UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2006 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. VICTOR FAUR, aka SirVic, aka Victor, aka Viktor, aka VickTheTrick, aka SirVictor, aka VicMech, aka VicGov, aka VicOingo, aka VicNasa, Defendant.	CR 06- I N D I C T M E N T [18 U.S.C. § 371: Conspiracy; 18 U.S.C. §§ 1030(a)(5)(A)(i), (a)(5)(B)(i): Unauthorized Access To A Protected Computer Intentionally Causing Damage; 18 U.S.C. §§ 1030(a)(2)(B), (c)(2)(B)(ii): Accessing Computer To Obtain Information From Agency of the United States In Furtherance of Criminal Acts; 18 U.S.C. § 1030(a)(3): Unauthorized Access To A Nonpublic, Government Computer]

The Grand Jury charges:

COUNT ONE

[18 U.S.C. § 371]

I. GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. The National Aeronautics and Space Administration ("NASA") was a department and agency of the United States, and was charged with developing new flight technologies for Earth-

bound and extraterrestrial usage; exploring and collecting scientific data about the Earth, moon, solar system, and Universe; and providing technologies to be used to support existing exploration programs, including the space shuttles and the international space station.

a. The Jet Propulsion Laboratory ("JPL") was a NASA center that was staffed and managed for the United States government by the California Institute of Technology, and was accordingly referred to as a federally funded research and development center. JPL was located in Pasadena, California, within the Central District of California. JPL was NASA's lead center for robotic exploration of the solar system. JPL also managed many different computer systems responsible for communicating with various spacecraft, including the Deep Space Network, which communicates with spacecraft in deep space.

b. The Goddard Space Flight Center ("Goddard") was a NASA-administered facility, located in Greenbelt, Maryland, which was home to the largest organization of scientists and engineers in the United States dedicated to studying the Earth, the solar system, and the Universe. Goddard also managed the Earth Observation System Operations Center, which was the computer system responsible for directing the movement of various satellites in orbit around Earth. Scientists would use these satellites to collect and transmit data to study the weather, geology, the movement of the oceans, the arctic, and global warming.

////

2. The Department of Energy ("DOE") was a department of the United States responsible for, among other things, developing new scientific technologies to provide additional sources of energy. The DOE operated research facilities around the United States, each of which relied upon computer systems to operate, including the Lawrence Berkeley National Laboratory in Berkeley, California; the Sandia National Laboratory in Livermore, California; the Oak Ridge National Laboratory in Oak Ridge, Tennessee; and the Thomas Jefferson National Accelerator Facility in Newport News, Virginia.

3. The United States Navy was part of the Department of Defense of the United States. Among other facilities, the United States Navy operated the United States Naval Observatory, in Washington, DC; the Spawar Systems Center, in Suffolk, Virginia; and the Naval Research Laboratory, in Washington, DC. Each of these facilities relied upon computers in collecting, storing, and analyzing scientific data.

4. The computers and computer systems at the facilities described in paragraphs 1 through 3 above:

a. were exclusively for the use of the Government of the United States, and were used in interstate commerce and communication;

b. were restricted in use to authorized personnel, each of whom had to enter a "username" and "password" before accessing the computer system;

c. were programmed to monitor and record the username, password, date and time of any access to the computer

system; and

d. were also programmed to track the identity of the computer used to access the computer systems identified in paragraphs 1 through 3, usually by recording the Internet protocol address (or "IP address") of the computer from which those systems were accessed. (An "IP address" is a unique numerical address assigned to every computer using the Internet; because they are unique, knowing the IP address that a computer is assigned makes it possible to determine which computer was using that IP address at a particular time.)

5. Defendant FAUR, and others known and unknown to the Grand Jury, belonged to a group known as "WhiteHat Team." According to the group's Internet website, one of the professed purposes of the "WhiteHat Team" group was to gain unauthorized access to NASA and other United States government computers, despite its illegality, because NASA "has the reputation as being the most secure informatic system on the internet, along with other military and [U.S.] government sites."

