

# **EXHIBIT D**

00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

ORIGINAL

filed by LUCY

1 RONALD RUS, #67369  
 rrus@rusmiliband.com  
 2 LEO J. PRESIADO, #166721  
 lpresiado@rusmiliband.com  
 3 RUS, MILIBAND & SMITH  
 A Professional Corporation  
 4 Seventh Floor  
 2211 Michelson Drive  
 5 Irvine, California 92612  
 Telephone: (949) 752-7100  
 6 Facsimile: (949) 252-1514

**FILED**  
 SUPERIOR COURT OF CALIFORNIA  
 COUNTY OF ORANGE  
 CENTRAL JUSTICE CENTER

SEP 29 2008

ALAN CARLSON, Clerk of the Court

R. Lucey  
BY R. LUCEY

BY FAX

7 Attorneys for Defendants BRIAN DUNNING and  
 8 THUNDERWOOD HOLDINGS, INC.

10 SUPERIOR COURT OF THE STATE OF CALIFORNIA  
 11 COUNTY OF ORANGE, CENTRAL JUSTICE CENTER

12 COMMISSION JUNCTION, INC.,

13 Plaintiff,

14 vs.

15 THUNDERWOOD HOLDINGS, INC. dba  
 16 KESSLER'S FLYING CIRCUS; TODD  
 DUNNING; BRIAN DUNNING; and  
 17 DOES 1 through 50, inclusive,

18 Defendants.

12 CASE NO. <sup>08</sup>00101025

13 [ASSIGNED FOR ALL PURPOSES TO  
 14 THE HONORABLE RANDELL L.  
 WILKINSON, DEPT. C25]

15 NOTICE OF MOTION AND MOTION TO  
 16 STAY DISCOVERY PENDING  
 17 CONCLUSION OF CRIMINAL  
 PROCEEDINGS; MEMORANDUM OF  
 18 POINTS AND AUTHORITIES;  
 DECLARATIONS OF WILLIAM J.  
 KOPENY AND BRIAN DUNNING IN  
 19 SUPPORT

20 DATE: October 29, 2008  
 21 TIME: 1:30 p.m.  
 22 DEPT.: C25

23 ///  
 24 ///  
 25 ///  
 26 ///  
 27 ///  
 28 ///

1

DECLARATION OF WILLIAM J. KOPENY

2

I, WILLIAM J. KOPENY, declare as follows:

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1. I am an attorney at law duly licensed to practice before the above-entitled Court. I represent Brian Dunning in connection with that certain criminal investigation described in more detail below. I have been a member of the bar of the United States District Court for the Central District of California since December 20, 1974, and have been representing individuals in connection with criminal investigations and criminal prosecutions for over 34 years. I have firsthand personal knowledge of the matters set forth herein, and if called upon to testify, would and could competently testify thereto.

2. In June 2007, I was retained by Brian Dunning as criminal counsel, in connection with the execution of a search warrant at his home on June 18, 2007, and his interrogation by agents of the Federal Bureau of Investigation ("FBI"). I immediately contacted the local FBI agents, one of whom I knew from a prior federal criminal matter I had handled, and I was informed that: (a) Mr. Dunning was being investigated for computer crimes by agents from the San Francisco Bay area; and (b) the items seized under the search warrant, which consisted primarily of computers, computer media, and hard copy documents, were in the custody of the agents in charge of the case and/or the Office of the United States Attorney for the Northern District of California.

3. I then contacted the FBI agents involved in the execution of the search warrant from the San Francisco Bay area and learned that the assigned federal prosecutor is Kyle F. Waldinger who is the United States Attorney in charge of the Computer Hacking and Intellectual Property Unit ("CHIP Unit") of the Office United States Attorney for the Northern District of California.

