe.

I would like to list some of the authentication enhancement solutions that Nevada State Bank evaluated. We looked at strengthening our static

password by requiring it to be changed more often or to be made longer. We looked at one-time password tokens; these involve a user name and password combined with a one-time password generated by a small form factor hardware token. This token would generate a random value that would remain valid for 60 seconds. The customer would have to enter this value as well as part of the log-in procedure.

We considered grid based one-time passwords. These are typically available on cards given to customers, and they would be used in conjunction with a username and password.

We considered public key infrastructure solutions – both software and token based. These make use of usernames and passwords and a digital certificate. This procedure would allow mutual authentication between the customer and the bank's servers.

We looked at user device site authentication systems. I will return to these in a moment.

Lastly, we considered out of band authentication. This involves the use of a username, password, and then a one-time token password would be delivered to the customer via an automated voice-based phone call.

Nevada State Bank® SecurEntry™

- Adaptive Authentication solution by RSA Security was selected.
- Solution features:
 - § Two factor authentication based on something the customer has (their computer) and something they know (password)
 - § Authenticates NSB® site to the customer with a customized image and phrase they chose before they enter their password
 - § Logging in from an unregistered computer prompts the customer to answer one of three customer selected challenge questions before entering their password and registering the computer for future logins
 - § No limit to the number of computers a customer can register
 - § Minimal change to the current login procedure
 - § No change in customer's existing User Name and Password
 - § Adequately mitigates authentication system threats

The solution that Nevada State Bank (NSB) decided to implement is an adaptive authentication solution provided by the company RSA Security. Their solution falls into the category of user/device site authentication.

The implemented solution features two factor authentication based on something the customer has (their computer in this case) and something they know (their existing password and username). When a customer registers a computer, a device ID is established utilizing secure cookies and flash-shared objects. Additionally, a device profile is

created based on device and network forensics. This creates a "fingerprint" of sorts that identifies the customer computer. The solution authenticates NSB's site to the customer with a customized image and phrase, which the customer has chosen during the computer enrollment process. They see this image and phrase prior to entering a password. This allows them to know they are at the valid NSB web site.

If a customer logs in from an unregistered computer, he is prompted to answer one of three randomly chosen questions from among those the customer chose at enrollment. Once the question has been answered correctly, the customer can then enter the password and log in. The customer then has the opportunity to register the new computer. Once a computer is registered, the customer is not prompted with the challenge question in the future when logging in from the new computer.

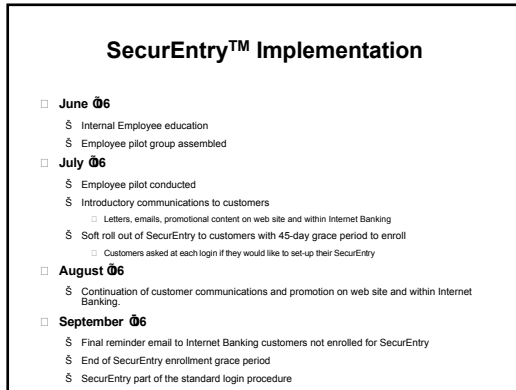
There is no limitation to the number of computers that can be used or registered by a customer. There is only minimal change to the current login procedure. There is no additional cost to the customer. There is no change to the customer's existing username and password.

This procedure adequately mitigates threats against the authentication system, specifically, the prevalent threats of phishing, pharming, credential guessing and those associated with spy ware.

The SecureEntry™ implementation at NSB took place over a four-month period beginning in June of 2006. I will give a quick overview of the implementation. In June, internal employee education took place regarding our solution. An employee pilot group was assembled to test our solution. In

July, the employee pilot program was conducted, and minor changes were made prior to rolling the solution out to customers.

We sent out introductory communications to banking customers, comprised of letters, emails, and promotional web content (including web demos).



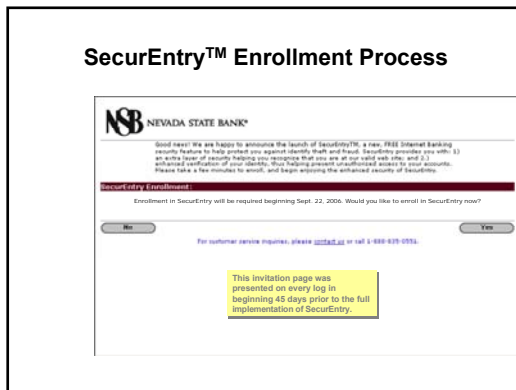
RSA stressed to us that customer communications was key. We took this best practices advice and tried to communicate with our customers through multiple channels.

In August, we had a soft rollout of SecureEntry™ to our customers with a 45-day enrollment grace period. In other words, enrollment was optional for 45 days. Customers were prompted each time they logged in if they would like to set up SecureEntry™ functionality.

In the first week of September, we sent out a final reminder email to existing Internet banking

customers who had not yet enrolled in SecureEntry™. We informed them of the impending deadline of September 22nd. On September 22nd, the enrollment grace period ended. SecureEntry™ then became part of our standard login procedure.

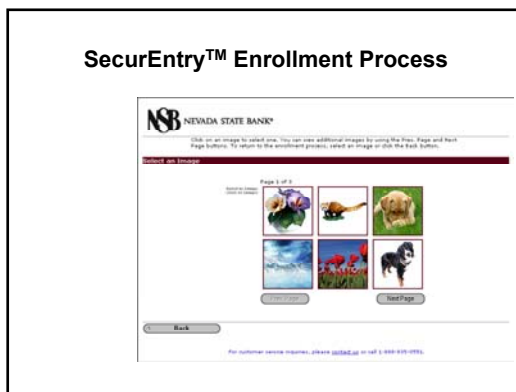
I would like to review briefly what our customers saw when enrolling for SecureEntry™.



