**IN THE UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF DELAWARE**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA,** | ) | |
| | ) | |
| **Plaintiff,** | ) | |
| | ) | |
| **v.** | ) | **Criminal Action No. 10-112-LPS** |
| | ) | |
| **XIANG LI,** | ) | |
| | ) | |
| **Defendant.** | ) | |

**GOVERNMENT'S SENTENCING MEMORANDUM**

**INTRODUCTION**

Through online theft of intellectual property, the United States is being victimized by "the greatest transfer of wealth in history." *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013 Before Sen. Comm. on Armed Services*, 112th Cong. 3 (Mar. 27, 2012) (opening statement of Sen. Levin) (quoting statement of Gen. Keith Alexander, Commander, U.S. Cyber Command & Director, National Security Agency). The Internet has enabled digital thieves located across oceans and around the world to steal intellectual property and secrets with ease, without limit, in silence, and on a daily basis. The value of what is being stolen is staggering – reaching into the hundreds of billions of dollars each year. *See* Dennis C. Blair, Jon M. Huntsman, Jr., et al., *Report of the Commission on the Theft of American Intellectual Property* 11 (2013), http://ipcommission.org/report/IP_Commission_Report_052213.pdf.

Defendant is a citizen of China and one of these digital thieves. To the best of the undersigned's knowledge, Defendant is the first Chinese citizen to be apprehended and prosecuted in the United States for cybercrimes he engaged in entirely from China.

At the time of his June 2011 arrest on the Island of Saipan, Defendant lived in the city of Chengdu, which is located in the Sichuan province, in Southwest China. From Chengdu, Defendant operated a series of websites over three years that sold pirated, industrial-grade software in which the access controls had been "cracked," or circumvented. In particular, Defendant engaged in over 700 transactions through which he distributed over $100 million pirated software to over 400 customers located in at least 28 states and over 60 foreign countries. Defendant also sold confidential and proprietary information obtained from the internal computer network of at least one "cleared defense contractor," which is "a private entity granted clearance by the Department of Defense to access, receive or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense." *See* National Defense Authorization Act for Fiscal Year 2013, H.R. 4310, P.L. 112-239, § 941(e)(1).

Defendant sold stolen property worth millions for pennies on each dollar. The tightly controlled and very valuable software products that Defendant distributed into the wild of the Internet are industrial-grade, digital tools used to design myriad products essential to daily life, the health and safety of the public, and U.S. national security. Defendant's customers included those in embargoed countries in the Middle East and Government employees and contractors holding security clearances at home. One customer, a "Chief Scientist" for an American defense contractor, even used the cracked software to design a component for the radar system of the "Marine One" Presidential helicopter.

For the reasons set forth below, the United States respectfully recommends that the Court impose a sentence of 210 months of imprisonment, which is at the top of the advisory Guidelines range. Following his term of imprisonment, Defendant will be deported to China. The

Government respectfully recommends that Defendant be sentenced to a post-incarceration period of supervised release of 3 years, which will commence if Defendant ever re-enters the United States subsequent to the service of his prison sentence and deportation.

## I. APPLICATION OF SECTION 3553(a) FACTORS

### A. Nature and Circumstances of the Offenses

#### 1. Online Investigation of the Crack99 Software Piracy Operation

In December 2009, Homeland Security Investigations ("HSI") Special Agents began investigating a website located at www.crack99.com, which advertised over 2,000 software products used in numerous applications, including aerospace simulation and design, defense, electronics, energy, engineering, explosive simulation, intelligence gathering, manufacturing, mining, space exploration, mathematics, storm water management, explosive simulation, and manufacturing plant design. The advertised software was pirated or "cracked," meaning that the software's licensing system files and other access and copy control features had been disabled, granting anyone in possession of it unlimited and unauthorized access to the software. *See* Website Screen Capture (Ex. 1).

The HSI investigation uncovered one of the general processes by which international cybercriminals obtain, crack and distribute software via the Internet. First, cybercriminals obtain legitimate copies of the software by a variety of means, including: (1) hacking or otherwise unauthorized access into private computer networks; (2) free software demonstration or trial copies (which limit modules or duration of access through license files); (3) website downloads; (4) unauthorized release of beta versions of software; (5) rogue employees providing the software to them; and (6) unscrupulous foreign distributors of the software. Second, these software "crackers" loosely organize into "Fan Groups" and crack software by disabling the

access/dissemination controls. Third, the "Fan Groups," which operate mostly in China and Russia, make the hacked software available on web forums or other online portals. Fourth, other cybercriminals obtain the cracked software from forums, websites, file transfer protocol sites or other means. Fifth, these "middle men" operate websites that advertise the sale of cracked software products and distribute that software through the Internet. Sixth, the "middle men" generally specialize in, and guide customers through, the complex technical installation process. Without the "middle men," complex, industrial-grade software that has been cracked is often inoperable and non-transferable.

Defendant was the "middle man" operator of the Crack99.com website, as well as similar websites located at "www.cad100.net" and "www.dongle-crack-download.com" ("the Websites"). Communicating via the Internet from China prior to his arrest, Defendant described himself to one of his customers as a member of "an international organization created to crack [software]." Email of 2/3/09 (Ex. 2). When asked who cracked the software, Defendant responded to another customer: "Experts crack, Chinese people Sorry can not reveal more." Email of 11/29/08 (Ex. 3).

The agents determined that Defendant employed a four-step process to reproduce and distribute pirated software to the website customers. *See* Website Screen Capture, Ex. 1. First, the website instructed potential customers to transmit an email to Defendant at china9981@gmail.com requesting to purchase an advertised, pirated software product. Second, Defendant responded to the customers' email requests by providing a sales price for the requested software and by instructing them to transmit payment – generally by wire transfer – to him or to a co-conspirator located in China. Third, Defendant would acquire the cracked software from other members of the cybercrime organization or "Fan Groups." Fourth, after

receiving payment, Defendant would transmit an email, or series of emails, to the customer with downloadable files containing the pirated software or a hyperlink to a download server holding such files. Defendant used computer servers in the United States, China, Malaysia, and Amsterdam to store and distribute the cracked software. Alternatively, Defendant would mail disks containing the pirated software to the customer.