4. Because initially, the searching agents had informed Mr. Dunning that anything the agents needed would be copied and that the computers and other materials seized would be returned within two weeks, on July 3, 2007, I contacted Mr. Waldinger to inquire whether Mr. Dunning was a "target" of the investigation, and whether we could expect his property to be returned within the time frame promised by the agents on the scene of the

1 search. Mr. Waldinger informed me that: (a) Mr. Brian Dunning is a target of the  
2 investigation, along with two other named persons; (b) the federal government is confident that  
3 a criminal offense could be proven, based on the fraudulent conduct of one or more persons;  
4 and (c) until the federal government has concluded its analysis of the computer media seized,  
5 the federal government is unwilling to discuss any resolution of its case. Since that first  
6 telephone call with Mr. Waldinger, I have had at least six other phone conversations with him  
7 and faxed to him at least three letters.

8           5. I have reviewed my file and in those letters I have confirmed in writing  
9 that Mr. Waldinger advised me that: (1) Mr. Dunning is a "target" of the federal criminal  
10 investigation; (2) the investigation concerns Thunderwood Holdings, Inc. ("Thunderwood")  
11 and Kessler's Flying Circus ("KFC") and its relationship with eBay, and allegations that  
12 "cookies" had been "forced" in violation of the terms of service with eBay and/or Plaintiff  
13 Commission Junction, Inc. ("Plaintiff"), which allegedly constitutes "cyber-fraud" under  
14 various federal fraud statutes.

15           6. Periodically, and as recently as September 18, 2008, I have conferred  
16 with Mr. Waldinger, and he has continued to confirm that Mr. Dunning is a target of an active  
17 investigation, that the federal government is not yet done with its investigation or analysis of  
18 the computers seized, and that he will contact me in the event an indictment is issued naming  
19 my client as a defendant, including any indictment for fraud, in which Plaintiff and/or eBay is  
20 the named victim based on the above. The investigation remains open and active.

21           7. Mr. Waldinger has confirmed that the criminal investigation of  
22 Mr. Dunning is ongoing, that search warrants other than that discussed above have issued, and  
23 in my opinion, based on my experience, I believe it is likely that the federal government has  
24 presented testimony in this investigation to the United States Grand Jury for the Northern  
25 District of California. In addition, the federal government has sought from the District Court,  
26 and obtained, several extensions of time to return all the materials seized from Mr. Dunning's  
27 home pursuant to the aforementioned federal search warrant, which called for its return within  
28 60 days unless additional time is granted. Typically, in order to obtain such permission from

1 the federal court, the United States Attorney must allege that there is an active criminal  
2 investigation, that the federal government believes the property seized constitutes, or is likely  
3 to constitute evidence of the suspected crime, and that additional time is reasonably needed to  
4 complete the investigation. With the exception of approximately 10% of the items seized,  
5 which items have nothing to do with eBay, Plaintiff or KFC, the federal government remains in  
6 possession of all other materials seized from Mr. Dunning, on the basis of its continued  
7 criminal investigation of him.

8           8. By its own description on the United States Department of Justice  
9 website, the CHIP Unit is charged with combating "cybercrime and intellectual property theft."  
10 In fact, that unit, and Mr. Waldinger have acquired a national reputation for being the first  
11 prosecutors in the nation to bring and win cyber-prosecutions based on previously untested  
12 legal theories. A true and correct copy of this description found on the website of the  
13 Department of Justice, is attached as Exhibit "3." In addition, the CHIP unit "works closely  
14 with the FBI and other agencies to establish a relationship with the local high tech community  
15 and encourage them to refer cases to law enforcement." A true and correct copy of this  
16 description found on the website of the Department of Justice, is attached as Exhibit "4."  
17 The CHIP Unit is specifically charged with coordinating law enforcement and the technology  
18 industry "to share expertise and information technology, to assist each other 24 hours a day,  
19 seven days a week, around the clock, to prevent cybercrime wherever possible..." A true and  
20 correct copy of this description found on the website of the Department of Justice, is attached  
21 hereto as Exhibit "5."