This screen shows what a customer saw when the grace period began. This is the invitation page for enrollment. It briefly describes the program and identifies the deadline of September 22nd. It allows them either to enroll or to bypass enrollment.

If a customer decided to enroll, he was taken to a page where he would select a secure entry phrase. Customers were also presented with a default image. That image could be changed. The phrase and image selected by the customer would later be seen on the password login page. Seeing the phrase and image would, in the future, authenticate

the NSB page to the customer. They would then know, in other words, that they were on the genuine NSB web site.



If a customer wanted to change an image, he would be taken to another page where he could select one of six additional randomly chosen images. These images reside in a data base containing thousands of images. The customer is offered three pages of images from which to make a selection.

Once an image is selected, the customer is returned to the image and phrase selection page. The customer would see the image selected and would enter the phrase previously selected.

A customer would then be taken to the "challenge

question” page where a selection would be made from among three challenge questions. These questions are used in later identification when logging in from an unregistered computer.

Finally, a customer would receive a page confirming all of his selections. There is an opportunity for further editing prior to final submission.

Upon submission, the customer would see a message that enrollment has been successful. They would then automatically be redirected to the Internet banking login page.

After a customer's first login using SecureEntry™, the customer will notice that the login area has changed. No longer would a customer be prompted

to enter his password in the NSB home page. They would only enter their user name. After entering a user name, the customer would be prompted to enter a password in a separate page.

NSB's business Internet banking customers would see the same change.

When initially logging into SecureEntry™ or when logging in from an unregistered computer, a customer will receive a challenge question page. The customer will be prompted to answer one of the three challenge questions selected during registration process. The question displayed on the web page is chosen at random. Upon answering the question correctly, the customer is offered the option to register the computer. If the computer is registered, a device ID is created for that particular computer. Once a computer is registered, the user will no longer receive challenge questions when that computer is used in the future.

After successfully answering the challenge question, or when logging in from a previously registered computer, a customer is presented with the site validation and password page. The customer would see his secure image and phrase in order to validate that he is on the genuine NSB web site. The customer would then receive a password prompt to continue the login process.

In conclusion, I would like to emphasize there are no silver bullets at this time that will address all online threats. There is no single solution that will eliminate all security threats. Our collective vigilance to address new, more sophisticated threats will need to continue as online technology and commerce continue to advance. Customers will continue to look to us for protection from, and education about, online threats. Since they are in a position of public trust, financial institutions have a greater responsibility to maintain that trust.

I appreciate the opportunity to speak with you today, and I will be glad to address any questions.

MR. UFFELMAN:

I have one comment in light of Mr. Martinez's report on the hijacking of a commercial web site here in Nevada. Presumably, visitors to that web site were unaware that it had been hijacked. The system of authentication put in place by NSB on its web site is designed to prevent movement of its site to a faked location. I presume that the NSB site could not be moved, or that if there were an attempt to move the site, it would have only limited effect. So, for example, if my wife had picked the cute puppy as her authentication picture, she might see flowers or something else. Is that correct?

MR. PALMAROZZO:

That is correct. A fake web site would not be able to duplicate the customized image and phrase the customer had selected. The fake site might be able to copy NSB's static web page to give the customer the appearance of our site, but it would not be able to generate the correct image and phrase.

SAC MARTINEZ:

It may be too early for you to know, but did you experience any significant loss of customer base or diminution of Internet banking use among your customer base upon rollout?

MR. PALMAROZZO:

No. We experienced a very high adoption rate. The deadline for enrollment was September 22nd; right now we are sitting at 94% of our active Internet banking customers enrolled in SecureEntry™. Clearly not everyone will like the solution their bank chooses, but our program has been very well received.

SAC MARTINEZ:

Does NSB post any recommendations regarding security configurations on personal computers as part of its program? I know you probably cannot endorse particular commercial products, but do you provide customers with any guidance as to how they might configure their computer to ensure they will be safer.

MR. PALMAROZZO:

We do not recommend particular configurations, but we do have a page on our site that addresses Internet security. We tell customers where they can go to get needed software but without endorsing a particular software application.

MR. FERGUSON:

Does NSB have a way for its customers to "unregister" a computer? So, for example, if they get rid of a computer, or change jobs, or change computers, can they unregister the computer they previously used?

MR. PALMAROZZO:

Yes. Within our personal and business Internet banking services Internet site, there is a "services" tab that contains a maintenance link. That link allows a user to unregister a computer that has been previously registered within the SecureEntry™ system. It allows a user to change an image, a phrase, the challenge questions and answers.

MR. FERGUSON:

Is there an expiration period for a registration? In other words, once a computer is registered, will it remain registered indefinitely, or will that registration lapse after, say, 90 days without a login accomplished from that computer?

MR. PALMAROZZO:

At this time, there is no automatic expiration period.

MR. EARL:

I know you are speaking as the web site administrator for Nevada State Bank; however, do you have any idea as to the speed similar security solutions are being adopted? The reason I ask is that several weeks ago, one of my home pages, Yahoo!, offered me a similar option to authenticate its site, so that when I went there I could be assured it was not being spoofed. It was not as sophisticated a solution as the one you described. Do you have any sense as to the take up of this type of technology?

MR. PALMAROZZO:

I can only speak to financial institutions. As stated in the FFIEC guidance, financial institutions are expected to comply by the end of this year (2006). My understanding is that only very rare exceptions will be allowed. Many banks are moving quickly to implement solutions. Those solutions may not be similar to ours since the FFIEC guidance allows some latitude in implementation. I know some NSB competitors are in compliance with the FFIEC at this time.