Defendant's role did not end with transmitting the cracked software to the website customers, and he was far from a simple mule or deliveryman. In many ways, Defendant's work was just beginning. Between February 2008 and June 2011, Defendant and his customers exchanged over 25,000 e-mails relating to pirated software. Because of the complex nature of the software and the licensing management systems designed to control access to and copying of it, the installation and operation of the cracked software was a highly technical and complicated process. Thousands of emails seized by the Government illustrate how Defendant served the critical function of guiding the Crack 99 customers through the installation and operation processes. Thus, Defendant made the software operable and transferable to anyone who possessed it. *See* "Crack 99 Operation" Demonstrative Chart (Ex. 4). Without Defendant's actions, the software would have remained inoperable and non-transferable.

Between April 2008 and June 2011, Defendant and his co-conspirators engaged in over 700 transactions through which they distributed pirated software to over 400 website customers located in at least 28 states and over 60 foreign countries. *See* List of Software Sold (Ex. 5).

Based on Defendant's electronic communications with website customers, there is no question that Defendant knew he was violating American intellectual property laws by selling the pirated software. First, Defendant clearly knew that he was selling unauthorized copies of the software. For example, one customer asked: "Can you please explain how your service can

provide this software for just 80 dollars? I am aware that the cost of Compusoft is much much more than this." Email of 4/19/10 (Ex. 6). Defendant responded: "this is cracked version software." *Id.* When another customer asked if the software he was buying from Defendant was "a complete version" and whether a "dongle [was] needed or included," and "what about updates," Defendant wrote: "this is cracked version . . . no need dongle . . . only the version no updates." Email of 2/11/10 (Ex. 7); Email of 8/23/09 (Ex. 8) (similar). Another customer questioned Defendant about the installation process, reporting that he was receiving a message that the access license would expire on "22 JAN 2010." Email of 1/8/10 (Ex. 9). Defendant explained that the software would remain operational beyond the "trial" period, because Defendant had altered the time limit set in the license file source code: "this is cracked versin! There is no limit you know?? you see? I edit the time . . . ." *Id.*

Not only did Defendant know that he was selling pirated software, he also sought to avoid law enforcement detection of his transactions and shipments. By transferring files via the Internet, Defendant sought to avoid U.S. Customs scrutiny that would come from mailing pirated software. In one email exchange, for example, a customer asked Defendant why he was reluctant to mail the customer a copy of the cracked software. Defendant answered: "Because the end of the strict customs checks. This is contraband." Email of 1/14/09 (Ex. 10). He also used file transfer protocol downloads of pirated software to avoid interception by U.S. Customs of mailed disks containing pirated software. See email of 7/21/08 (Ex. 11) ("Now CD-ROM by mail is illegal. Customs may be destroyed"). When another customer asked Defendant why he did not use PayPal to conduct the pirated software transactions, Defendant wrote: "Because PayPal prohibit the sale of cracked software." Email of 12/15/09 (Ex. 12).

Defendant continued to engage in this unlawful conduct even after victim companies demanded that he stop the infringement of their intellectual property rights. Defendant received various "cease and desist" demands from software manufacturers pursuant to the Digital Millennium Copyright Act. As one victim-company representative wrote:

> You are illegally selling an old version of TraumaCad on your website. You are ordered to cease and desist and to immediately remove the product from your website. Failure to comply will result in full prosecution through the United States Department of Justice, Computer Crime & Intellectual Property [Section].

Email of 4/6/10 (Ex. 13). Another victim-company likewise demanded that Defendant cease and desist from selling its software, adding:

> We had found that the software which Elgris Technologies has all legal rights for (E-Tools E-Studio Pro 4.42) is offered on your Web site for $100. Elgris Technologies is getting no compensation for the product sales and intend to defend its software IP (intellectual property) by contacting all appropriate USA and China authorities.

Email of 3/5/09 (Ex. 14).

**2. Online Undercover Purchases of Pirated Software from Defendant**

Between January 2010 and June 2011, undercover law enforcement agents made a series of purchases of pirated software advertised on Defendant's website. The agents accessed the website, located at http://www.crack99.com, from computers connected to the Internet from locations in Delaware and Pennsylvania. The agents corresponded by email with Defendant about their purchases. They negotiated prices for each article of pirated software with Defendant. They received from Defendant electronic files containing the pirated software or hyperlinks that enabled them to download the pirated software from computer servers located in the United States. They also received instructions from Defendant on how to install the pirated software. At Defendant's direction, the agents transmitted a series of wire transfers totaling

$8,615 from a Western Union location in Delaware to Defendant and a co-conspirator located in Chengdu, China, as payment for over $1 million worth of software they purchased.

Beginning in December 2010, undercover agents and Defendant began to formulate a plan in which the agents would resell copies of pirated software provided by Defendant to small businesses in the United States. On January 4, 2011, an undercover agent transmitted an email to Defendant seeking to purchase copies of fifteen cracked software products. Defendant agreed to supply the requested pirated software products for $1,467. Defendant also offered to design counterfeit packaging for the fifteen software programs for an additional price of $1,500.

Defendant also informed the undercover agent that he had "More pleasant surprises." In particular, Defendant stated that he had approximately twenty gigabytes of valuable internal data obtained from the computer network of an American company that designed software for military and intelligence applications. Defendant offered to sell this internal data to the undercover agents for an additional $3,000.

On January 11, 2011, an undercover agent transmitted an email to Defendant requesting a sample of the counterfeit design packaging he offered to produce. Defendant sent an email to the undercover agent with an attached image file showing a disc bearing the counterfeit label of an Ansys software product. Defendant stated in this email: "All included CD printing, design, and exquisite box. Color graphic design… Your customers satisfied with your decision." *See* Email of 1/11/11 (Ex. 14A).