22           9. The word "target" is a term of art within the United States Department of  
23 Justice, and it is to be distinguished from a "witness" and/or a "person of interest." Under  
24 Justice Department guidelines, the prosecutor is required to inform a person or his attorney  
25 when he has achieved the status of "target" because that person is actively believed to be a  
26 future defendant, based on an ongoing investigation. This guideline is in place to avoid any  
27 later claim that the "target" failed to invoke his rights against self-incrimination because he or  
28 she wrongly believed he was not going to be prosecuted. Thus, anyone who is informed that

00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

1 he is a "target" has an enormous motive to obtain counsel and assert his privilege against self-  
2 incrimination.

3 10. On advice of and through counsel, Mr. Dunning has asserted his right to  
4 remain silent, i.e., has asserted his Constitutional privilege against self-incrimination under the  
5 Fifth Amendment to the United States Constitution following the execution of a search warrant  
6 at his home and the questioning by FBI agents, and I have advised him to assert the same  
7 privilege in response to any question asked of him at any deposition, in response to any  
8 interrogatory or request for admission, and in response to any demand for production of  
9 documents (the possession of which is privileged under *United States v. Doe* (1988) 487 U.S.  
10 201, 108 S.Ct. 2341, 101 L.Ed.2d 184).<sup>4'</sup>

11 11. Under the Fifth Amendment, a person need not be guilty of any crime to  
12 enjoy a Constitutional privilege not to provide information that the government or any party  
13 seeks to compel him or her to provide. (*People v. Lucas* (1995) 12 Cal.4th 415, 453  
14 ["Innocent persons, as well as the guilty, are entitled to invoke the privilege"]; *Grunewald v.*  
15 *United States* (1957) 353 U.S. 391, 421, 77 S.Ct. 963, 982, 1 L.Ed.2d 931; see also Ratner,  
16 *Consequences of Exercising the Privilege Against Self-Incrimination.*) Rather, if the  
17 information sought *could, conceivably*, form a single evidentiary or factual link in a chain of  
18 circumstantial evidence which chain of evidence *could support an inference* that the person is  
19 culpable for any criminal offense, in violation of any state or federal law, that person cannot be  
20 compelled by legal process, subpoena or court order to provide such information, upon his or  
21 her invocation of the protection of the Fifth Amendment. (*Hoffman v. United States* (1951)  
22 341 U.S. 479, 486, 71 S.Ct. 814, 818, 95 L.Ed. 1118; *United States v. Neff* (9<sup>th</sup> Cir. 1980)

23  
24  
25 <sup>4'</sup> On behalf of Mr. Dunning I herewith assert that in producing such records he would be "testifying" as to  
26 their existence and to his control over them in a way that is protected by his Fifth Amendment privilege against  
27 self-incrimination. *Fisher v. United States* (1976) 425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39; *United States v.*  
28 *Doe* (1984) 465 U.S. 605, 104 S.Ct. 1237, 79 L.Ed.2d 552 (*Doe I*); and *Doe v. United States* (1988) 487 U.S.  
201, 108 S.Ct. 2341, 101 L.Ed.2d 184 (*Doe II*), a line of cases in which the Supreme Court emphasized that the  
act of producing potentially incriminating documents under government compulsion may have impermissible  
testimonial aspects. These cases are applicable to this case since they hold that the Fifth Amendment protects  
against compulsory surrender of (1) personal business records, (2) in the possession of a sole proprietor or  
practitioner, (3) with respect to the testimonial act implicit in the surrender itself.

00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

1 615 P.2d 1235, 1239; *Prudhomme v. Superior Court* (1970) 2 Cal.3d 320, 325-326; *In re*  
 2 *Misener* (1985) 38 Cal.3d 543, 546-551.)