MR. UFFELMAN:

The degree of risk in each Internet transaction is assessed by each bank, and each decides what to do. Some banks allow a customer to view his account balance, but will not allow transactions like funds transfers without additional levels of security. So, if a customer wants to do a quick balance check, single factor identification is sufficient. However, if a customer wants to change something – move money, switch funds from checking to savings accounts, make an online transfer to a third party – then some type of second tier authentication will be required. That option is afforded to each bank.

MR. PALMAROZZO:

That is correct. Ultimately, each bank has to answer to its regulators.

MR. EARL:

If there are no further questions, we would all like to thank you for your presentation. I would also like to express my appreciation to Mr. Uffelman for assisting in making the arrangements that brought you here this morning.

As you may know, the Nevada Legislature has shown increasing interest in activities in the commercial world that would limit unauthorized access to customer information across a wide variety of areas. I will certainly endeavor in the production of the meeting minutes to accurately reflect the endeavors of your bank and the industry as you have presented them here this morning.

Agenda Item 6 – Update on the implementation of the student Internet safety program in the Clark County School District

RAC COLLEDGE:

Let us move on to our next agenda item.

MR. EARL:

We would like to welcome back Ms. Dixie Stephens. Board members will recall that Ms. Stephens is in charge of implementing the student Internet safety program. When she last spoke to us, that program was in its early stages. The focus was on training the trainer. An effort was underway to train at least one teacher in every school who would then train other teachers on the program. We are now in a new school year, and we would like to ask Ms. Stephens to provide us with an update on that teacher training and on the roll out of the program.

MR. PICKRELL:

Before Ms. Stephens begins, I would like to ensure everyone is aware of the magnitude of the program. Clark County School District is the fifth largest school district in the United States. We

have pretty close to 20,000 instructors and teachers across the district. We have well in excess of 320 schools. I have heard questions asking why the program is not fully implemented. People have to understand this is a major effort, and the district does not have a lot of resources. Having said all that, let me introduce Ms. Dixie Stephens. She is from the curriculum professional center within Clark County School District.

Ms. STEPHENS:

Mr. Earl sent me some questions to address. If you have questions, please ask them at any time. Some of the questions addressed the training I mentioned last spring.

We were able to train approximately 100 teachers in the two months we had to implement the i-SAFE program. This is an on-line, train the trainers program. We showed the teachers how to access i-SAFE with the expectation that they could take what they learned back to their schools, pass on what they learned, and conduct their own training.

Classroom instruction on Internet safety is a part of every syllabus for computer-based learning in the schools. This includes middle school computer literacy programs and high school computer science programs. Each course includes Internet safety in the syllabus.

We took a quick survey – not a complete survey – prior to coming to this meeting. Of the teachers responding, 50% are actively teaching Internet safety. They were pretty honest. They use both on-line resources and other resources that they might have from text books or other sources. Not all are using i-SAFE. There are other good on-line resources available. Teachers pretty much pick and choose based on what fits best into their curriculum.

We asked teachers what was the student response to this instruction. The response was very positive; 73% felt that the students responded “well” or “excellently” to the materials. It is good to know that students are not nodding off or ignoring the concept of Internet safety.

Some of the teacher comments made in the survey were that students were unaware or did not understand all of the implications of MySpace or blogs or other Internet sites. The more information we can put out, the better.

We also implemented a parental outreach program. Quite honestly, we have not done this very well. This is one of the goals for this year. We only had about 8% report that they had put together some kind of package – an assembly or something on the school web site – to alert parents and share information with them. We need to set that part of the program up and try to reach parents more effectively so that they can be pro-active in order to protect their students at home.

I think the school district has done a very good job of protecting kids while they are at school. We have a wonderful filtering system. It is not perfect. As everyone knows, the web changes so quickly that we can not keep up with all the inappropriate sites. However, our system catches a large number of them.

We also have a procedure in place so that if I come across a site, or if a student tells me of an inappropriate site, I can quickly post that site so that it will be blocked almost instantaneously so it can not be accessed by other students.

I am a parent with two boys, aged 11 and 14. This topic is dear to my heart. Our weakness is for students at home. Parents are not as knowledgeable as their children regarding computer and Internet use. They simply are unaware of the best safety procedures.

Parental outreach needs to be stepped up. We need to address that in a better manner in the future.

Turning to on-line professional development programs, we were able to offer money to the 100 teachers who have been involved. This is always a nice incentive. We did a combination of face-to-face and on-line training. I was one of the instructors. We put together safety information for them and then I showed them the on-line training, which they could take at their leisure. Instead of having to be at a meeting, they could access the training from home in their spare time. Once that training was complete, they have access to materials that can be downloaded for classroom use. This is a very good curriculum for kindergarten through twelfth grade.

Our survey showed most teachers preferred face-to-face instruction. On-line content training is fairly new in the district. We are rolling that out again. I believe that as teachers attend more on-line meetings, they will become more comfortable with that format. We are going to keep working on this.

We have plans for more training this year. We did not start training until late last year. I only had several months to train our nine-month teachers who stop working in June. We will start training next month, offering at least one session a month depending on funding and interest.

The training is voluntary. We have to work around teaching schedules. This means training takes place after school or on weekends.

Last year I was able to attend a new teacher orientation and present Internet safety instruction. This was a good opportunity. I plan to take advantage of opportunities like this as they arise.

I am also working with the current technical education department on Internet safety. They work with teachers in the schools who teach computer classes. We will be working closely to ensure the information and training gets to those teachers.

Turning to lessons learned to date, we know we need to reach our parents. We need more training. Teacher comments indicated they did not know training was available. We need to better publicize what we are doing so that programs can be taken advantage of by more teachers. This month is cyber security month. I attended a conference in Maryland last week. I returned with activities for every day of the month. I will be posting those to our interact forum – our email system for the school district. Hopefully, teachers will pick those up for incorporation into their curriculum.

