GENERAL ORDER

DISTRICT OF COLUMBIA

Title
Washington Area Criminal Intelligence Information Systems (WACIIS)

Topic/Number
GO-SPT-302.07

Effective Date **June 11, 2003**

Distribution **A**

Rescinds:
General Order 302.7 (WACIIS)

I. BACKGROUND

The Washington Area Criminal Intelligence Information System (WACIIS) is a centralized computer based criminal information intelligence network. The system can be an invaluable investigative tool when used appropriately. In addition, the system provides for comprehensive case management of law enforcement investigations.

II. POLICY

The policy of the Metropolitan Police Department is to establish policies, procedures, and responsibilities for members utilizing the Washington Area Criminal Intelligence Information System (WACIIS). The WACIIS system is designed to be an effective case management and investigative tool.

III. DEFINITIONS

For the purpose of this directive, the following terms shall have the designated meanings:

1. WACIIS - Washington Area Criminal Intelligence Information System.

2. Authorized Person - any member of this department or person working with the department having a legitimate need to use the WACIIS system.

3. WACIIS System Administrator – the individual responsible for overall management of the WACIIS system.

4. Investigative Personnel - members of the Department who, by virtue of his/her assignment, conduct intelligence gathering and/or follow-up of criminal investigations.

5. Incident Based Investigations - investigations of incidents occurring in the field, which result in the generation of a PD Form 251 (Event Report) i.e., homicide, rape, robbery, theft, etc.

6. Non-Incident Based Investigations - investigations which originate as a result of information coming to the department's attention that requires further investigation in order to develop probable cause for an arrest. This includes any investigation in which a PD 251 was not prepared and exceeds one (1) tour of duty in order to complete (e.g., vice investigations). This does not include forcible stops that are reported in the PD 76 module of WACIIS.

IV. REGULATIONS

A. WACIIS users shall: (CALEA 51.1.1-d)

1. Have access to investigative and criminal intelligence.

2. Enter and retrieve information from WACIIS for legitimate law enforcement purposes.

3. Obtain all information entered into the WACIIS system legally.

4. Not enter into WACIIS any information about the political, religious, or social views, associations, or activities of any individual or group, unless such information directly relates to criminal conduct. There must be a basis to believe there is a reasonable possibility that an individual or organization is involved in criminal activity. (CALEA 51.1.1-a-b)

5. Complete reports and forms through the WACIIS system. This includes investigative reports, warrant affidavits, witness and defendant statements, arrest forms, death reports and other forms installed in the WACIIS system. (CALEA 51.1.1-b)

B. The finding of Reasonable Suspicion is the threshold requirement for the entering of intelligence information into the WACIIS system. The entry of information is limited to criminal conduct and relates to activities that present a threat to the community. (CALEA 51.1.1-a)

C. Members assigned to investigative functions shall: (CALEA 51.1.1-d)

1. Be trained and certified to utilize the WACIIS system.

2. Be issued a WACIIS user account code and obtain a personalized password.

3. Familiarize themselves with the WACIIS system and various codes and instructions on the use of the system.

D. Members assigned to investigative functions shall complete the forms and documents available in the WACIIS system in lieu of pre-printed investigative forms (i.e., PD forms, warrant affidavits, etc.), or forms available electronically using a word-processing application. All reports must be forwarded to a supervisor for approval upon completion. (CALEA 51.1.1-d / 82.2.4)

E. Persons authorized to use the WACIIS system are required to use his/her assigned user account code and personalized password. Under no circumstances shall a member use a user account code or password other than his/her own.

F. Information entered into the WACIIS system must be as accurate as possible. If inaccurate information is observed within the system:

1. The element WACIIS liaison shall immediately be notified.

2. The WACIIS liaison shall notify the WACIIS System Administrator, thru WACIIS electronic mail (e-mail), of any discrepancies.

G. In the event of software malfunctions, the situation shall be brought to the attention of the MPD Help Desk at 727-5284, during business hours, 0630-1800 hours, Monday-Friday.

H. When major problems occur with the WACIIS system during non-business hours, notify the Synchronized Operations Command Center (SOCC), who will notify a member of Information Technology.

I. Training and certification.

1. The Institute of Police Science (IPS) shall develop a centralized training curriculum and certification program for all WACIIS system users.

2. Members desiring to use the WACIIS system shall be required to:

a. Attend training and fulfill all certification requirements prior to utilizing the WACIIS system. (CALEA 33.1.2)

b. Route all training and certification requests to IPS, through his/her respective training coordinator.

c. Familiarize him/herself with the WACIIS on-line help module.