3 12. I have reviewed the complaint in this matter and based on my  
 4 understanding of the allegations and issues in this civil matter, Mr. Dunning has, through  
 5 counsel, already asserted his Fifth Amendment privilege against self-incrimination in  
 6 connection with an inquiry by the Federal Government into the identical facts alleged in this  
 7 case, and clearly is entitled to its protection in the context of this case. In my opinion, any  
 8 court order compelling Mr. Dunning to respond to the allegations of the complaint, and/or to  
 9 respond to discovery propounded to him would constitute "compelled self-incrimination"  
 10 within the meaning of the Fifth Amendment and California's constitutional privilege against  
 11 self-incrimination. (Please see *People v. Lucas, supra*, 12 Cal.4th at 453.)<sup>27</sup>

12 13. Based on these descriptions of the function, purpose and manner of  
 13 operating on the part of the CHIP Unit, together with my 34 years of experience defending  
 14 individuals in criminal cases, it is clear that any and all information obtained from  
 15 Mr. Dunning in the course of discovery in this case will be shared with, and will be monitored  
 16 by, the federal government in aid of the criminal investigation and/or prosecution of  
 17 Mr. Dunning.

18 I declare under penalty of perjury under the laws of the State of California that  
 19 the foregoing is true and correct.

20 Executed this 29th day of September, 2008, at Irvine, California.

21   
 22 \_\_\_\_\_  
 23 WILLIAM J. KOPNY

24  
 25  
 26 <sup>27</sup> "[I]n order to approve invocation of the privilege "it need only be evident from the implications of the  
 27 question, in the setting in which it is asked, that a responsive answer to the question or an explanation of why it  
 28 cannot be answered might be dangerous because injurious disclosure could result." ( *People v. Cudjo, supra*, 6  
 Cal.4th at p. 617, 25 Cal.Rptr.2d 390, 863 P.2d 635, quoting *Hoffman v. United States* (1951) 341 U.S. 479, 486,  
 71 S.Ct. 814, 818, 95 L.Ed. 1118.)" *Id.* at p. 453 [Underlining and Italics supplied.]

EXHIBIT  
3



00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

**EXHIBIT "3"**

EXHIBIT  
4

00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

[Email this Document](#)

**CHIP (COMPUTER HACKING AND INTELLECTUAL PROPERTY)  
FACT SHEET**

**HISTORY**

Nine additional units will be added to a program called CHIP (Computer Hacking and Intellectual Property) that has proven successful in Northern California. That project demonstrated the benefits of a unit of prosecutors working closely with the FBI and other agencies to establish a relationship with the local high tech community and encourage them to refer cases to law enforcement. In addition, the project provides the skills and training not yet available to law enforcement on a widespread basis.

The new CHIP units are the next phase in the Department's ongoing efforts to combat cybercrime and Intellectual Property theft. In 1991, the Department created what is now the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division. This Section is comprised of 22 attorneys who specialize in these crimes and provide national training, advice and coordinate prosecution of computer intrusion and intellectual property cases. The CHIP team members will complement the highly trained network of prosecutors at CCIPS and the US Attorneys' Offices.

**PROGRAM DETAILS**

CHIP units will be established in eight cities in addition to San Francisco, where the concept was pioneered. The cities have been chosen based on a number of factors, including their proximity to high-tech industry areas, their potential for growth in that area and the presence of adequate FBI resources to investigate these crimes.

-Los Angeles	-Dallas
-San Diego	-Seattle
-Atlanta	-Alexandria, Virginia
-Boston	
-New York (Brooklyn and Manhattan)	

- Together, the 10 units will have a total of 77 positions, including 48 prosecutors.
- This will provide 4 to 6 prosecutors in each participating district, through combining new and existing resources in the selected districts.

**RESOURCES**

The FY 2001 Appropriation provided \$3,074,000 to fund 50 positions and 25 FTE, including 28 attorneys.