II. OBJECTS OF THE CONSPIRACY

6. From on or about October 8, 2004, and continuing to on or about October 12, 2006, in Los Angeles County, within the Central District of California, and elsewhere, defendant VICTOR FAUR, also known as ("aka") "SirVic," "Victor," "Viktor," "VickTheTrick," "SirVictor," "VicMech," "VicGov," "VicOingo," and "VicNasa" ("FAUR"), and others known and unknown to the Grand Jury, conspired and agreed to commit offenses under Title 18, United States Code, Sections 1030(a)(5)(A)(i) and (a)(5)(B)(i),

namely, knowingly causing the transmission of a program, information, code and command, and intentionally causing damage without authorization to protected computers operated by NASA, the DOE, and the United States Navy, and causing these entities to suffer more than $5,000 loss in a one-year period; under Title 18, United States Code, Sections 1030(a)(2)(B) and (c)(2)(B)(ii), namely, intentionally and without authorization accessing computers operated by NASA, the DOE, and the United States Navy, and thereby obtaining information from those United States departments and agencies, thus furthering criminal acts in violation of the laws of the United States; and under Title 18, United States Code, Section 1030(a)(3), namely, intentionally and without authorization accessing a nonpublic computer exclusively used by NASA, the DOE, and the United States Navy.

III. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

7. The objects of the conspiracy were to be accomplished, in substance, as follows:

a. Defendant FAUR would obtain unauthorized access to a NASA, DOE or United States Navy computer using a computer program to cycle through millions of possible username and password combinations until one of them gained him access. (This method of gaining unauthorized access is also known as a "brute force attack."). Once accessed by FAUR or others, such computers were "compromised."

b. After defendant FAUR compromised a computer at NASA, the DOE, or the United States Navy by his unauthorized

access, he would intentionally impair the integrity and availability of data, information, and the programs and systems of that computer by causing it to execute various computer programs defendant FAUR transferred onto that computer. These programs would operate to grant him high-level access to that computer and would provide him with actual usernames and passwords of authorized computer system users contained within the system.

c. Using the usernames and passwords belonging to other users, defendant FAUR would obtain unauthorized access to other computers within the same system or in other government systems, using the internal connections between the computers in those systems.

d. As defendant FAUR obtained access to each additional computer within the system, he would intentionally impair the integrity and availability of data, information, and the programs and systems of that computer by causing it to download computer programs stored on various Internet websites he controlled. Those websites included, but were not limited to, www.sirvic.org, www.sirvic.biz, www.whitehat.cc, and www.sirvic.cc.

e. The computer programs defendant FAUR caused to be downloaded performed one or more of the following functions, and are known collectively as "hacker tools":

(i) programs called "root kits" would grant him high-level access to the entire computer;

(ii) programs called "local system exploits" would grant him mid-level access to particular user accounts on that computer (rather than to every user account on the computer, as a root kit would);

(iii) programs called "keystroke loggers" would record any keystrokes made on the computer, thereby enabling him to capture additional usernames and passwords once they were typed;

(iv) programs called "sniffers" would scour the computer's hard drive and memory for strings of characters that could be usernames and passwords;

(v) programs called "spoofers" would alter or conceal the true identity (as noted above, the IP address) of the computer, thereby making it easier to use the compromised computer to launch anonymous attacks on other computers; and

(vi) programs called "log cleaners" would erase the username, password, access date and time, and access IP address information otherwise automatically monitored and recorded for each NASA, DOE, and United States Navy computer.

f. Defendant FAUR would further intentionally impair the integrity and availability of data, information, and the programs and systems on the compromised computers operated by NASA, the DOE, and the United States Navy in one of several ways:

(i) Defendant FAUR would vandalize the compromised computer systems by causing those computers to display images and words indicating that the system had been "hacked," or compromised unlawfully.

(ii) Defendant FAUR would download computer programs onto the compromised computers that would enable these computers, unbeknownst to NASA, the DOE, or the United States Navy, to serve as hosts for online, real-time Internet conversations using Internet relay chat ("IRC"), which defendant and his co-conspirators would subsequently use to communicate with one another.

(iii) Defendant FAUR would download other computer programs onto the compromised computers that would scour the computers looking for possible usernames and passwords, and would mail that data to electronic mail ("e-mail") accounts that defendant FAUR controlled or otherwise accessed.