On January 20, 2011, an undercover agent transmitted a Western Union wire transfer in the amount of $4,350 from a location in Claymont, Delaware to Defendant's co-conspirator in Chengdu, China as payment for the design packaging for the previously ordered fifteen software programs and the twenty gigabytes of proprietary data from an American software company, a

"cleared defense contractor." On February 1, 2011, the undercover agents received a mail package that contained six DVDs. Each contained numerous files, including the fifteen software programs the undercover agents had ordered from Defendants. Defendant informed the undercover agents that he would provide the twenty gigabytes of proprietary data from the American software company in the near future.

**3. Defendant's Arrest in Saipan Following Delivery of Digital Contraband**

Through various email messages and Skype transmissions, HSI agents convinced Defendant that they were U.S.-based counterfeiters who could resell cracked software and counterfeit labeling Defendant would supply at a much higher price than Defendant had been charging through the Crack 99 website. Defendant arranged to travel from Chengdu, China to the Island of Saipan in June 2011 to meet with the undercover agents. At the meeting, Defendant was to transfer the pirated software, design packaging and twenty gigabytes of proprietary data paid for by the undercover agent in January 2011. Defendant and the undercover agents also were to discuss their plan for Defendant to transmit pirated software and related counterfeit packaging and labeling to the undercover agents via the Internet, which the undercover agents would assemble and resell to small businesses in the United States.

On June 6, 2011, Defendant flew from China to Saipan to meet with the undercover agents. On June 7, 2011, Defendant met with undercover agents at a hotel in Saipan. During this recorded meeting, Defendant delivered to the undercover agents DVDs containing cracked versions of the fifteen software products ordered by the agents, as well as cracked versions of "Satellite Took Kit" 6.1.3, 8.1, and 9.2.1 software and various add-on software modules, installation programs and cracked license files associated with the software products. *See* Video of Undercover Meeting (Ex. 15); Still Image of Defendant Delivering Software (Ex. 16).

Defendant also delivered multiple computer disks with counterfeit packaging and product labeling indicating that they contained various software products, including:

a. Ansys 13.0
b. NI Labview
c. Agilent EMPro
d. Ansoft Nexxim
e. Antenna Magus
f. CST Studio Suite
g. Matlab
h. Ansoft Designer
i. Vector Works
j. Hyper Works
k. Pronest
l. Ansoft Maxwell
m. Ansoft HFSS
n. Mastercam
o. Catia V5R20
p. Ansoft Simplorer

See Images of Counterfeit Disks (Exs. 17-31). Defendant also provided the agents with disks containing approximately twenty gigabytes of proprietary data unlawfully obtained from the internal computer network of an American software company, a "cleared defense contractor."

As noted above, Defendant's electronic communications made clear that Defendant knew he was violating American intellectual property laws by selling the pirated software and counterfeit labeling and packaging. Defendant's actions and statements during the recorded undercover meeting not only underscore his criminal intent, but they also illustrate an attitude of complete disregard for American law. *See* Video of Undercover Meeting, Ex. 15. During the meeting, Defendant explained that the agents would have no problems with U.S. Customs if they separated the disks containing the pirated software from the counterfeit labeling and packaging Defendant had just delivered to them. *See id.* Clip 1. Defendant instructed the agents to tell any Customs agent who questioned them about the software that it was being used only for study

purposes, and Defendant assured one agent that he would not "end up in handcuffs" if he did so. *See id.* Clip 2.

Defendant's attitude and interaction with the agents also illustrates how ineffectual civil remedies are in combating online intellectual property theft by international cybercriminals. As noted above, Defendant had received various "cease and desist" demands from software manufacturers pursuant to the Digital Millennium Copyright Act. When asked about receiving such notices, Defendant responded that he simply ignored and deleted them. *See id.* Clip 3.

At the conclusion of the meeting, Defendant was arrested by federal law enforcement agents, and the items that he brought with him to the meeting were seized. During a search of Defendant's hotel room, agents seized various pieces of computer equipment, including digital storage devices and a laptop computer. Defendant was flown from Saipan to the District of Delaware for prosecution.

A forensic analysis of the computer equipment and removable digital media seized from Defendant confirmed that it contained pirated copies of the software ordered by the undercover agents and counterfeit packaging and documentation for such software. Defendant's equipment also contained scores of other cracked software programs, installation and operational data relating to the programs and data files associated with the operation of the Crack99.com website.

The forensic analysis also confirmed that Defendant had, in fact, delivered six disks containing approximately twenty gigabytes of proprietary data exfiltrated from an internal file transfer protocol site of an American software company that was a "cleared defense contractor." This data included: the software license server; training and "flash videos" used to teach users how to operate the software; mapping data files including 3-dimensional imagery files; military and civilian aircraft image models; a software module containing data associated with the

International Space Station; a complete listing of all of the software modules created by the company, as well as the 3-dimensional graphic images associated with these modules; a high resolution, 3-dimensional imaging program; various training courses under a folder called "Programmers Workshop;" and various other files including PDF and power point files associated with the software. The disks even contained music files uploaded by the company's employees to the internal server and then stolen by hackers.

**4. Pirating of Industrial-Grade Software**

The software sold by Defendant has a broad range of applications, including aerospace simulation and design, defense, electronic design automation, energy, engineering, explosive simulation, intelligence gathering, manufacturing, mining, space exploration, mathematics, storm water management, telecommunications design, and manufacturing plant design. These products are far different from the type of consumer entertainment products (like a movie or music file) often digitally pirated for the enjoyment of the passive consumer. Instead, these are industrial grade, digital engineering tools used to design myriad products essential to daily life, the health and safety of the public, and U.S. national security.

