United States Probation & Pretrial Services

District of Kansas

Cybercrime Policy:

Computer & Internet Monitoring Program

Introduction

The High-Technology and Computer Crime Policy and Procedure (HACC) Manual was initially created in June 2003. As technology evolves, the U.S. Probation Office for the District of Kansas is faced with the unique challenge of addressing the issues with respect to offenders who commit crimes through the use of a computer. It has become increasingly necessary for the United States Probation Office to keep pace with the technological advancements being made by offenders and preparing ourselves to supervise offenders convicted of computer related offenses. In addition, supervision of these cyber-offenders is complicated by a variety of legal and technical issues.

These policies and conditions are intended to assist officers in the supervision of cyber-offenders and reduce potential risks to the community. The conditions were designed to take into account current as well as emerging technologies, and are intended to apply to the wide variety of electronic services and devices that may be utilized by defendants or offenders.

Crimes we may expect to encounter include, but are not limited to, possession or distribution of child pornography, identity theft, counterfeiting, forgery, theft, copyright violations, official corruption, drug trafficking, and terrorism. With this in mind, the U.S. Probation Office will embody both traditional and technological practices to address the risk posed by these defendants and offenders, consistent with directives of the Court.

Monitoring software and hardware and computer searches and seizures are only some of the tools involved in the supervision of defendants or offenders who have been convicted of computer-related-offenses. All traditional supervision techniques, such as collateral contacts, home contacts, surveillance, location monitoring, and access to financial records remain valid tools in the supervision of the computer-related offender.

Authority

The Computer & Internet Monitoring Program is authorized only as a condition of pretrial release, probation, or supervised release and is not authorized as a sentence by itself. It may be imposed in the original setting of pretrial release or post-conviction supervision conditions. It also may be imposed as a modification to existing release or supervision conditions.

Program Administration

The Chief U.S. Probation Officer, or his/her designee, is responsible for the overall operation of the program and shall appoint a Cybercrime Officer(s) to be responsible for updating the Cybercrime Policy, advising officers on cybercrime issues, coordinating periodic cybercrime training, and designating workgroup members.

Pretrial Supervision

Cases should initially be considered for cybercrime-related special conditions during the pretrial bond and supervision stage. A judicial officer, under the authority of Title 18, U.S.C. 3142(c)(B)(XIV), may impose any condition which is reasonably necessary to assure the appearance of the defendant as required and the safety of any person and the community including a computer monitoring and search condition.

The officer should use information from all available sources, including, but not limited to, the defendant, family members, the case agent and/or Assistant U.S. Attorney to assist in identifying the need for computer search or monitoring conditions. If the instant offense or prior convictions did not involve the use of a computer, the condition may not be appropriate. The fact that a defendant is charged with a sex-related offense or has related background characteristics may not be sufficient to justify the imposition of the Computer & Internet Monitoring Program condition.

The officer should assess, in consultation with the Cybercrime Officer(s) and/or the Supervising U.S. Probation Officer, whether or not the defendant could reasonably be supervised without the imposition of search or computer monitoring conditions. If it is determined the condition is appropriate, the officer should recommend the defendant be placed into the Computer & Internet Monitoring Program and that the appropriate condition be imposed by the judicial officer.

In 2006, with the passing of the Adam Walsh Child Protection and Safety Act, the Bail Reform Act was modified to require the imposition of electronic monitoring as a condition of pretrial release for any case that involves a minor victim under 18 U.S.C. §§ 120, 1591, 2241, 2242, 2244(a)(1), 2245, 2251, 2251A, 2252(a)(1) to (3), 2252A(a)(1) to (4), 2260, 2421, 2422, 2423, 2425, or a 2250 failure to register offense. Additionally, it further requires, at a minimum the defendant abide by specified restrictions on personal associations, place of abode and travel; avoid all contact with an alleged victim of the crime and with a potential witness who may testify concerning the offense; and other conditions specified in § 3142(c)(1)(B)(vi), (vii), (viii). It may be appropriate in these cases to impose the pretrial computer monitoring conditions as a means of verifying the defendant's compliance with the required conditions for no contact with an alleged victim or potential witness.