The following chart shows the proposed unit composition:

Districts	New AUSA Allocation	"AUSA" District Match	Total CHIP AUSAs	New Paralegal Allocation	New Support Allocation	"Support" District Match	Unit Position Total
California CD	2	4	6	1	1	2	10
California ND	4	2	6	1	2	1	10
California SD	2	2	4	1	1	2	8
Georgia ND	2	1	3	0	0	0	3

	00/00/0000	08:37	FIRST LEGAL SUPPORT	714 541 8182			
Massachusetts	2	2	4	2	0	6	
New York ED	2	2	4	0	2	0	6
New York SD	3	2	5	0	1	1	7
Texas ND	3	1	4	0	2	0	6
Virginia ED	4	2	6	1	2	1	10
Washington WD	3	2	5	0	2	1	8
Total	28	20	48	4	17	8	77

## **COMPONENTS**

The program has 3 components: (1) **Prosecution**, (2) **Regional Prevention and Outreach** and (3) **Regional Training**.

### **1. Prosecution**

- CHIP units will prosecute computer intrusions, copyright and trademark violations, theft of trade secrets and economic espionage, theft of computer and high tech components and other Internet crimes.

### **2. Regional Prevention and Outreach**

- Prosecutors will work with CCIPS, the FBI and other agencies to establish good working relationships with the high tech community and to encourage victims of high tech crime to report such crimes to law enforcement.

### **3. Regional Training**

- Cybercrime fighting requires special skills. CHIP units will receive the same high-level training provided by CCIPS, but will also be expected to develop and offer regional training programs to increase expertise among federal, state and local prosecutors.

- CHIP units will also be encouraged to send attorneys to work at CCIPS to train, and to call upon CCIPS for assistance in providing local training.

- **More information on: CHIPs Program**
- **More information on: Attorney General Ashcroft's Remarks**
- **More information on: Law Enforcement Coordination for High-Tech Crimes**
- **More information on: Intellectual Property Policy**
- **More information on: Computer Crime Policy**

Want to receive news of updates to the [cybercrime.gov](http://cybercrime.gov) website?

Send a blank message to: [cybercrime-subscribe@topica.com](mailto:cybercrime-subscribe@topica.com) and we will add you to our email newsletter list.  
([Mailing list privacy information](#))

Go to . . . [CCIPS home page](#) || [Justice Department home page](#)

Updated page December 9, 2002  
[usdoj-crm/mis/lrr](#)

00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

**EXHIBIT "4"**

00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

[Email this Document!](#)

**CHIP (COMPUTER HACKING AND INTELLECTUAL PROPERTY)  
FACT SHEET**

**HISTORY**

Nine additional units will be added to a program called CHIP (Computer Hacking and Intellectual Property) that has proven successful in Northern California. That project demonstrated the benefits of a unit of prosecutors working closely with the FBI and other agencies to establish a relationship with the local high tech community and encourage them to refer cases to law enforcement. In addition, the project provides the skills and training not yet available to law enforcement on a widespread basis.

The new CHIP units are the next phase in the Department's ongoing efforts to combat cybercrime and Intellectual Property theft. In 1991, the Department created what is now the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division. This Section is comprised of 22 attorneys who specialize in these crimes and provide national training, advice and coordinate prosecution of computer intrusion and intellectual property cases. The CHIP team members will complement the highly trained network of prosecutors at CCIPS and the US Attorneys' Offices.

**PROGRAM DETAILS**

CHIP units will be established in eight cities in addition to San Francisco, where the concept was pioneered. The cities have been chosen based on a number of factors, including their proximity to high-tech industry areas, their potential for growth in that area and the presence of adequate FBI resources to investigate these crimes.

-Los Angeles	-Dallas
-San Diego	-Seattle
-Atlanta	-Alexandria, Virginia
-Boston	
-New York (Brooklyn and Manhattan)	

- Together, the 10 units will have a total of 77 positions, including 48 prosecutors.
- This will provide 4 to 6 prosecutors in each participating district, through combining new and existing resources in the selected districts.

**RESOURCES**

The FY 2001 Appropriation provided \$3,074,000 to fund 50 positions and 25 FTE, including 28 attorneys.