3. The Director, Institute of Police Science, shall make space available at the IPS for such instruction.

J. Operations

The number and type of menu functions available are directly related to the level of access assigned to each authorized user. Access to information shall vary among members by assigned security level. Adjustments shall be made whenever a member is promoted, transferred, or departs employment with the department. (CALEA 42.1.3-d)

1. There are nine (9) levels of access to the WACIIS system. Members requesting authorization to use the WACIIS system and to initiate a system password shall:

   a. Contact the Help Desk to obtain a new account form.

   b. Complete the form and return to the Help Desk.

   c. Contact the Help Desk when a member's password has expired or been forgotten.

2. The generation of new case files are based on incident based investigations. Case numbers shall be obtained in accordance with standard WACIIS training procedures.

3. Investigators shall ensure that the case is updated regarding any new information about the case, particularly any administrative designators concerning case status (i.e., open, closed, suspended, etc.). (CALEA 42.1.3-b)

4. Data and Information in the WACIIS System shall be entered in:

   a. Accordance with data entry standards contained in the on-line help module.

   b. A confidential (hidden) database for sensitive information. Requests for hidden cases shall be made through the chain of command to the Special Services Commander.

5. Dissemination of data shall:

   a. Be for legitimate law enforcement purposes only.

   b. Not be disseminated outside of the member's organizational element without the express approval of an official of that element. Intelligence information relating to active investigations shall not be released to any individual without a personal consultation with the primary member handling the investigation or that member's supervisor.

Note: In the event dissemination (verbal or paper) is authorized by the member's supervisor, the dissemination shall be documented in the member's case file or in the appropriate field/screen in the WACIIS system. (CALEA 51.1.2)

c. As a default, be accessible to any authorized WACIIS user for information on all closed cases. Requests to restrict access to closed cases in the WACIIS system shall be made through the chain of command to the commander of the member's organizational element or his designee (i.e., limiting access to members within a District, Division, Branch, Section, etc.).

6. Resolution of conflicts concerning investigations shall be handled through the chain of command. The Special Services Commander shall resolve conflicts that cannot be resolved at a lower level.

7. Investigative unit supervisors are required to ensure that information entered into the WACIIS system by his/her subordinates is accurate, prior to approving reports on-line. The WACIIS system administrator or his designee shall randomly validate information contained within the WACIIS system. Investigative supervisors shall ensure that any information or case file entered by his/her subordinates is purged from the system when it is determined to be of no further value or does not fit the criteria described in this directive. (CALEA 42.1.3-e)

8. Members shall not rely solely on information contained in the WACIIS system for obtaining affidavits. Members shall confirm information obtained from the WACIIS system prior to swearing to its accuracy. Information contained in warrant affidavits shall be independently verified.

9. When the WACIIS system is down (temporarily deactivated) members shall:

a. Be notified, via the WACIIS bulletin board, prior to any planned deactivation of the WACIIS system. The bulletin board message shall include when the system will be reactivated.

b. Complete essential items in "hard copy" form or form templates in the event that the WACIIS system experiences downtime, and, within 24 hours, enter it into the WACIIS system.

10. One of the functions of the WACIIS system is to reduce the amount of paperwork generated. Copies of WACIIS data should not be produced unless a specific need can be demonstrated.

K. Juveniles

Due to the sensitive nature of juvenile records, special precautions must be taken with regard to entering and retrieving WACIIS records associated with juvenile subjects. (CALEA 51.1.1-b / 82.1.1-a)

a. When a date of birth for a juvenile (subject under eighteen years of age) is entered into WACIIS, the designation " juvenile" shall appear.

b. Members shall ensure that all data involving juveniles are not available to any unauthorized persons.

c. When juvenile records are purged, the WACIIS system manager shall ensure complete deletion from the WACIIS system of the record for which the juvenile was arrested or charged.

L. Accountability

1. Members entering and retrieving information through the WACIIS system shall be held strictly accountable for the proper use and disposition of its content.

2. Information from the WACIIS system shall be used for official law enforcement purposes only, and shall not be given to persons outside the field of law enforcement. For the purpose of this order, the law enforcement field shall consist of any agency having primary responsibility for the administration of criminal justice and which allocates a substantial portion of its budget for this purpose.

3. All investigative information must be placed in WACIIS in a timely manner.

M. Security

1. Under no circumstances shall a member reveal his/her WACIIS personalized password to any persons, except to the Help Desk or WACIIS System Administrator personnel.

2. Members utilizing the WACIIS system shall take extraordinary precautions to ensure that information is not observed or available to unauthorized persons.