The software purchased by the undercover agents is illustrative of the types of industrial grade and sensitive software sold by Defendant. In January 2010, for instance, undercover agents purchased a pirated copy of "Satellite Tool Kit 8.0" ("STK"), which is designed to assist the military, aerospace, and intelligence industries through scenario-based modules that simulate real-world situations, such as missile launches, warfare simulations on land, sea, and air, flight trajectories, and the simultaneous monitoring of numerous assets in different theaters of war. It is designed and manufactured by Analytical Graphics, Inc., a 250-employee company located in Exton, Pennsylvania. Defendant charged the agents $1,000 for software worth more than

$150,000. Agents later bought an updated version of STK 9.2.1 from Defendant for $2,000. This updated version was worth over $240,000, and Defendant was selling a cracked version of it within weeks of its commercial release.

STK is a very valuable and critical tool for aerospace, military and intelligence simulation. According to STK marketing materials, the software is used for aircraft and unmanned aerial vehicle ("UAV") systems; communications and electronic warfare; geospatial intelligence; missile defense; navigation; range safety; space exploration; space superiority; and spacecraft mission design and operations. *See* STK Marketing Brochure (Ex. 32). For example, this software is central to improved decision support in military and intelligence operations, aiding such decision making as "which sensor to task for an unplanned target, where to direct forces while ensuring communications connectivity, and how to place airborne surveillance assets while avoiding enemy radar." *See* "Dynamic Analysis Software" Marketing Brochure (Ex. 33).

We have attached a video that explains the various military and intelligence uses of STK. *See* AGI Marketing Video (Ex. 34). The video discusses how STK allows the military to engage in "battlespace management" by creating "the ability to fuse geospatial intelligence with real-time operations to provide decision-makers with the opportunity to comprehensively understand the activities of friendly, hostile and neutral forces." The software supports the mission planning, real-time operations, and post-mission analysis necessary to maintain decision superiority" in battlespace. *See id.*; *see also* Video of STK Simulation of Intercontinental Missile Defense System (Ex. 34).

There is little reason why any person or entity outside of the military and intelligence sectors would use, or even possess, this software for any lawful purpose. There are two possible

scenarios by which Defendant came into possession of this software and related data, either of which is extremely serious and disconcerting. First, based on statements he made to customers prior to his arrest, Defendant might have acquired this software and related data as a member of a large international cybercrime organization. Second, based on his post-arrest statements to the probation officer, such software and data may be available to any average, ordinary Chinese intellectual property thief with an Internet connection, and that stealing such sensitive software is "fine and normal" and "prevalent" in Chinese culture. *See* PSR ¶ 55. Reasonable minds may differ as to which scenario raises greater concern for the United States Government and American companies victimized by Chinese cyber-theft.

In February 2010, undercover agents purchased a pirated copy of "Quartus II Nios Embedded Suite v9.0," "Quartus II v9.0 FPGA Full Working," and "Quartus II DSP Builder 9.0" from Defendant via the Internet. These software products, which were manufactured by Altera Corporation, are used in reprogrammable logic design to address a range of concerns -- from power consumption to performance to cost. Customers use Quartus in a wide variety of industries, including automotive, broadcast, computer and storage, consumer, industrial, medical, military, test and measurement, wireless, and wireline. The agents paid Defendant $340 for Altera software products worth over $10,000.

In March 2010, undercover agents purchased pirated copies of "HyperSizer v.5.3.29" and "HyperSizer v.5.3" from Defendant via the Internet. These two software products were designed and produced by Collier Research and Development Corporation, a small, family-owned software company in Virginia. The HyperSizer software assists in the weight reduction, structural design and stress analysis of the composite materials used in the construction of aircraft and spacecraft. The estimated retail value of the HyperSizer product is approximately

$50,000. Defendant sold it to the agents for $200.

Another product that undercover agents purchased from Defendant was "CST Studio Suite." This electromagnetic simulation software "is the culmination of many years of research and development into the most accurate and efficient computational solutions for electromagnetic designs." CST Website (Ex. 35). It includes CST Microwave Studio, which is "the leading edge tool for the fast and accurate 3D simulation of high frequency devices and market leader in Time Domain simulation. It enables the fast and accurate analysis of antennas, filters, couplers, planar and multi-layer structures and SI and EMC effects etc." *Id.* It also includes CST EM Studio, which is a "tool for the design and analysis of static and low frequency EM applications such as motors, sensors, actuators, transformers, and shielding enclosures." *Id.* CST Particle Studio "has been developed for the fully consistent simulation of free moving charged particles. Applications include electron guns, cathode ray tubes, magnetrons, and wake fields." *Id.*

Defendant also distributed leading products manufactured by Ansys, Inc., a company that develops and globally markets engineering simulation software and services widely used by engineers, designers, researchers and students across a broad spectrum of industries and academia, including aerospace, automotive, manufacturing, electronics, biomedical, energy and defense. For instance, Defendant sold Ansys's Multiphysics, a product suite that:

> . . . allows engineers and designers to create virtual prototypes of their designs operating under real-world multiphysics conditions. As the range of need for simulation expands, companies must be able to accurately predict how complex products will behave in real-world environments, where multiple types of coupled physics interact. ANSYS multiphysics software enables engineers and scientists to simulate the interactions between structural mechanics, heat transfer, fluid flow and electromagnetics all within a single, unified engineering simulation environment. . . .

Ansys Website (Ex. 36); Video Simulation of World Trade Center Attack Using Ansys Technology, CD, Ex. 34. Defendant also sold a cracked copy of "HFSS," which is:

> … the industry-standard simulation tool for 3-D full-wave electromagnetic field simulation and is essential for the design of high-frequency and high-speed component design. HFSS offers multiple state-of the-art solver technologies based on either the proven finite element method or the well-established integral equation method. You can select the appropriate solver for the type of simulation you are performing.
> . . . .
>
> Engineers rely on the accuracy, capacity, and performance of HFSS to design high-speed components including on-chip embedded passives, IC packages, PCB interconnects and high-frequency components such as antennas, RF/microwave components and biomedical devices. With HFSS, engineers can extract scattering matrix parameters (S,Y, Z parameters), visualize 3-D electromagnetic fields (near- and far-field) and generate ANSYS Full-Wave SPICE models that link to circuit simulations. Signal integrity engineers use HFSS within established EDA design flows to evaluate signal quality, including transmission path losses, reflection loss due to impedance mismatches, parasitic coupling and radiation.