The following chart shows the proposed unit composition:

Districts	New AUSA Allocation	"AUSA" District Match	Total CHIP AUSAs	New Paralegal Allocation	New Support Allocation	"Support" District Match	Unit Position Total
California CD	2	4	6	1	1	2	10
California ND	4	2	6	1	2	1	10
California SD	2	2	4	1	1	2	8
Georgia ND	3	1	4	0	2	0	6

	00/00/0000	08:37	FIRST LEGAL SUPPORT	714 541 8182		
Massachusetts	2	4	0	2	0	6
New York ED	2	4	0	2	0	6
New York SD	3	2	5	0	1	7
Texas ND	3	1	4	0	2	6
Virginia ED	4	2	6	1	2	10
Washington WD	3	2	5	0	2	8
Total	28	20	48	4	17	77

## **COMPONENTS**

The program has 3 components: (1) Prosecution, (2) Regional Prevention and Outreach and (3) Regional Training.

### **1. Prosecution**

- CHIP units will prosecute computer intrusions, copyright and trademark violations, theft of trade secrets and economic espionage, theft of computer and high tech components and other Internet crimes.

### **2. Regional Prevention and Outreach**

- Prosecutors will work with CCIPS, the FBI and other agencies to establish good working relationships with the high tech community and to encourage victims of high tech crime to report such crimes to law enforcement.

### **3. Regional Training**

- Cybercrime fighting requires special skills. CHIP units will receive the same high-level training provided by CCIPS, but will also be expected to develop and offer regional training programs to increase expertise among federal, state and local prosecutors.

- CHIP units will also be encouraged to send attorneys to work at CCIPS to train, and to call upon CCIPS for assistance in providing local training.

- **More information on: CHIPs Program**
- **More information on: Attorney General Ashcroft's Remarks**
- **More information on: Law Enforcement Coordination for High-Tech Crimes**
- **More information on: Intellectual Property Policy**
- **More information on: Computer Crime Policy**

Want to receive news of updates to the [cybercrime.gov](http://cybercrime.gov) website?  
Send a blank message to: [cybercrime-subscribe@topica.com](mailto:cybercrime-subscribe@topica.com) and we will add you to our email-newsletter list.  
(Mailing list privacy information)

Go to . . . [CCIPS home page](#) || [Justice Department home page](#)

---

Updated page December 9, 2002  
[usdoj-crm/mis/terr](http://usdoj-crm/mis/terr)

---

EXHIBIT

5

---



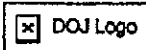
00000000

08:37

FIRST LEGAL SUPPORT

714 541 8182

**EXHIBIT "5"**



# Computer Crime and Intellectual Property Section (CCIPS)

## Law Enforcement Coordination for High-Tech Crimes

- 
- A. The Computer Hacking and Intellectual Property (CHIP) Program
  - B. High Technology Law Enforcement Training Opportunities
  - C. Coordination Between Law Enforcement and Industry
  - D. DOJ Speaks Out on Law Enforcement Coordination to Address Cybercrime

### A. The Computer Hacking and Intellectual Property (CHIP) Program

In 1995, at the recommendation of the then-Computer Crime Unit (now the Computer Crime and Intellectual Property Section (CCIPS)), the Department of Justice created the Computer and Telecommunication Coordinator (CTC) Program to protect the nation's businesses and citizens from the rising tide of computer crime and intellectual property theft by designating one or more prosecutors in every U.S. Attorney's Office to be responsible for these issues. In 2001, following a successful model developed in the Northern District of California, the Department expanded the program in ten cities by designating Computer Hacking and Intellectual Property (CHIP) units. These units typically involved more prosecutors than under the CTC program and were specifically charged with building relationships in-district with the FBI, other agencies, and the local high tech community. New units were added frequently thereafter. In 2005, the CTC and CHIP programs were combined into a unified CHIP program. More information on the CHIP Program and historical information on the CTC program is available below.