(iv) Defendant FAUR would set up e-mail accounts for himself on the compromised computers.

g. In undertaking the above-described means, defendant FAUR would make unauthorized access to compromised computers at NASA, the DOE, and the United States Navy, from his home computer either (A) directly from an Internet access account he controlled in Romania; or (B) indirectly by using a Romanian Internet account to access the compromised computers through (i) America Online ("AOL") accounts held by unknowing third parties that defendant accessed without authorization; (ii) computers defendant used to host Internet websites; or (iii) computers into which defendant had obtained unauthorized access at institutions of higher learning in the United States, such as Harvard University, Stanford University, University of California at Berkeley, and University of California San Diego.

8. By these means and as a result of the conduct described in paragraphs 6 and 7 above:

a. One hundred fourteen (114) computers at NASA facilities were compromised. NASA suffered approximately $1.366 million in losses, comprised in part of the cost to respond to the intrusions, to conduct damage assessments, and to restore the data, programs, systems, and information to its condition prior to the intrusions. The loss also included the consequential cost of loss of scientific data due to the necessity of considering data on compromised computers to be suspect and thus of no scientific value because of interruption of service and the danger of corrupted data.

b. Twenty-one (21) computers that were part of the DOE's computer system were compromised. The DOE suffered $55,421 in losses, comprised of the cost to respond to the intrusions, to conduct damage assessments, and to restore the data, programs, systems, and information to its condition prior to the intrusions.

c. Twenty (20) computers belonging to the United States Navy were compromised. The Navy suffered $38,850 in losses, comprised of the cost to respond to the intrusions, to conduct damage assessments, and to restore the data, programs, systems, and information to its condition prior to the intrusions.

IV. OVERT ACTS

9. In furtherance of the conspiracy and to accomplish the objects of the conspiracy, defendant FAUR and others committed

various overt acts within the Central District of California and elsewhere, including, but not limited to, the following:

E-Mail Accounts and Websites Controlled by Defendant FAUR

a. On or about April 8, 2003, defendant FAUR created an e-mail account with Yahoo!, which was filmenoidivx@yahoo.com, and listed a Hotmail account, filmenoidivx@hotmail.com, as an "alternative" e-mail contact for the filmenoidivx@yahoo.com e-mail account.

b. Between on or about February 14, 2006, and on or about June 9, 2006, defendant FAUR accessed the filmenoidivx@yahoo.com e-mail account.

c. Between on or about February 14, 2006, and on or about June 9, 2006, defendant FAUR used the filmenoidivx@yahoo.com e-mail account to correspond with the company hosting the www.sirvic.org website.

d. On or about November 24, 2004, defendant FAUR created an e-mail account with Yahoo!, which was vicafk@yahoo.com, and listed the same Hotmail account, filmenodoidivx@hotmail.com, as an "alternative" e-mail contact for the vicafk@yahoo.com e-mail account.

e. Between on or about April 2, 2006, and on or about October 9, 2006, defendant FAUR accessed the vicafk@yahoo.com e-mail account.

f. Between on or about April 2, 2006, and on or about October 9, 2006, defendant FAUR used the vicafk@yahoo.com e-mail account to send e-mail messages designed to "test" the mail systems on the computers used to host the websites www.sirvic.biz

and www.whitehat.cc.

g. Between on or about January 25, 2006, and on or about April 25, 2006, defendant FAUR accessed the website www.sirvic.biz.

h. Between on or about January 25, 2006, and on or about April 25, 2006, defendant FAUR stored various computer files used to facilitate computer intrusions on the computer hosting the www.sirvic.biz website, and those programs had the same file names and functions as portions of files discovered on compromised computers at NASA, the DOE, and the United States Navy.

i. Between on or about February 2, 2006, and on or about March 21, 2006, defendant FAUR accessed the website www.sirvic.org.

j. Between on or about February 2, 2006, and on or about March 21, 2006, defendant FAUR stored various computer files used to facilitate computer intrusions on the computer hosting the www.sirvic.org website, and those programs had the same file names and functions as portions of files discovered on compromised computers at NASA, the DOE, and the United States Navy.

k. Between on or about April 29, 2006, and on or about May 10, 2006, defendant FAUR accessed the website www.whitehat.cc.