Ansys Website, Ex. 36, at 3.

Another very valuable product that Defendant distributed was "Advanced Design System" (ADS), which is manufactured by Agilent Technologies. Agilent describes ADS as:

> … the world's leading electronic design automation software for RF, microwave, and high speed digital applications. In a powerful and easy-to-use interface, ADS pioneers the most innovative and commercially successful technologies, such as X-parameters and 3D EM simulators, used by leading companies in the wireless communication & networking and aerospace & defense industries. For WiMAX™, LTE, multi-gigabit per second data links, radar, & satellite applications, ADS provides full, standards-based design and verification with Wireless Libraries and circuit-system-EM co-simulation in an integrated platform.

Agilent Webpage (Ex. 37).

Based on the foregoing facts, the Probation Officer included a 3-level, "Aggravating Role" enhancement under Guidelines Section 3B1.1(b). *See* PSR ¶¶ 67, 75. Defendant's

objection to the application of that enhancement should be overruled. Under Section 3B1.1(b), a 3-level enhancement applies where the defendant "was a manager or supervisor (but not an organizer or leader) and the criminal activity involved five or more participants or was otherwise extensive." U.S. Sentencing Guidelines Manual § 3B1.1(b). Defendant concedes that his criminal activity was "otherwise extensive," and the facts summarized above establish that extensiveness beyond any doubt. Defendant asserts, though, that he was not a "manager or supervisor." That assertion is factually baseless and should be rejected.

As noted above, well before his arrest, Defendant described himself to numerous sources as a member of a much larger "international organization created to crack [software]." Email of 2/3/09, Ex. 2. In another email, Defendant explained that he did not actually crack the software license files; "Experts crack, Chinese people Sorry can not reveal more." Email of 11/29/08, Ex. 3. In a May 2009 email, Defendant stated: "I need to use your money to seek the help of experts to cracker master I earn 10% of the profits." Through hundreds of transactions and tens of thousands of emails, Defendant served the critical role of "middle man" – operating the Crack99.com website; acquiring from Fan Groups the cracked software requested by customers; negotiating the details of each transaction; collecting payment; distributing the cracked software; and aiding the customers in the installation and operation processes. As such, Defendant was a quintessential "manager or supervisor" within this international cybercrime organization.[1]

[1] Even if the Court were to decline to apply an "Aggravating Role" enhancement under Section 3B1.1(b), an upward departure of 3 levels would be warranted because Defendant "exercised management responsibility over the property, assets, or activities of the criminal organization." U.S. Sentencing Guidelines Manual § 3B1.1 App. Note 2.

**5. Distributing Over $100 Million Worth of Stolen Software Around the World**

The software that Defendant stole, distributed and helped his criminal customers install and operate was worth well over $100 million. As noted above, Defendant engaged in over 700 transactions through which he sold pirated software and data during the 3-year period of the conspiracy. The Government has not calculated the value of all of the pirated software sold by Defendant. Doing so would produce a number that would be at the top of -- if not off of -- the Section 2B1.1 table used to establish the applicable Guidelines enhancement. Simply put, we stopped counting once we exceeded a value of $100 million.

Below are two charts that illustrate how we calculated the value as exceeding $100 million. The first chart below represents a sampling of 144 out of over 700 transactions in which Defendant sold pirated software to customers (not including the undercover agents) prior to his June 2011 arrest in Saipan. Based on this sampling alone, the value of the software sold in these 144 transactions equaled $97,312,961.40.

| **Software** | **Number of Sales** | **Individual Price** | **Total** |
|---|---|---|---|
| Mastercam | 15 | $68,500 | $1,027,500.00 |
| Siemens Unigraphics NX | 25 | $250,000 | $6,250,000.00 |
| Oracle | 11 | $30,000 | $330,000 |
| NI Labview | 19 | $8,600 | $163,400.00 |
| Ansys HFSS | 15 | $50,660 | $759,900.00 |
| Catia | 20 | $3,812,241.57 | $76,244,831.40 |
| Agilent ADS | 15 | $823,022.00 | $12,345,330.00 |
| Solid Works | 24 | $8,000 | $192,000.00 |
| **Total** | **144** | **N/A** | **$97,312,961.40** |

The second chart below illustrates the value of the pirated software that Defendant delivered to the undercover agents in Saipan. This chart does not include the many other software products that Defendant sold to the undercover agents via the Internet prior to the June 2011 undercover meeting. It also does not include prices for each of the software programs Defendant delivered to the agents in Saipan. The value of just the listed software delivered by Defendant in Saipan equaled $5,040,504.57.

| **Software** | **Number of Sales** | **Individual Price** |
|---|---|---|
| Mastercam | 1 | $68,500.00 |
| Ansys 13.0 (includes several modules) | 1 | $338,055.00 |
| Agilent EmPro | 1 | $135,703.00 |
| NI Labview | 1 | $8,600.00 |
| Ansys HFSS | 1 | $50,660.00 |
| Catia | 1 | $3,812,241.57 |
| Ansoft Nexxim | 1 | $95,210.00 |
| Antenna Magnus | 1 | X |
| CST Studio Suite | 1 | X |
| Matlab | 1 | X |
| Ansoft Designer | 1 | $42,375.00 |
| Vector Works | 1 | X |
| Hyper Works | 1 | X |
| Pronest | 1 | X |
| Ansoft Maxwell | 1 | $15,435.00 |
| STK 6.1.3 | 1 | $150,000.00 |
| STK 8.1 | 1 | $150,000.00 |
| STK 9.1 | 1 | $150,000.00 |
| Ansoft Simplorer | 1 | $23,725.00 |
| | | |
| **Total** | | **$5,040,504.57** |

When the values from these two charts are added together, the total value of the stolen software sampled in these charts and distributed by Defendant equals $102,353,465.97. Defendant has no factual basis to dispute that this figure represents the retail value of the stolen software, as provided to the Government by the software manufacturers.