I will be glad to answer your questions.

MR. EARL:

While I am not very familiar with the i-SAFE program, I do know that one of the modules deals with the subject of cyber bullying. This topic has been widely addressed in the traditional and on-line press over the past several months. Do you include the cyber bullying module in instruction? Have you received feedback from teachers or parents regarding how the program has addressed this issue?

MS. STEPHENS

Both i-SAFE and NetSmartz, another popular program with great content, address cyber bullying. Unfortunately, I do not have any information on the impact of our program on cyber bullying or how it is being received.

However, cyber bullying is a huge issue, particularly at the middle school level. The problem seems to start in late elementary school. It dies out a little at the secondary school level, which is good to know. Apparently, as kids mature, they step back from this a little. We do need to address the problem in middle school by addressing middle school teachers.

SAC MARTINEZ:

Do you have metrics, or perhaps just some sense, of how often students will report incidents that have occurred while they were on line either at home or at school to school officials? What is done with that information?

MS. STEPHENS

Reports like this are made to the discipline committee. Typically, I do not have access to that information. If there is a need for that information, I am pretty sure we could ask for it. It would probably be available on an individual school basis as it is privileged information at that level.

SAC MARTINEZ:

If that information can be sanitized for your use, it might be helpful for you in deciding how best to target your outreach and training. It might provide good guidance regarding what the kids are actually experiencing.

MS. STEPHENS

That is a great idea. I will see what the process is to see if obtaining that information is possible.

MR. EARL:

This is not really a question, rather an issue appropriate to raise with Board members. This meeting is likely our last meeting before the Legislature convenes. I anticipate I will be asked to appear before various legislative committees. Perhaps others will be asked as well. I wonder if there is additional input from Board members regarding possible future Board activities or recommendations regarding student Internet safety in schools or otherwise. If there are suggestions, I will be glad to incorporate them in any presentation I make, or answers to questions that might be asked of me.

MR. PICKRELL:

Both Ms. Stephens and I believe that additional resources would certainly help the district. We simply need more resources to implement these programs. We would be glad to elaborate at a later date. Again, resources are always an issue.

RAC COLLEDGE:

We mentioned this at other meetings: is there interest among law enforcement agencies represented on the Board in identifying agency personnel who could act as liaisons or presenters to students, parents, teachers, or faculty? Could agencies participate in such an endeavor?

SAC MARTINEZ:

Actually, the group here in Las Vegas had a short off-line conversation about this before starting the Board meeting. Absolutely. This is part of my expectation regarding the duties of our cyber investigators. We have considerable material and training opportunities that can be made available. I have access to speakers on the national level as well. These people might come from the FBI cyber division. They might easily be convinced to come to Las Vegas. I am open to such possibilities. I think we need to have further conversations about types of assistance the FBI might provide.

MS. STEPHENS

One of the requests made by teachers was for additional information on what was happening in the community generally. They have already requested a partnership to expand their understanding beyond the schools. I look forward to working with you on this issue.

MR. EARL:

When we undertook our mission review in the spring, we sent a questionnaire to local law enforcement agencies in Nevada. We provided them with rather rudimentary training tools on CDs. One of the questions we asked was whether local police and sheriff's departments were interested in providing assistance to schools upon the invitation of the school. My recollection of

the results is that there was considerable interest by local law enforcement, but that they lacked materials. More importantly, they also had a resource problem in terms of officers sufficiently well to be able to respond to a school's invitation to make a presentation.

I am heartened by Mr. Martinez's remarks. My office is more that willing to facilitate any contacts by passing on school inquiries to the appropriate liaison people at the FBI or other organizations.

RAC COLLEDGE:

In the northern part of the state, Immigration and Customs Enforcement (ICE) can provide assistance to do similar outreach. I also suggest that the Board, perhaps through the Attorney General's Office reach out to the larger school districts in the northern part of the state, not only Washoe County, but Lyon County and Douglas County. These areas are growing rapidly.

MR. EARL:

I have one additional observation. The individuals who would provide briefings at the request of schools are law enforcement officers first and foremost. Their availability would be subject to their law enforcement activities.

The Board's budget request for upcoming fiscal years includes additional State personnel to serve as computer forensic examiners and investigators. Should the Legislature decide to fund these positions, we might consider interviewing applicants with school outreach in mind. They would have to follow up their forensic analysis with courtroom testimony. Someone who can explain things in court ought to be able to make a reasonable presentation to teachers, parents, and children. We should keep this possibility in mind as well.

Agenda Item 7 – Overview of the Department of Information Technology mission to secure governmental information systems of the State of Nevada

RAC COLLEDGE:

Let us move on to agenda item seven.

MR. EARL:

Board members may recall that at our July meeting, the Board decided to recommend several changes to our underlying statute. One of those changes would modify the Board's mission to include providing assistance to the Department of Information Technology (DoIT).

Senator Wiener, in particular, expressed interest in hearing more about the current mission of DoIT. This would be a first step in considering how the Board might be of assistance in furthering the DoIT mission to secure government information systems against illegal intrusions and other criminal activities.

With that in mind, we will hear from both Mr. Savage, a Board member and the DoIT Director, and Mr. Elste, the new Chief Information Security Officer.

MR. SAVAGE:

The role of the DoIT Office of Information Security is to serve the entire State. It has evolved and expanded a great deal over the last several years. In 2000, when I was first hired, there was no organized State-wide security effort at all. We started the office with a single person. We were granted two additional positions during the 2003 Legislative session for a total of three. In the 2005 session, we were granted a total of five additional positions for a total of eight. We will be requesting even more additional positions during the upcoming 2007 Legislative session.