3. Members shall not leave the personal computer (PC) unattended while logged into the WACIIS system. The exception to this is when a member has the ability to lock his/her workstation.

4. Misuse of the WACIIS system shall result in the appropriate disciplinary action and/or criminal prosecution in accordance with the applicable laws of the District of Columbia or the United States.

5. At least annually, an audit of the WACIIS system shall be conducted for the verification of all passwords, access codes, or access violations. (CALEA 82.1.6)

N. The WACIIS users group

1. The WACIIS users group shall consist of:

a. WACIIS liaison from each District or Division, and

b. WACIIS System Administrator

2. The WACIIS system manager shall serve as Chairperson of the WACIIS users group.

O. WACIIS System Administrator

The WACIIS System Administrator shall be responsible for:

1. Coordinating and implementing WACIIS system objectives, rules, and regulations.

2. Maintaining the integrity of the WACIIS system by, among other things, ensuring an annual audit of the WACIIS system as described in Section L, 5 of this directive. (CALEA 82.1.6)

3. Conducting routine system management functions, such as backing up data and program files as determined necessary, monitoring audit logs, etc. (CALEA 82.1.8)

a. WACIIS computer files are backed-up on tapes at a pre-determined time, every day of the week, usually during hours of limited use.

b. Should the backing up process require that users temporarily refrain from accessing and using the WACIIS system, the WACIIS System Administrator shall, whenever possible, ensure that system users are notified ahead of time.

c. The WACIIS system Administrator shall ensure that the backing up process is supervised.

d. The backing up process shall be carried out in a manner that meets accepted methods, standards, procedures, and specifications for the hardware and software that is being backed up.

e. The tapes upon which records are backed up shall be securely stored in a location of limited access. Tapes shall be kept in a cool environment and in accordance with manufacturer's specifications. Until they are ready to be recycled, degaussed, or destroyed, they shall be maintained in an environment free of magnetic fields.

f. Creating and updating, as needed, a system disaster recovery plan.

4. Planning future enhancements to WACIIS that are aligned with MPD's mission and strategic goals. (CALEA 11.6.1)

5. Furnishing authorized members with WACIIS system user account codes and assisting them in creating a personal password.

6. Deleting user account codes for those members leaving a job position that had previously permitted access to the WACIIS system.

7. Evaluating requests for software enhancements made by WACIIS users; if justified, budgeting and planning the implementation of software enhancements.

8. The publication and maintenance of WACIIS system operational manuals, memoranda, and procedural modifications.

9. Filling requests for WACIIS system information and statistical searches and data.

10. Acting as the department's liaison with outside agencies concerning WACIIS related issues.

P. The Office of Professional Responsibility (OPR)

Members assigned to OPR shall be exempt from the provisions of this order pertaining to entering investigations into the WACIIS system. However, they shall comply with the remaining sections of this order.

V. PROCEDURES

A. Office of Superintendent of Detectives (OSD) supervisors shall be responsible for:

1. Ensuring that investigative personnel utilize the WACIIS system;

2. Verifying the accuracy of the data entered into the WACIIS system by his/her subordinate members; (CALEA 51.1.1-a)

3. Verifying that relationships entered into the WACIIS system (i.e., subjects, vehicles, telephones, addresses, etc.) are established and accurately correlated;

4. Approving WACIIS system documents to be electronically forwarded to him/her by his/her subordinates; (CALEA 82.2.4)

5. Responding, via Department e-mail, to requests for the creation of new criminal investigation case numbers in other than incident based offenses; and

6. Ensuring that members who have been identified as needing additional or refresher WACIIS system training receive such training. (CALEA 33.1.5)

B. The Director, IPS, shall:

1. Make space available at the IPS for WACIIS system training and certification; and (CALEA 33.2.2-a)

2. Identify instructors who can be utilized to provide user training for the WACIIS application. (CALEA 33.2.1-b / 33.3.1)

C. District Commanders and OSD Commanders shall be responsible for:

1. Causing WACIIS system security to be a frequent subject of investigative roll call training within their element; (CALEA 33.5.2)

2. Causing frequent inspection of the area surrounding WACIIS computer terminals to ensure that security procedures are being adhered to; (CALEA 53.2.1-a)

3. Establishing procedures for generating non-incident-based offense case files within his/her organizational element;

4. Establishing procedures for the dissemination of WACIIS system data for members of his/her Command;

5. Ensuring that members of his/her Command adhere to WACIIS system validation procedures.

// SIGNED //
Charles H. Ramsey
Chief of Police

CHR:NMJ:MAR:njg