The Probation Office correctly looked to the retail value of the software in determining that at least a 24-level enhancement should be applied under Section 2B5.3(b)(1) based on a conservative calculation of the "infringement amount" as between $50 million and $100 million.[2] As explained in Application Note 2(A) to Section 2B5.3:

> The infringement amount is the retail value of the infringed item, multiplied by the number of infringing items, in a case involving any of the following:
>
> (i) The infringing item (I) is, or appears to a reasonably informed purchaser to be, identical or substantially equivalent to the infringed item; or (II) is a digital or electronic reproduction of the infringed item;
>
> . . . .
>
> (iii) The retail value of the infringing item is difficult or impossible to determine without unduly complicating or prolonging the sentencing proceeding;
>
> . . . .
>
> (v) the retail value of the infringed item provides a more accurate assessment of the pecuniary harm to the copyright or trademark owner than does the retail value of the infringing item.

Although the application of any one of these is sufficient, Sections 2(A)(i), (iii) and (v) each apply to this case and require the use of the retail value of the "infringed item." Subsection (i) applies because the pirated software is a digital and electronic reproduction of the copyrighted software and because the manufacturers of the software samples purchased by the government from the website confirmed that the purchased software was authentic. Subsection (iii) applies

---

[2] Because the "infringement amount" actually exceeds $100 million, Section 2B5.3(b)(1) and 2B1.1(b)(1)(N) call for application of a 26-level enhancement. To avoid the need for a protracted hearing aimed at totaling the value of hundreds of different stolen software programs, the Government does not object to the Court's application of the 24-level enhancement, instead of the 26-level enhancement.

because proving the retail value of over 550 different copyrighted software titles owned by approximately 200 different manufacturers would substantially prolong the sentencing hearing. Subsection (v) applies because the retail value of the actual software is what the manufacturers would have reasonably received if Defendant's customers had lawfully purchased the software.

Defendant claims that he sold the software for much less than its retail value. Based on very limited transactional data the United States was able to obtain from certain U.S.-based payment remitters, the Government confirmed that Defendant obtained proceeds in excess of $60,000 from the sale of pirated software. Importantly, this figure does not include any payments that Defendant received from foreign-based payment processors.

Defendant asks this Court to ignore the value of the stolen software and to base his sentence only on the amount of money he gained from selling the software. For the reasons noted above, doing so would be legally erroneous. Such an approach also ignores the harm suffered by the victims of the digital looting in which Defendant and his co-conspirators engaged. The absurdity of Defendant's position is made clear by a simple hypothetical. Suppose it were possible for Defendant to use the Internet to enter the Smithsonian Museum of Natural History and steal the Hope Diamond. As of 2011, the Hope Diamond was reportedly insured for $250 million. Suppose further that Defendant then sold the Hope Diamond on the Crack99 website for $25. It is doubtful that any fair-minded person would characterize Defendant's hypothetical crime as a $25 theft of a rock. Defendant's theft of over $100 million worth of software also should not be trivialized.

**6. Distributing Pirated Software to Global Customers Working in Sensitive Positions or on Sensitive Products**

Defendant sold cracked software to over 400 customers located in at least 28 states and 60 foreign countries. *See* Chart of Customer Countries (Ex. 38). Defendant's customers included foreign governments, U.S. Government employees, defense contractors, engineers, small businesses and individuals located in embargoed countries.

Defendant's operation served as a way for those in embargoed countries to obtain software they could not lawfully purchase. In February 2010, for example, a Syrian national emailed a U.S. software company seeking a quote on an electronic design automation software product valued at approximately $24,000. The U.S. software company informed the Syrian national that U.S. law prohibited it from selling this software to those in Syria. The Syrian national then emailed Defendant, who transmitted the cracked software product to the Syrian national in Syria, after Defendant received a wire transfer of $185 from Syria.

Some of Defendant's biggest customers were Americans who held significant engineering positions, and security clearances, with government agencies and government contractors. For instance, Defendant sold and transmitted via the Internet 12 cracked software programs to Cosburn Wedderburn, who was then a NASA electronics engineer, working at NASA's Goddard Space Flight Center, in Greenbelt, Maryland. Between September 2008 and November 2010, Wedderburn exchanged multiple e-mails with Defendant to obtain pirated software programs with an estimated retail value exceeding $1.2 million. These software programs have a broad range of applications including electric engineering, aerospace, telecommunications design and electronic design automation. Wedderburn used the cracked software for consulting jobs involving electronic and aerospace simulations. Wedderburn also

conducted a thermal simulation contract for China-based Huawei Technologies, Ltd. using the cracked software. Wedderburn also uploaded the cracked software he purchased from Defendant onto a NASA computer network, potentially exposing that network to malware and viruses located on the cracked software.

Also by way of example, Defendant sold and transmitted via the Internet 10 cracked software programs to Dr. Wronald Best, the "Chief Scientist" at a Kentucky-based government contractor that services the U.S. and foreign militaries and law enforcement with a variety of applications such as radio transmissions, radar usage, microwave technology, and vacuum tubes used in military helicopters. Between November 2008 and June 2009, Dr. Best exchanged over 260 e-mails with Defendant to obtain 10 pirated software programs. The estimated retail value of the 10 pirated software programs Dr. Best received from Defendant exceeds $600,000.

Dr. Best used this cracked software to design components used in military helicopters (including the Blackhawk helicopters), Patriot missiles, police radars and breathalyzer equipment used by the many police departments in the United States. Most appalling, though, was Dr. Best's use of cracked software to design a component used in the weather radar system employed in the Presidential helicopter fleet – "Marine One."