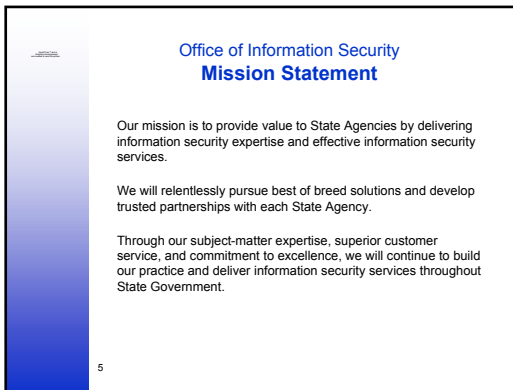
We take information security very seriously. I would like to turn the presentation over to Mr. Jim Elste. He has gotten considerable work done in the short time he has been with us.

MR. ELSTE:

As Mr. Savage mentioned, I am the new Nevada Chief Information Security Officer and have been on the job for four weeks. I have been trying to understand what our present capabilities are, in part, to be able to articulate that to various organizations and groups.

My presentation will provide an overview with a focus on services relevant to the law enforcement community.

Let me begin by sharing my credentials. I have been in information security for 10 years and IT for 20. I hold a CISSP and CISM, two security certifications. I came to Nevada from Massachusetts where I was the chief security officer for the executive office of Health and Human Services. I have a background in information security consulting with organizations like IBM, Ernst & Young. I have also done independent consulting. I have observed security issues in both public and private environments. The basics of information security apply regardless of the type of organization.



Office of Information Security
Mission Statement

Our mission is to provide value to State Agencies by delivering information security expertise and effective information security services.

We will relentlessly pursue best of breed solutions and develop trusted partnerships with each State Agency.

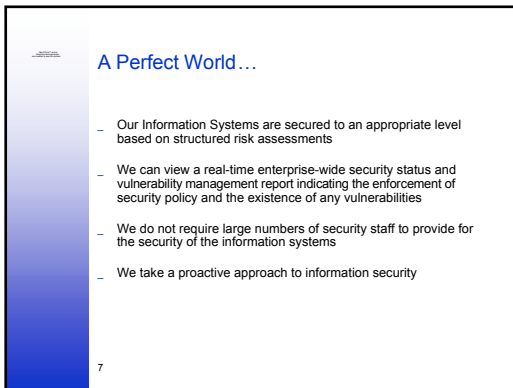
Through our subject-matter expertise, superior customer service, and commitment to excellence, we will continue to build our practice and deliver information security services throughout State Government.

5

We have developed a mission statement for the Office of Information Security. Fundamentally, we are to provide value to State agencies by delivering information security expertise and effective information services. We will relentlessly pursue “best of breed” solutions to ensure we develop trusted partnership with our agencies so that they can rely on us for their information security needs. We will provide subject matter expertise, a customer service approach, and a commitment to excellence in our practice in delivering information security services throughout the State government.

Turning to terminology, we consider vulnerabilities to be both weaknesses in the technical environment as well in the controls and procedures used to administer a technical environment. Those vulnerabilities give rise to risks. We are primarily concerned about the management of risks in our information securities systems environments.

The most succinct definition of risk is: “Risk is uncertainty that matters.” These are things we do not know that we are concerned about. By managing risk effectively, we can develop security – a feeling of being free from danger by implementing measures that improve our risk posture and minimize potential exploitation of vulnerabilities.



A Perfect World...

- Our Information Systems are secured to an appropriate level based on structured risk assessments
- We can view a real-time enterprise-wide security status and vulnerability management report indicating the enforcement of security policy and the existence of any vulnerabilities
- We do not require large numbers of security staff to provide for the security of the information systems
- We take a proactive approach to information security

7

If we were in a perfect world, our information systems would be secure at an appropriate level based on structured risk assessments. We could characterize the risk and put the appropriate controls in place. We would be able to view in real time information about vulnerabilities and how they are addressed. We would know whether there are policy violations. We would not require large numbers of staff to enable information security in our environment. Everything we did would be fundamentally pro-active. That is for a perfect world.

The real world is different. For the most part, we do not really know where we are in terms of vulnerabilities, the risks, and our security posture. Our security staff and our systems administrators are stretched to the breaking point. They have many priorities and much work to do. We operate in a reactive mode at present. To a very large extent, we simply hope that the

information systems are not compromised or attacked. Hope is not a very effective security measure.

In moving forward, we need to consider what we are trying to protect. What information is valuable? What are the systems that support that valuable information? What is the infrastructure that underlies those systems? We have to understand our information philosophy. What is an acceptable risk tolerance? What is appropriate from the perspective of process control and technology? We need to understand what level of security we want, or need to achieve, in our environments.

Effective Risk Management

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to **protect the organization and its ability to perform the mission**, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

- NIST Special Publication 800-30 Rev A

10

Finally, we need some mechanism to measure the effectiveness of our information security program. At the end of the day, we are addressing effective risk management. This is guidance from NIST on risk management. Risk management is protecting the organization and its ability to perform its mission. Regardless of the mission of a State agency, information security focuses on protecting those information systems that are relied upon in the performance of the agency mission through risk management and good security practices.

There are four basic elements in the information security life cycle. "Assessments" means being able to understand the risks we are exposed to. We look to protecting our environment and putting certain security measures and countermeasures in place. We look to monitoring our environment so we know when a security event takes place. We need a structured response to security incidents in our environment.

We are doing security risk assessments and technical vulnerability assessments as well as physical security assessments for the different agencies. From a protection standpoint, we are

looking at the policy, standards, and procedures. These articulate proper practices that should be adhered to.