Proposed Pretrial Supervision Condition

The following condition is recommended as the standard pretrial condition:

> *As directed by the U.S. Probation Officer, the defendant shall cooperate with and abide by the policies of the United States Probation Office's Computer and Internet Monitoring Program which includes restrictions and/or prohibitions related to: computer and Internet usage, possession and use of electronic, cellular, gaming, and Internet appliance devices; possession and use of computer hardware and software, encryption hardware or software, and accessing certain types of web sites to include: social networking, chat rooms, and those depicting sexually explicit conduct or*

pornographic material. The defendant will also be subject to computer monitoring, and will provide the United States Probation Office with a complete inventory of all electronic and Internet capable devices, user account information, and password(s).

Presentence Preparation

Cases should initially be considered for the Computer & Internet Monitoring Program special condition during the presentence investigation process. Key components of the presentence report that assist in determining the defendant's level of knowledge and potential/ability for recidivism include, but are not limited to detailed offense conduct information, education data (degrees, certifications, e.g., Microsoft Certified Systems Engineer), employment history, and criminal history. When preparing a presentence report for the Court on a defendant convicted of a sex or cybercrime offense (computer and/or Internet-related crime, i.e., 18 U.S.C. 1030), the officer should have the defendant complete a Computer & Internet Use Questionnaire and Computer Hardware Data Form, if it appears likely that the defendant's sentence may result in a non-prison term. (see *Forms Directory*). Please refer to the District of Kansas Sex Offender policy for guidance on sex offense cases.

Recommendations for Supervision Conditions

Tenth Circuit case law does not allow for an absolute restriction from computer access, except possibly in the most extreme case. As such, monitoring software/hardware, coupled with computer search/seizure serves as the "least intrusive" and "least restrictive" method for controlling the risk that may be posed by most cyber offenders. Offenders are permitted to use a computer and access the Internet, with the clear understanding that their computer activities are being monitored.

The following condition is recommended as the standard sex offender supervision condition:

As directed by the U.S. Probation Officer, the defendant shall cooperate with and abide by the policies of the United States Probation Office's Computer and Internet Monitoring Program which includes restrictions and/or prohibitions related to: computer and Internet usage, possession and use of electronic, cellular, gaming, and Internet appliance devices; possession and use of computer hardware and software, encryption hardware or software, and accessing certain types of web sites to include: social networking, chat rooms, and those depicting sexually explicit conduct or pornographic material. The defendant will also be subject to computer monitoring, and will provide the United States Probation Office with a complete inventory of all electronic and Internet capable devices, user account information as well as password(s).

The following condition is recommended as the standard cyber crime supervision condition:

> *As directed by the U.S. Probation Officer, the defendant shall cooperate with and abide by the policies of the United States Probation Office's Computer and Internet Monitoring Program which includes restrictions and/or prohibitions related to: computer and Internet usage, possession and use of electronic, cellular, gaming, and Internet appliance devices; possession and use of computer hardware and software, encryption hardware or software, and accessing certain types of web sites to include: chat rooms and those that describe or promote unauthorized access to computer systems. The defendant will also be subject to computer monitoring, and will provide the United States Probation Office with a complete inventory of all electronic and Internet capable devices, user account information as well as password(s).*

In addition to this cybercrime condition, the presentence report writer should consider the applicability of other supervision conditions including search, location monitoring and financial disclosure. The addition of a condition for search and location monitoring should be considered according to the guidelines outlined in the District of Kansas Search and Seizure Policy and Location Monitoring Program Policy, respectively. A specific condition for financial disclosure may be appropriate based upon the nature and circumstances of a specific case (e.g., a Distribution of Child Pornography case for profit).

Computer & Internet Monitoring Program Agreement

Defendants/Offenders ordered to participate in the Computer & Internet Monitoring Program will be required to sign a Computer & Internet Monitoring Program Participant Agreement in conjunction with the type of client – Pretrial, Cybercrime, or Sex crime – being supervised (see Forms Directory). The agreement will provide specific directives and guidelines for the defendant/offender to follow in order to effectively monitor the defendant/offender's computer and Internet access and use. This also allows the U.S. Probation Office to efficiently assure adequate supervision of the defendant/offender without imposing numerous special conditions. The agreement is intended to reduce the risk that the offender will access unmonitored computers, use hardware/software which will interfere with or prevent effective monitoring, or otherwise attempt to circumvent the monitoring process. This agreement will be updated by the Cybercrime Officer(s) on at least an annual basis, to account for changing technology. All defendants/offenders enrolled in the Computer & Internet Monitoring Program will be notified, in writing, of any changes.