### B. Seriousness of Offenses, Promotion of Respect for the Law, Provision of Just Punishment, and Deterrence

#### 1. The Importance of Intellectual Property to the American Economy and the Gravity of the Threat Posed by Intellectual Property Theft

Intellectual property has become the keystone of the American economy. As a 2012 report issued by the United States Department of Commerce noted, "Innovation—the process through which new ideas are generated and successfully introduced in the marketplace—is a primary driver of U.S. economic growth and national competitiveness. . . . The granting and

protection of intellectual property rights is vital to promoting innovation and creativity and is an essential element of our free-enterprise, market-based system." U.S. Dep't of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," v (March 2012) http://www.esa.doc.gov/sites/default/files/reports/documents/ipandtheuseconomyindustriesinfocus.pdf ("DOC Report). Without the protection of intellectual property laws, the creators of intellectual property lose the economic benefits of their work, undermining incentives to invest in the development of products that have become essential to our daily lives. *See id.* These creators also are placed at a disadvantage vis-à-vis those who can just copy and use a product developed by others without incurring any of the costs associated with developing that product.

Defendant's criminal operation illustrates the point perfectly. Companies that spent millions of dollars to develop very sophisticated, industrial-grade software had it stolen by international cybercriminals, sometimes within days or weeks of its release. These international pirates, in turn, sold cracked copies of the software to: (1) those who cannot lawfully purchase it; (2) foreign governments that chose not to attempt to purchase it lawfully; and (3) businesses and individuals who used it to design and manufacture products provided to governments, businesses and consumers. The international cybercriminals and their customers profited at the expense of the software creators and those who use goods made with compromised digital tools.

As part of the Prioritizing Resources and Organization from Intellectual Property Act of 2008 (PRO-IP Act), Congress directed the executive branch to conduct an analysis of the threat posed by intellectual property rights violations, including the costs to the United States economy and threats to health, safety and national security. In November 2011, the National Intellectual Property Rights Coordination Center, an inter-agency task force established and led by the United States Department of Homeland Security, Homeland Security Investigations, published a

global analysis of the IPR threat to the United States. *See* National Intellectual Property Rights Coordination Center, "Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad," (Nov. 2011), http://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/view ("IPR Report").

The IPR Report concluded that Internet-facilitated, intellectual property theft has become one of the most serious criminal and economic problems facing our country. Intellectual property theft negatively affects the economic health of rights holders through lost profits, brand dilution, and enforcement costs. It has a similar negative effect on our national economy through the loss of jobs, tax revenue and customs receipts. The Department of Commerce has identified 75 "IP-intensive" industries that account for 40 million jobs, or 27.7 percent of all jobs, in the United States. *See* IPR Report, at vii. The same report noted that "IP-intensive industries accounted for about $5.06 trillion in value added, or 34.8 percent of U.S. gross domestic product, in 2010." *Id.*

Pirated software is especially pernicious because it is so easily reproduced and disseminated in the relative anonymity of the Internet. Online piracy is also an area of explosive growth in the consumption of counterfeit goods by American consumers. The IPR Report estimates that online piracy "currently accounts for between 6.5 and 12 percent of the total value of infringing goods" and estimates the value of online piracy as possibly reaching $240 billion by 2015. *See* IPR Report, at 18. Another report estimated China's illegal software market as reaching $9 billion in 2011, out of a total market of nearly $12 billion, thus setting a piracy rate of 77 percent. *See* Business Software Alliance, "Shadow Market: 2011 BSA Global Software Piracy Study," at 6 May 2012,

http://portal.bas.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-

Standard.pdf. The largest market for pirated software, though, was the United States, with a commercial value of pirated software approaching $10 billion. *See id.* at 6.

Pirated software is also particularly dangerous because it often is accompanied by malware or viruses that can compromise the integrity and security of data stored or accessed through computers or networks on which the pirated software is installed. This, in turn, can lead to massive identity theft, financial fraud, cyber-espionage and other criminal conduct. As Defendant's conduct so amply demonstrates, the Internet has fueled these threats, giving criminals increased access to an bottomless victim pool, facilitating deception as to the nature of the products supplied, and altering the ways in which counterfeit goods are moved to consumers.

Online intellectual property theft also poses a significant danger to public health and safety. The use of pirated software that may not function properly in the design of equipment and other goods used by the military, law enforcement agencies and other entities in critical infrastructure creates a risk of significant physical injury. It also undermines the national security of the United States and provides a funding source for international criminal and terrorist organizations. There also is an ever-increasing threat to national security from system failures or breaches of sensitive systems through back doors opened by pirated software or counterfeit components.

A marketing video created and used by Ansys, Inc., one of the victim companies, illustrates some of these concerns. *See* Ansys Video "Realize-Product-Promise," CD, Ex. 34. The narrator in the video explains why Ansys's software is so essential to producing safe, reliable products for use by governments, businesses, and consumers. After showing video of a cell phone, a jet engine, a motorcycle, wind turbines, and a child safety seat, the narrator explains:

> These products that protect our everyday lives . . . are promises, to your customers, to your shareholders, your colleagues, and to yourself, that the product you envisioned is the product you delivered, that there have been no compromises, that every what-if question, every idea and possibility about what each product can be and the promise it holds has been asked and answered with absolute and total confidence . . . .

*Id.*

**2. The Need to Promote International Respect for U.S. Law, to Punish International Intellectual Property Theft and to Deter Defendant and Other International Cybercriminals**

This case is unique in many ways. As far as the undersigned can tell and judging by the value of the intellectual property stolen, it is the largest criminal copyright infringement case brought to sentencing by the United States. It is the first criminal intellectual property case resulting in the conviction of a Chinese cybercriminal for crimes committed entirely from China. It is the first instance we know of where sensitive data from the internal computer network of a "cleared defense contractor" has been hand-delivered back to U.S. law enforcement by a Chinese cybercriminal after being stolen from the American company's computer network.