Information Security Lifecycle - Elements

Assess <ul style="list-style-type: none">- Security Risk Assessments- Technical Vulnerability Assessments- Physical Security Assessments	Monitor <ul style="list-style-type: none">- Intrusion Detection Systems (NIDS/HIDS)- Web Traffic Monitoring- Log File Reviews
Protect <ul style="list-style-type: none">- Policies, Standards, & Procedures- Technical Security Architecture- Security Awareness & Training	Respond <ul style="list-style-type: none">- Computer Security Incident Response Team (CSIRT)- Continuity of Operations & Disaster Recovery Planning (COOP/DRP)- Security Investigations & Forensics

12

The technical security architecture addresses the mechanisms that should be employed to protect our environments.

The final piece is security awareness and training. This entails educating our end user community so that it is the first line of defense.

When it comes to monitoring, we are considering intrusion detection systems able to do such things as web traffic monitoring and the review of log files to detect an actual security incident. I am a serious advocate of formalizing our response capabilities. We need to construct a security incident response team. We need to develop and promulgate continuity of operations and disaster recovery plans. We need to engage, as needed, in computer investigations and forensics. I will speak later about forensics.

Rather than focus on assessment and our protection mechanisms, it is more appropriate to a law enforcement perspective that we deal with monitoring and response capabilities. Monitoring can be illustrated by this information from the Defense Information Systems Agency. The underlying data is a bit dated; they did a vulnerability assessment in the early 1990s.

They launched 38,000 attacks against federal agencies. The protection mechanisms of the targeted agencies blocked about 35% of the attacks, some 13,000 attacks. That means 24,000 attacks managed to penetrate the environment. From a detection perspective, only 4% of those attacks were detected. So out of 24,700 attacks, 988 were detected. Of those 988 detected attacks, only 267 were reported. Put another way, if a single attack were to constitute a security incident, the chance that security incident would be detected and reported was about 0.7%.

We need to be able to detect events occurring in our environment with a fair degree of certainty. We also need to ensure those detections are reported to our incident response capability so that a response is possible.

The question is: How do we identify an attack? An increase in overall network traffic, higher CPU or memory utilization, unexpected levels of traffic generated by internal hosts, unexpectedly large log file entries, an unexpected change in the mix of traffic carried by a network – all of these things tend to indicate an incident of some sort is taking place.

I would like to be able to explain how monitoring could reveal unauthorized access and unwanted internal activity. However, issues of how, when and where we monitor involve issues that are inappropriate to discuss in a public forum. Those capabilities are available to defend our systems. We do not want to inform those people with malicious intent what we are able to capture in our environment.

Incident Management - CSIRT

Incident Management is designed to provide a structured response capability based on a documented Incident Management Plan.

- Develop and document an Incident Management Plan and associated procedures.
- Form a **Computer Security Incident Response Team (CSIRT)**
 - a CSIRT is a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency.
- Benefits of a CSIRT include:
 - Limit damage caused by incident
 - Technological
 - Financial
 - Public relations
 - Personnel
 - Enable resolution of incident
 - Enhance resiliency
 - Learn to improve security
 - Facilitate Disciplinary Action and/or Prosecution

18

Once we detect an event, we need to have a structured response to that event. This is accomplished primarily through the existence of an incident management plan. There are several elements involved. First, a formal, documented incident management plan is necessary. Second, a computer incident response team needs to be formed. We do have an incident response team in place. One of my duties is to ensure that members of that team have structured information and guidance on their roles and responsibilities in responding to an incident.

The notion of this team entails the coordination of an appropriate response to a security incident for a defined constituency. So, I need to investigate the needs and expectations of the end user as part of the work of designing the team.

The benefits are pretty clear. A good, organized response can limit the impact of a security incident. We can limit the impact technically, from a public relations perspective, from a personnel perspective, as well as limiting any financial damage.

Six Stages of Incident Management

1. Avoiding the incident.
2. Preparing to manage the incident.
3. Recognizing the incident.
4. Containing the incident.
5. Resolving the incident.
6. Learning from the incident.

20

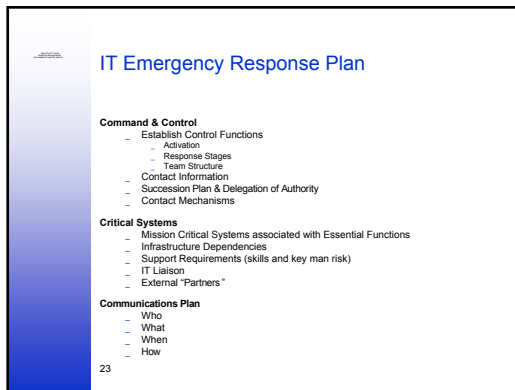
There are six phases of incident response of concern. First and foremost is preparation. The better prepared we are before an incident, the better our chances of providing a coordinated response. Once an incident occurs, we need to identify that occurrence, classify the incident, and attempting to trace the incident to its origins. We then need a structured response to limit the damage, and, as quickly as possible, remove the incident from the environment. Then a post-mortem is needed to understand what happened, what we could have done better, and what can be done in the future to improve countermeasures and/or our

internal practices in response.

We would like to avoid an incident if possible. We must be prepared to manage the incident. Once it occurs we need to recognize it, contain it, resolve it, and learn from it.

These measures blend into the related issue of continuity of operations planning and disaster recovery planning. A security incident falls into the higher probability category of occurrence than does a disaster or significant physical catastrophe. However, the potential for such a catastrophe exists. As part of our security function, we need to ensure that an organization is prepared to respond to disasters or catastrophic events.