Monitoring Software

The U.S. Probation Office for the District of Kansas, currently utilizes Internet Probation & Parole Control, Inc. (IPPC) to monitor a defendant/offender's computer and Internet usage. The monitoring software is installed on the defendant/offender's machine and records all computer activity such as applications running, key strokes typed, and websites visited. The software then uses the Internet to forward regularly scheduled and "event" email reports. This is the least restrictive method and

does not require direct contact with the defendant/offender. The software can only monitor in a Windows environment. At present no software is available to monitor activity in MAC, Linux, or other operating systems.

Computer monitoring software should only be installed, modified, or removed under the direction of an officer with the Cybercrime Workgroup. In addition, installation should occur only after a preliminary review of an offender's computer system, to ensure that no contraband or unauthorized software/hardware is present. The preliminary review should be conducted in a forensically sound manner, using the least intrusive method possible, by a trained, designated member of the Cybercrime Workgroup. There will be a periodic review of any information received from monitoring software.

There are also software applications (Field Search, Presearch, Imagescan and similar programs) that require an on-site visit to where the computer is maintained. Recorded information on the computer's configuration and use is retrieved from the software. This is more restrictive and can require a field contact.

The District of Kansas utilizes both software that forwards information via the Internet and direct access software.

Computer Searches/Seizures

Computer searches may be conducted when the Court has imposed a special condition authorizing such a search, verbal consent is given by the defendant/offender, or when the defendant/offender has specifically provided written consent to a search of his/her computer by completing the Consent to Search Electronic Media Form (see Forms Directory).

Computer searches should be conducted by forensically sound methods, in the least intrusive manner possible. Since improper or inappropriate search techniques could result in serious problems (including data loss, damage to equipment, evidentiary problems, and potential civil liability), searches of computers and computer equipment should only be conducted by the Cybercrime Officer(s)/Workgroup or a trained, designated staff member. IT staff may provide technical consultation, but are not considered law enforcement personnel and may not directly participate in computer searches.

Every effort should be made to complete the computer search on-site. However, the computer and/or storage media (e.g., hard drives, disks, CDs, DVDs) may be seized if it becomes clear the search cannot be completed on-site due to safety concerns, time constraints or technical difficulties. If the search cannot be completed on-site, the offender will be provided a receipt of all items seized, as delineated by District of Kansas Search and Seizure policy. Every effort will be made to complete a search of seized items in a timely manner. Once it has been determined that the seized equipment is no longer needed, either due to revocation or termination of supervision, officers should first consult with the Court to determine the Court's opinion regarding return of the equipment. Prior to

the return of any equipment every effort should be made to remove any and all prohibited data. If available, officers should use the restore to factory setting option or some type of system restore function prior to returning the equipment. In the event that this is not available or fails to remove the prohibited data, then the equipment will either be reformatted (computer systems, storage devices) or destroyed (burned CD's/DVD's or systems that cannot be restored or reformatted).

Searches of an individual, residence, vehicle or place of business should be applied for, planned, and conducted in a manner consistent with the U.S. Probation Office for the District of Kansas Search Policy, which is based upon the Judicial Conference Committee on Criminal Law Model Search and Seizure Guidelines.

Violations

If it appears the defendant/offender has committed an illegal act, the supervision officer will inform the Court, U.S. Attorney's Office and/or the appropriate law enforcement agency of any information regarding the commission of a new crime.

Forms

Computer Hardware & Internet Data Form
Pretrial CIMP Agreement
Sex Offender CIMP Agreement
Cybercrime CIMP Agreement
Computer Activity Log
IPPC Forms
3rd Party Computer Search Acknowledgment Form
Consent to Search Waiver Form - Electronic Media
Handheld Device Form
Gaming Device Form
Computer Password Protected Form
Employer Computer & Internet Use Form
Authorized Computer & Internet Device Form
Software License Form
Username & Password Form
Permission to Sell/Purchase Form

Effective Date: July 29, 2013
Revised March 7, 2014 - Computer Searches/Seizures Section