Perhaps most importantly, it may be the first case where a Chinese cybercriminal has sought a short sentence from an American court by claiming that cyber-theft of American intellectual property is culturally acceptable in China. As Defendant told the probation officer: " I was learning about computer software. There were forums online. Many people were interested in acquiring certain software, and many people put it online for free. In Chinese culture, sometimes this is 'fine and normal' and sometimes people don't look at it as a violation." PSR ¶ 55. Defendant went on to explain that cyber-theft is "prevalent" in China, opining that "[p]robably ten million people in China are doing things illegally with software." *Id.*

There is much reason to accept, as accurate, Defendant's assertions that the digital looting of American companies through cyber-theft has achieved some level of acceptability in China. Recent months have brought widespread news reports of rampant cyber-theft and economic espionage emanating from China. As a NEW YORK TIMES article published days ago reported:

> The culture of hacking in China is not confined to top-secret military compounds where hackers carry out orders to pilfer data from foreign governments and corporations. Hacking thrives across official, corporate and criminal worlds. Whether it is used to break into private networks, track online dissent back to its course or to steal trade secrets, hacking is openly discussed and even promoted at trade shows, inside university classrooms and on Internet forums.

Edward Wong, "Hackers Find China Is Land of Opportunity," NEW YORK TIMES, May 22, 2013, http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html?pagewanted=all&_r=1&. The article went on to recount earlier reports that American cybersecurity experts have documented that most cyber-attacks emanating from China occur from 9 a.m. to 5 p.m. Beijing time. *Id.*; *see also* Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," WASHINGTON POST, May 27, 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

A recent report amplified concerns about China-based cyber-theft. *See* Dennis C. Blair, Jon M. Huntsman, Jr., et al., *Report of the Commission on the Theft of American Intellectual Property* 11 (2013), http://ipcommission.org/report/IP_Commission_Report_052213.pdf ("IP Commission Report"). The report declared that "China is the world's largest source of IP theft." *Id.* at 2. Based on a canvassing of various studies and sources, the IP Commission Report

estimated that between 50% and 80% of all intellectual property theft is tied to China. The report also noted that much of China-based cyber-theft "stems from undirected, uncoordinated actions of Chinese citizens and entities who see within a permissive domestic legal environment an opportunity to advance their own commercial interests. With rare penalties for offenders and large profits to be gained, Chinese businesses thrive on stolen technology." *Id.* at 18.

The sentence imposed on Defendant must promote respect for intellectual property laws and attempt to deter both Defendant and all others engaged in software piracy – both in the United States and abroad. The market capitalization and value of today's business organizations is inextricably tied to their intellectual property. *See* IP Commission Report at 11 ("According to a figure cited in the President's 2006 Economic Report to Congress, 70% of the value of publicly traded corporations is estimated to be in 'intangible assets.'"). United States national security depends, in significant part, on protection of the digital technology used by the entities that support and comprise the federal government. Thus, the value of some of our largest and most important companies, as well as our national security, is largely dependent on protecting digital crown jewels. If those jewels are subject to cyber-looting without consequence, the economic foundation and national security of this country are imperiled.

The sentence imposed on Defendant must reject the notion that international cybercrime is not serious here, even if it is acceptable or encouraged abroad. The message needs to go forth that those sitting behind keyboards, beyond oceans and engaging in egregious and systematic digital looting of intellectual property will suffer severe consequences if they should ever find themselves a defendant standing in the well of a United States District Court.

### C. The Need to Avoid Unwarranted Sentencing Disparities

The Court also must ensure that the sentence imposed does not create unwarranted disparities relative to sentences imposed on other defendants for similar crimes. The difficulty, of course, is that Defendant's criminal conduct is of a magnitude and character that has rarely, if ever, been seen in this Court.

There has been only one other defendant sentenced in this district for criminal copyright infringement through operation of a software piracy website. *See United States v. Jaime Lynn Snyder*, No. 11-97-SLR (D. Del.). In that case, Jaime Lynn Snyder was sentenced to 46 months in prison for operating a website through which she sold $5.9 million worth of consumer software to individuals. At the risk of considerable understatement, the Snyder case pales in comparison to this one.

Foremost, of course, is the value of the software stolen and then released onto the Internet where unlimited access and copying could be had by anyone with a cracked copy of the software. Snyder distributed approximately $5.9 million worth of pirated software. Defendant hand-delivered software and internal proprietary data worth more than that to the agents in Saipan alone. The value of what Defendant stole and passed on to other criminals over three years runs into nine figures.

Snyder was also selling off-the-shelf consumer software products manufactured by such companies as Microsoft and Adobe. Her method of providing user access to the software was as simple as it comes: providing product keys to use during automated installation. This was nothing close to the sophisticated type of software cracking and installation that Defendant was undertaking. Unlike Snyder, Defendant distributed tightly controlled, industrial-grade software to others around the world. Also unlike Snyder, Defendant engaged in ongoing, highly technical

and complex efforts to aid Crack 99 customers in installing and operating the sophisticated software he gave them. Even more unlike Snyder, Defendant also sold and hand delivered 20 gigabytes of confidential, proprietary data exfiltrated from the internal file transfer protocol site of a "cleared defense contractor."

Defendant's customers used the pirated software for purposes that potentially impact the health and safety of individuals and the national security of this country. None of the consumer software that Snyder disseminated was used in the military and intelligence sectors or raised any national security concern. To the best of the government's knowledge, no one who obtained pirated software from Snyder used it to design geospatial intelligence or missile defense systems, and no one used it to design parts for the radar system in the President's helicopter.

Thus, the need to avoid sentencing disparities necessitates a sentence beyond the 46 months that Snyder received for selling $5.9 million worth of consumer software.

## CONCLUSION

For the foregoing reasons, the United States respectfully recommends that the Court impose a sentence of 210 months of imprisonment, and 3 years of supervised release.

Respectfully submitted,

CHARLES M. OBERLY, III
United States Attorney

By: /s/ David L. Hall
David L. Hall
Assistant United States Attorney

By: /s/ Edward J. McAndrew
Edward J. McAndrew
Assistant United States Attorney

Dated: May 30, 2013