An understanding of the critical functions of an organization is critical to planning a response for disaster or physical catastrophe. Delegation of authority and succession planning within an organization are also key elements. Critical systems that support the organization must be identified. We need to be able to “devolve” the organization, or relocate the organization to a disaster recovery site. Communications plans need to be created so that during a disaster, the protocols for communication are well understood and work efficiently.



There are several important additional considerations in an emergency response plan from an IT perspective. Command and control is essential. Who is going to activate the plan? What are the immediate steps in response? Contact information for the responders is critical. Having a succession plan to deal with the unavailability of a member of the team is also necessary. Communications means having viable alternatives since the office phones and the office email system may not be operational or effective in a disaster scenario.

Mission critical systems and the associated essential functions must be well understood. The infrastructure dependencies must be elaborated so that an appropriate infrastructure can be created to support the necessary systems.

Support requirements drives toward the concept of “key man risk” – if there is a single individual who knows how to operate the application or the data base that supports the application, that individual has become a single point of failure. There need to be liaisons into the IT world and an understanding of identified external partners. These are also part of the strategic response mix.

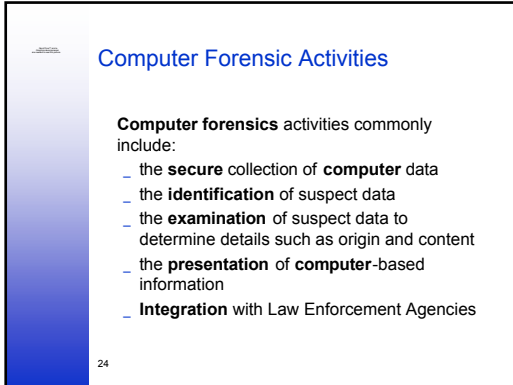
The communications issues are fairly straightforward. Who do we need to communicate with? What are we going to be communicating about? When do we communicate with them, and how do we communicate with them?

Lastly, I want to address computer forensics. I know the Board is interested in this issue. I know that Mr. Earl has described the budget request, and that law enforcement is particularly keen to have a computer forensics capability.

From the Office of Information Security perspective, computer forensics is the front end of the investigation where we determine whether an event constitutes a criminal act. If so, then we engage law enforcement at that time, and turn over our investigation to law enforcement investigators.

Our forensics capability has to be able to discriminate between administrative incidents and criminal occurrences. For example, we might deal with sexual harassment where we might

investigate email exchanges and make a determination with HR and management whether conduct constituted a criminal act. If so, we would engage law enforcement.



Computer Forensic Activities

Computer forensics activities commonly include:

- the **secure** collection of **computer** data
- the **identification** of suspect data
- the **examination** of suspect data to determine details such as origin and content
- the **presentation** of **computer**-based information
- **Integration** with Law Enforcement Agencies

24

We do not want to impair law enforcement investigations by not having a good forensics capability in house. If we confiscate a computer as part of an administrative or security incident response, we want to ensure we maintain the evidentiary value of material when it gets transferred to law enforcement.

This is the natural bridge between information security and the threshold engagement of law enforcement. We need to have a very good marriage between these two functions so that law enforcement is confident that nothing our forensics

capability does will impair evidence in the process. We need to know who to contact when, and how to contact law enforcement in order to engage as quickly as possible.

We need to flush this out, and this venue seems to be the appropriate one to table these considerations. We need to tie our operations together very tightly.

I spend time working on security in Malaysia. In conclusion, I found this quotation very helpful. "Don't think there are no crocodiles just because the water is calm." Just because the alarm bell has not gone off today does not mean that security incidents are not high risk. We in information security will do everything we can to assess the situation, to provide good guidance on protection mechanisms, to monitor the environment, and to respond to incidents as effectively as possible.

I will be happy to take any questions.

RAC COLLEDGE:

We have discussed, both formally and informally, the seamless transition from the administrative to the criminal. Having worked internal affairs within the old U.S. Customs Service, I am very familiar with the problems. What may start off as an event that appears to be administrative on its face, can suddenly be transformed into a bizarre criminal investigation. There may have been no indication that criminal acts were being committed using a governmental system. I think we might want to follow up on this, not only with my organization, but also with both FBI and Secret Service involvement at the federal level. The Attorney General's Office and the Department of Public Safety should be involved at the State level.

Your natural progression would be to contact State agencies first, and then, depending on the threat, if it extended beyond the borders of the State or the United States, federal issues would likely be involved.

The evidentiary issue is one that we as a group, and as representatives of individual law enforcement agencies, are very concerned about. The transition from State to federal is important. Evidence must be preserved so that it meets requirements at the federal level that may not exist at the State or local level.

We should address these issues at an earlier opportunity in a smaller, more select group.

MR. SAVAGE:

I agree with that 100%.

MR. EARL:

If my office can facilitate those discussions either north or south, I would certainly be glad to. I am not sure what that might entail. We can discuss that off line. One of the Board's missions is to facilitate cooperation among federal, State, and local officers in detecting, investigating, and prosecuting technological crime. Certainly any incident involving the possible compromise of the State's information and technology systems falls into that category. Not only is cooperation important for the reason identified by Mr. Colledge (the implication of federal statutes and federal crimes), but also because, at the present time, the bulk of the computer forensic assets within Nevada are in the hands of federal agencies.

If, for example, there is a State computer system in the north implicated in any type of crime – whether the target of an external attack or internally used to commit one crime or another – the actual computer forensics examination would, at present, be conducted by a federal officer. One of Mr. Colledge's personnel would conduct any examination.

For both of these reasons, it is important we engage in the grassroots liaison so that DoIT operational personnel know who to call, when to call, and know what to expect in terms of assistance from both State and federal law enforcement agencies.