- CHIPs Unit Established in the Eastern District of California United States Attorney Office (October 19, 2004)
- CHIPs Unit Established in the Eastern District of Virginia United States Attorney Office (January 14, 2002)
- CHIPs Unit Established in Central District of California United States Attorney Office (September 6, 2001)
- CHIPs Unit Established in Southern District of New York United States Attorney Office (September 5, 2001)
- CHIPs Unit Established in the Eastern District of New York (August 21, 2001)
- Fact sheet on Computer Hacking and Intellectual Property (CHIP) units (July 20, 2001)

08/10/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

- Attorney General Ashcroft's Speech Announcing Expansion of CHIP Program and Establishment of Nine New CHIP units (July 20, 2001)
- The Computer and Telecommunications Coordinator (CTC) Program, Stacey Levine, USA Bulletin (May 2001)
- CTC Responsibilities

#### B. High Technology Law Enforcement Training Opportunities

- Training Opportunities

#### C. Coordination Between Law Enforcement and Industry

##### Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue

On April 5, 2000, the Department of Justice hosted a Cybercrime Summit at Stanford Law School, titled "Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation," at which Attorney General Janet Reno and members of the Justice Department and other law enforcement agencies met with representatives of information technology and Internet companies. The main topic of the Summit was how to improve cooperation between law enforcement and industry in investigating computer network hacking. Linked below are the Attorney General's Opening Remarks from the Summit, as well as the Question & Answer session between industry representatives and the Attorney General.

- Opening Remarks of Attorney General Janet Reno at the Cybercrime Summit (April 5, 2000)
- Question and Answer Session with Attorney General Janet Reno at the Cybercrime Summit (April 5, 2000)

##### The Cybercitizen Partnership: Industry and Government Alliance

On March 15, 1999, Attorney General Janet Reno announced a new Cybercitizen Partnership, a new alliance between law enforcement and the technology community. The goal of the partnership is to coordinate the efforts of government, industry and the public to ensure public safety and responsible computer use. The partnership will also promote computer ethics and civic responsibility in the cyber age and aid law enforcement and industry in the battle against "on-line outlaws." The partnership will consist of three complementary segments. The first segment is a "good cybercitizenship" public awareness campaign. The second is a user-friendly computer and network security directory to help public and private sector organizations quickly find computer security resources. The third is an Information Security Professional fellowship program between industry and government that will raise the awareness levels of participants with respect to the views, perspectives and needs of their respective counterparts.

00/00/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

- Statement by Attorney General Janet Reno to Announce the Cybercitizen Partnership at the ITAA Policy Summit (March 15, 1999)
- ITAA and Attorney General Janet Reno Unveil New Tech Partnership (March 15, 1999)

#### D. DOJ Speaks Out on Law Enforcement Coordination to Address Cybercrime

##### Assistant Attorney General Michael Chertoff's Testimony Before the House Subcommittee on Crime

On June 12, 2001, Assistant Attorney General Michael Chertoff testified before the Members of the Subcommittee on Crime of the Committee on the Judiciary. In his statement he addressed the nature of cybercrime and the Department's current efforts to combat that problem.

- Text of Assistant Attorney General Michael Chertoff's testimony before the House Subcommittee on Crime of the Committee on the Judiciary (June 12, 2001)

##### Attorney General Ashcroft's Remarks Before the First Annual Computer Privacy, Policy & Security Institute

On May 22, 2001, videotaped remarks by Attorney General John Ashcroft were presented before the first Annual Computer Privacy, Policy and Security Institute. In his speech, the Attorney General addressed the Institute's concerns of computer security and threats to information assets and the means by which industry and law enforcement can work together in fighting cybercrime.

- Text of Attorney General Ashcroft's Remarks Before the First Annual Computer Privacy, Policy & Security Institute (May 22, 2001)
- View Video Taped Remarks (21 Megabytes)  
\*Approximate download time: 56K Modem=55 minutes
- View Video Taped Remarks (13 Megabytes)  
\*Approximate download time: 56K Modem=35 minutes

*\*Note: the listed download times are estimated times under optimal conditions. Your actual download times may vary depending on your modem, internet traffic, and your internet connection type.*

##### Attorney General Reno's Address to the ITAA Cybercrime Summit

On June 9, 2000, Attorney General Janet Reno gave the keynote address at the ITAA Cybercrime Summit. In her speech, the Attorney General discussed the means by which industry and law enforcement can work together in fighting cybercrime. The text also includes the question and answer section.