l. Between on or about April 29, 2006, and on or about May 10, 2006, defendant FAUR stored various computer files used to facilitate computer intrusions on the computer hosting

the www.whitehat.cc website.

m. Between on or about September 22, 2004, and on or about May 9, 2006, defendant FAUR stored, in various computer files located on the computer hosting the www.whitehat.cc website, hundreds of snapshots of the images appearing on the computer screens (called "screen captures") of compromised computers at NASA, the DOE, and the United States Navy.

n. On or about April 15, 2006, defendant FAUR created an e-mail account with Yahoo!, which was nasarewt@yahoo.com.

o. Between on or about April 5, 2006, and on or about June 10, 2006, defendant FAUR used the nasarewt@yahoo.com e-mail account to receive e-mails -- sent from an e-mail account he created on compromised NASA computers -- containing usernames and passwords for those computers.

p. On or about April 5, 2006, defendant FAUR created an e-mail account with Google, which was nasarewt@gmail.com.

q. Between on or about April 5, 2006, and on or about June 8, 2006, defendant FAUR used the nasarewt@gmail.com e-mail account to receive e-mails -- sent from an e-mail account he created on compromised NASA computers -- containing usernames and passwords for those computers.

Unauthorized Intrusions at NASA's JPL Facility

r. On or about November 5, 2005, defendant FAUR accessed without authorization a computer at JPL, known as pluto.jpl.nasa.gov (IP address 137.78.73.111), and thereafter without authorization connected to newyork.jpl.nasa.gov (IP address 137.78.73.39) using a secure connection between those two

computers.

s. On or about November 5, 2005, defendant FAUR downloaded IRC software to newyork.jpl.nasa.gov and, from that computer, transmitted messages to other people using the IRC software while identifying himself as "SirVic."

t. On or about March 8, 2006, defendant FAUR accessed without authorization a computer located at JPL, known as hoopla.jpl.nasa.gov (IP address 137.78.15.72), and caused a root kit program to be downloaded onto that compromised computer.

u. On or about March 18, 2006, defendant FAUR accessed without authorization a computer located at JPL, known as rockymt.jpl.nasa.gov (IP address 137.78.73.46).

v. On or about March 18, 2006, defendant FAUR used his unauthorized access to the rockymt.jpl.nasa.gov computer (IP 137.78.73.46) to download a local system exploit and log cleaner program onto that computer from the website www.sirvic.org, and to alter the opening computer screen to read: "Since NASA is so lame in security lately, we decided to teach them a lesson."

w. On or about March 22, 2006, defendant FAUR accessed without authorization a computer at JPL known as cosmos.jpl.nasa.gov (IP 137.78.11.41), indirectly through unauthorized access to an AOL user account and unauthorized access to a computer located at Harvard University.

x. Between on or about April 5, 2006, and on or about June 9, 2006, defendant FAUR, through unauthorized access, caused a computer at JPL known as lilypad.jpl.nasa.gov (IP address 137.78.169.84) to transmit e-mail messages containing usernames

and passwords for JPL computers from SirVic@jpl.nasa.gov to e-mail addresses he controlled, nasarewt@yahoo.com and nasarewt@gmail.com.

Unauthorized Intrusions at NASA's Goddard Facility

y. On or about February 19, 2006, defendant FAUR accessed a computer at Goddard, known as oingo.gsfc.nasas.gov (IP address 128.183.105.227). Defendant FAUR then caused a computer program enabling IRC chat to be placed on that computer, and, using the nicknames "VicNasa" and "VicOingo," transmitted the following message in the IRC channel he was using: "USER SirVic... Look mommy, i work for nasa again! =)".

z. Between on or about April 4, 2006, and on or about April 13, 2006, defendant FAUR accessed without authorization a computer at Goddard known as istas1.gsfc.nasa.gov (IP address 128.183.166.5), indirectly through unauthorized access to several different AOL user accounts and unauthorized access to a computer located at Stanford University.

aa. Between on or about April 4, 2006, and on or about April 13, 2006, defendant FAUR caused the computer at Goddard known as istas1.gsfc.nasa.gov (IP address 128.183.166.5) to access websites he controlled, namely, www.sirvic.biz and www.whitehat.cc.

bb. On or about April 29, 2006, defendant FAUR accessed without authorization a computer at Goddard, known as roy.gsfc.nasa.gov (IP address 128.183.167.254).

cc. On or about April 29, 2006, defendant FAUR used his unauthorized access to the roy.gsfc.nasa.gov (IP address

128.183.167.254) computer to download and execute a root kit program, and to modify the opening computer screen to read as follows: "This system is *PRIVATE* property of the #WhiteHat Security Team." The banner listed the system administrator as "SirVic@SirVic.biz."