After sitting through briefings that FBI, ICE, and Secret Service personnel have provided to attorney groups around the State, I know that those agencies are increasingly sensitive the disruption that can occur in a corporation or government agency if portions of networks are seized in a criminal investigation. I think there also needs to be some protocol, worked out in advance, so that Mr. Savage's people will be aware of the requirements of various law enforcement agencies regarding the seizure or replication of hard drives that might be implicated. We need to be able to balance the State's interest in ensuring that its computer information systems remain on line and functional during the period of any investigation regardless of whether the incident is administrative or a more involved criminal investigation.

I think all this is ripe for discussions involving DoIT and law enforcement personnel.

RAC COLLEDGE:

Let me suggest that between now and the next Board meeting, we convene a working group to take a look at this, particularly before the Legislative session ends, given that both DoIT and the Attorney General's Office have interest in additional staffing and resources. It may be appropriate to ensure the Legislature is aware that various law enforcement agencies are cooperating to reach some of these protocols and identifying other concerns.

MR. SAVAGE:

I agree completely. That is definitely the right way to go.

SAC MARTINEZ:

Absolutely. We at the FBI will be available at any time with any level of expertise we need to plug into that conversation. I think it is very encouraging we all recognize the need to have this lash-up and to be able to conduct, at the State level, the type of forensic examinations that can then be handed over. This is very, very important. Federal officials walk into some very messed up situations when we work intrusion cases. We are best able to help those who have done a good job of observing all the protocols that have been discussed today.

I do want to raise an additional issue. Having a media response plan ahead of time, especially if there is a data breach, is extremely important. At present, media will focus like a laser on any incident of that type. You have all read reports for other states, the University of California system and the state of Alaska, for example. You will be inundated with media interest. Having a previous walk-through will really put you ahead of the game should an incident arise that touches on these issues.

Agenda Item 8 – Report, discussion, recommendations and actions regarding budget submission and legislative proposals.

MR. EARL:

The budget for fiscal years 2008 and 2009 that was approved by the Board has been incorporated into the budget submission of the Office of the Attorney General. I undertook some late coordination with Dale Liebherr, the Interim Chief Investigator in the Attorney General's Office to ensure that compensation levels for the requested forensic computer examiners and investigators were consistent with those existing within the department.

I have discussed the Board, its mission, our mission review of the spring, and the budget with the analyst in the Legislative Counsel Bureau who will present the Board's request to the money committees during the legislative session. I have offered further in-depth discussions, and I believe it is fair to say that there is a good understanding of the Board's concerns and interests.

Shortly after the last Board meeting, I provided the Legislative Counsel Bureau staff with the changes the Board has proposed for its underlying statute, NRS205A, and with the forfeiture legislation approved in concept by the Board last spring. Within the last week, the week preceding this meeting, I have checked with the supervising attorney, and was assured that drafting within the LCB was proceeding without apparent problems. Obviously, I will continue to monitor that and follow through to ensure that the Board's recommended legislative changes are fully incorporated into the Bill Draft Request (BDR).

Agenda Item 9 – Report on action regarding data compromise at the Department of Veterans Affairs.

MR. EARL:

At our last meeting, Board Chairman, Attorney General Chanos, undertook to consider sending a letter in his capacity as Attorney General rather than as Board Chair, to the Nevada Congressional Delegation expressing concern about the potential data compromise at the Veterans Administration through the loss, and, fortunately, the subsequent recovery, of a laptop computer and external storage device.

I want to report to the Board that such a letter was sent. Board members have been provided with an electronic copy of the Attorney General's letter. Prior to the delivery of that letter to the offices of the Nevada Congressional Delegation members, I was in contact with the relevant staffer in each of those offices. Copies of that letter were also provided to key veterans groups. I am unaware of any follow-up, certainly none has been directed to me, nor, I believe, to Attorney General Chanos. I attribute this to the public assurances that were provided in the weeks after the laptop computer was recovered. I felt it important to inform the Board that the action discussed at our last meeting was undertaken by the Attorney General.

While I have the floor, I would like to thank all the speakers who presented here. Special thanks go to Ms. Dixie Stephens, who came back a second time. We appreciate the update.

Agenda Item 10 – Board Comments

RAC COLLEDGE:

Are there comments from any Board members? I hear none.

Agenda Item 11 – Public Comments

RAC COLLEDGE:

Are there comments from members of the public? I hear none.

Agenda Item 12 – Scheduling of future meetings

MR. EARL:

The scheduling of our next meeting is likely to be problematic. The 74th Legislative begins on February 5, 2007. This poses several challenges. It is highly unlikely we will be able to meet in the LCB facilities we are in presently. Second, our legislative members, and the incoming Attorney General to a lesser degree, will be on call for legislative duties and testimony. Other Board members may find themselves in Carson City from time to time.

I have talked to Senator Wiener. She suggested the Board attempt to meet during the first several weeks of the Legislative session. If that is amenable to the Board, I will attempt to schedule a meeting, probably using facilities within the Attorney General's Office sometime during the last two weeks of February. I would be looking for as many Board members as possible to attend physically in Carson City.

Does any Board member have suggestions or other information that would bear on how or when we next meet?

MR. FERGUSON:

I am sure Mr. Earl has already spoken to someone at the Attorney General's Office regarding use of our conference rooms here and in Carson City. I am sure we would be able to make arrangements for the use of those facilities in the absence of the LCB rooms.

MR. EARL:

If there are no other comments, I will move forward with scheduling early in the Legislative session.

RAC COLLEDGE:

I would like to thank everyone for attending today. I thought the speakers were very informative, and I look to working with everyone in the future.

The Board meeting adjourned at 11:43 a.m.

Respectfully submitted,

James D. Earl
Executive Director

Approved by the Board at its subsequent meeting on March 20, 2007.