- Text of Attorney General Reno's Keynote Address at the ITAA Cybercrime Summit (June 9, 2000)

09/30/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

### **Attorney General Janet Reno Testifies Before Senate Appropriations Committee**

On Monday, February 16, 2000, Attorney General Janet Reno testified before the United States Senate Committee on Appropriations. Her testimony provided an overview of cybercrime and the challenges that it presents to law enforcement today.

- Testimony by Attorney General Janet Reno before the United States Senate Committee on Appropriations (February 16, 2000)

### **Attorney General Janet Reno Introduces Law Net Initiative**

On January 10, 2000, Attorney General Janet Reno gave remarks before the National Association of Attorneys General in which she announced a new Law Net initiative. The Law Net will be a "strong, permanent network of federal, state and local computer crime experts to do the following: To share expertise and information technology, to assist each other 24 hours a day, seven days a week, around the clock, to prevent cybercrime wherever possible, and to bring those responsible for such crime, when it does occur, to justice; To work with industry, the academic world and privacy groups to build trust and to protect our privacy and the Constitutional rights of all Americans; And finally, to ensure that the Internet is a force that brings this world together and builds understanding across peoples and places and time.

- Remarks of the Honorable Janet Reno, Attorney General of the United States, to the National Association of Attorneys General (January 10, 2000)

### **Attorney General Janet Reno Addresses the High Technology Crime Investigation Association 1999 International Training Conference**

On Monday, September 20, 1999, Attorney General Janet Reno addressed the High Technology Crime Investigation Association 1999 International Training Conference in San Diego, California. Her speech focused on the importance of interagency and state and federal law enforcement cooperation, as well as on the Department of Justice's policy position on encryption regulation.

- Speech by Attorney General Janet Reno before the High Technology Crime Investigation Association 1999 International Training Conference (September 20, 1999)

### **President Clinton Addresses National Academy of Sciences on Keeping America Secure for the 21st Century**

On January 22, 1999, President William Jefferson Clinton addressed the National Academy of Science. His speech was titled "Keeping America Secure for the 21st Century." The speech he gave is available via the link below:

- President Clinton's Speech to National Academy of Sciences (January 22, 1999)

0000/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

**Go to . . . CCIPS home page || Justice Department home page**

---



08/10/0000

08:37

FIRST LEGAL SUPPORT

714 541 8182

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**SERVICE LIST**

*Commission Junction, Inc. v. Thunderwood Holdings, Inc., et. al.*  
OCSC Case No. 30-2008 00101025 CU BC CJC

ATTORNEYS FOR PLAINTIFF  
COMMISSION JUNCTION, INC.:

John H. Ernster, Esq.  
Phil J. Montoya, Jr., Esq.  
Ernster Law Offices, P.C.  
70 South Lake Avenue, Suite 750  
Pasadena, CA 91101  
Telephone: (626) 844-8800  
Facsimile: (626) 844-8944

CO-COUNSEL FOR PLAINTIFF  
COMMISSION JUNCTION, INC.:

Scott Patrick Barlow, Esq.  
General Counsel  
30699 Russell Ranch Road, Suite 250  
Westlake Village, CA 91362  
Telephone: (818) 575-4500  
Facsimile: (818) 575-4501

ATTORNEYS FOR CO-DEFENDANTS  
KESSLER'S FLYING CIRCUS AND  
TODD DUNNING:

Stewart H. Foreman, Esq.  
Freeland, Cooper & Foreman LLP  
150 Spear Street, Suite 1800  
San Francisco, CA 94105  
Telephone: (415) 541-0200  
Facsimile: (415) 495-4332  
E-mail: [foreman@freelandlaw.com](mailto:foreman@freelandlaw.com)