Unauthorized Intrusions at DOE Facilities

dd. On or about November 27, 2005, defendant FAUR accessed without authorization a computer at Lawrence Berkeley National Laboratory known as jacin03.nersc.gov (IP address 128.55.47.34), indirectly through unauthorized access to a computer located at University of California, Berkeley.

ee. On or about November 27, 2005, defendant FAUR used his unauthorized access to the jacin03.nersc.gov (IP address 128.55.47.34) computer to cause that computer to access the website www.sirvic.cc, and to download IRC software and hacker tools.

ff. On or about January 18, 2006, defendant FAUR accessed without authorization a computer at the Sandia National Laboratories known as nubar.ca.sandia.gov (IP address 146.246.227.32), indirectly through unauthorized access to a computer located at Harvard University.

gg. On or about January 18, 2006, defendant FAUR, through his unauthorized access to the nubar.ca.sandia.gov (IP address 146.246.227.32) computer, caused that computer to access the website www.sirvic.cc and download IRC software, and to transmit the following message on IRC channel #Whitehat: "Look mommy, I'm working for Sandia National Laboratories =)_".

hh. On or about July 20, 2006, defendant FAUR accessed without authorization a computer at Jefferson Laboratory, known as jlab8.jlab.org.

ii. On or about July 20, 2006, defendant FAUR, through his unauthorized access to the jlab8.jlab.org computer, caused that computer to access the website www.sirvic.biz and to download a file that contained various hacker tools, including tools that would enable a person to use secure connections between computers on the same computer system.

jj. On or about July 20, 2006, defendant FAUR, through authorized access to the jlab8.jlab.org computer, accessed without authorization another computer at Jefferson Laboratory, known as clonpc3.jlab.org.

kk. On or about July 20, 2006, defendant FAUR, through his unauthorized access to the clonpc3.jlab.org computer, caused that computer to access the website www.sirvic.biz and download IRC chat software and log cleaner programs.

Unauthorized Intrusions at Naval Facilities

ll. On or about March 29, 2006, defendant FAUR accessed without authorization a computer located at the United States Naval Observatory known as draco.usno.navy.mil (IP address 198.116.61.109).

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A)(i), (a)(5)(B)(i)]

On or about March 8, 2006, in Los Angeles County, within the Central District of California, ane elsewhere, defendant VICTOR FAUR, aka "SirVic," "Victor," "Viktor," "VickTheTrick," "SirVictor," "VicMech," "VicGov," "VicOingo," and "VicNasa," knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a computer, namely, the Jet Propulsion Laboratory computer known as hoopla.jpl.nasa.gov (IP address 137.78.15.72), which was exclusively for the use of the United States Government and which was used in interstate and foreign commerce and communication, and, as a result of such conduct, impaired the integrity and availability of data, a program, a system, and information that caused loss to one or more individuals during a one-year period beginning on or about March 8, 2006, and aggregating at least $5,000 in value.

COUNT THREE

[18 U.S.C. §§ 1030(a)(5)(A)(i), (a)(5)(B)(i)]

On or about March 18, 2006, in Los Angeles County, within the Central District of California, and elsewhere, defendant VICTOR FAUR, aka "SirVic," "Victor," "Viktor," "VickTheTrick," "SirVictor," "VicMech," "VicGov," "VicOingo," and "VicNasa," knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a computer, namely, the Jet Propulsion Laboratory computer known as rockymt.jpl.nasa.gov (IP address 137.78.73.46), which was exclusively for the use of the United States Government and which was used in interstate and foreign commerce and communication, and, as a result of such conduct, impaired the integrity and availability of data, a program, a system, and information that caused loss to one or more individuals during a one-year period beginning on or about March 18, 2006, and aggregating at least $5,000 in value.

COUNT FOUR

[18 U.S.C. §§ 1030(a)(5)(A)(i), (a)(5)(B)(i)]

On or about March 22, 2006, in Los Angeles County, within the Central District of California, and elsewhere, defendant VICTOR FAUR, aka "SirVic," "Victor," "Viktor," "VickTheTrick," "SirVictor," "VicMech," "VicGov," "VicOingo," and "VicNasa," knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a computer, namely, the Jet Propulsion Laboratory computer known as cosmos.jpl.nasa.gov (IP address 137.78.11.41), which was exclusively for the use of the United States Government and which was used in interstate and foreign commerce and communication, and, as a result of such conduct, impaired the integrity and availability of data, a program, a system, and information that caused loss to one or more individuals during a one-year period beginning on or about March 22, 2006, and aggregating at least $5,000 in value.

COUNT FIVE

[18 U.S.C. §§ 1030(a)(5)(A)(i), (a)(5)(B)(i)]

On or about May 4, 2006, in Los Angeles County, within the Central District of California, and elsewhere, defendant VICTOR FAUR, aka "SirVic," "Victor," "Viktor," "VickTheTrick," "SirVictor," "VicMech," "VicGov," "VicOingo," and "VicNasa," knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a computer, namely, the Jet Propulsion Laboratory computer known as lilypad.jpl.nasa.gov (IP address 137.78.169.84), which was exclusively for the use of the United States Government and which was used in interstate and foreign commerce and communication, and, as a result of such conduct, impaired the integrity and availability of data, a program, a system, and information that caused loss to one or more individuals during a one-year period beginning or about May 4, 2006, and aggregating at least $5,000 in value.

COUNT SIX

[18 U.S.C. §§ 1030(a)(2)(c), (c)(2)(B)(ii)]

On or about May 4, 2006, in Los Angeles County, within the Central District of California, and elsewhere, defendant VICTOR FAUR, aka "SirVic," "Victor," "Viktor," "VickTheTrick," "SirVictor," "VicMech," "VicGov," "VicOingo," and "VicNasa," intentionally accessed a computer, namely, the Jet Propulsion Laboratory computer known as lilypad.jpl.nasa.gov (IP address 137.78.169.84), which was exclusively for the use of the United States Government and which was used in interstate and foreign commerce and communication, and thereby obtained information, namely, usernames and passwords, from NASA, an agency or department of the United States, and committed this offense in furtherance of criminal acts in violation of the laws of the United States, namely, conspiracy to commit computer intrusion and computer intrusion, in violation of 18 U.S.C. § 371 and 18 U.S.C. §§ 1030(a)(5)(A)(I), (c)(5)(B)(i), respectively.

COUNTS SEVEN THROUGH TEN

[18 U.S.C. § 1030(a)(3)]

On or about the following dates, in Los Angeles County, within the Central District of California, and elsewhere, defendant VICTOR FAUR, aka "SirVic," "Victor," "Viktor," "VickTheTrick," "SirVictor," "VicMech," "VicGov," "VicOingo," and "VicNasa," intentionally and without authorization accessed the following non-public computers at the Jet Propulsion Laboratory, which is part of NASA and thus an agency of the United States, which computers were exclusively for the use of the Government of the United States:

COUNT	DATE	NON-PUBLIC COMPUTER ACCESSED
SEVEN	March 8, 2006	hoopla.jpl.nasa.gov (IP address 137.78.15.72)
EIGHT	March 18, 2006	rockymt.jpl.nasa.gov (IP address 137.78.73.46)
NINE	March 22, 2006	cosmos.jpl.nasa.gov (IP address 137.78.11.41)

////

////

////

////

////

////

////

COUNT	DATE	NON-PUBLIC COMPUTER ACCESSED
TEN	May 4, 2006	lilypad.jpl.nasa.gov (IP address 137.78.169.84)

A TRUE BILL

_____
Foreperson

GEORGE S. CARDONA
Acting United States Attorney

THOMAS P. O'BRIEN
Assistant United States Attorney
Chief, Criminal Division

BRIAN M. HOFFSTADT
ERIK M. SILBER
Assistant United States Attorneys
Cyber and Intellectual Property Crimes Section