Republic of the Philippines
NATIONAL POLICE COMMISSION
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
OFFICE OF THE CHIEF, PNP
Camp BGen Rafael T Crame, Quezon City

MEMORANDUM CIRCULAR
NO.: 2021-141

21 SEP 2021

GUIDELINES AND PROCEDURES IN REPORTING, RECORDING, MONITORING AND DISPOSITION OF CYBERCRIME AND CYBER-RELATED INCIDENTS

1. REFERENCES:

a. Revised Penal Code (RPC);
b. Republic Act (RA) No. 10175 (Cybercrime Prevention Act of 2012);
c. Executive Order No. 2 series of 2016;
d. NAPOLCOM Memorandum Circular (MC) No. 94-017 entitled, "Adopting a Uniform Criteria in Determining When a Crime is Considered Solved," dated June 2, 1994;
e. PNP MC No. 2020-051 (Amendment of the Terminologies of the PNP MC No. 2018-050 entitled, "Guidelines and Procedures in Reporting Crime Incidents and its Supplemental Guidelines" dated August 4, 2020;
f. PNP MC No. 2018-050 entitled, "Guidelines and Procedures in Reporting Crime Incidents," dated January 7, 2019;
g. Investigative Directive No. 2017-002 entitled, "Directive on the Referral and Conduct of Digital Forensics Examination" dated December 4, 2017;
h. PNP Criminal Investigation Manual (Revised 2011);
i. Memorandum from D, LS addressed to D, ACG with subject, "Legal Opinion on the Proposed Investigative Directive," dated January 22, 2021; and
j. Memorandum from ACG addressed to TDIDM with subject: Guidelines and Procedures in Reporting, Recording, Monitoring and Disposition of Cybercrime and Cyber-Related Incidents, dated February 1, 2021.

2. RATIONALE:

RA No. 10175, otherwise known as the Cybercrime Prevention Act of 2012, defines and penalizes another set of crimes[1], collectively referred to as cybercrimes. The law also recognizes the complexity of investigating "existing" crimes committed with the aid of technology.

Due to the peculiar nature of cybercrime incidents, the approach of investigation and determination of customer satisfaction vastly differ from that of investigating traditional crimes. For instance, a victim of libel by a dummy Facebook account would only want the account to be deleted; once done, the victim becomes disinterested in pursuing the case. Or, in a case of threat using a text message, a

[1] Sections 4 and 5 of R.A. No. 10175

disclosure of data[2] of a service provider would tell that the mobile number used is a prepaid subscriber. In this case, the investigators would usually have no other recourse.

For CY 2017 to 2019, the PNP Anti-Cybercrime Group (ACG) has received a total of 10,665 complaints. Out of said complaints, 681 were filed before the Office of the Prosecutor, 4,126 were deemed resolved through other means, and the remaining 5,858 were considered unsolved.

Hence, to resolve the cybercrimes and cyber-related incidents not covered in the PNP MC No. 2018-050, the Directorate for Investigation and Detective Management (DIDM) crafted this MC to be adopted by the PNP especially by the ACG in recording, reporting, monitoring, and disposition of cases of cybercrime and cyber-related incidents.

3. SITUATION:

With the activation of the ACG in 2013, the PNP has recorded a surge of reports on cybercrime incidents that resulted in the increase of non-index; however, the solution efficiency remained low because of cases which were not pursued.

The definition of "case solved" under NAPOLCOM MC No. 94-017, would initially give the impression that other legal means of considering a case solved are not covered by the definition; however, a closer review actually gives room for other means of solution. In particular, other means of crime solution may be based on the liberal interpretation of the following rule:

> "A case shall be considered solved as per parameter set forth in **LOI 02-09 (UCPER),** which was clearly defined under **NAPOLCOM MC No. 94-017**, paragraph 2 of solved cases which states that "**a case shall be considered solved when some elements beyond police control prevent the arrest of the offender, such as when the victim refuses to prosecute after the offender is quoted identified or the offender dies or absconds.**"

The term "such as" connotes that the cases mentioned therein are not exclusive and are merely examples of instances "beyond police control," thus, there is no prohibition to provide/identify similar circumstances under the principle of *ejusdem generis*.

A classic example is the refusal of a victim to further cooperate in the cybercrime investigation in such a way that the identity of offender/s or elements of the crimes could no longer be ascertained without such cooperation. Another is the deletion/deactivation of the suspect's social media account wherein it exceeds the data retention period before the police starts a cybercrime or cyber-related crime

---

[2] by virtue of a Warrant to Disclose Computer Data under A.M. No. 17-11-03-SC or the Supreme Court Rule on Cybercrime Warrant

investigation, and the victim could not provide evidence of its existence or identification.

The two examples are but a few of reasonable circumstances when a cybercrime or cyber-related crime investigator could no longer proceed with the investigation.

In addition to this, the present Guidelines and Procedures in Reporting Crime Incidents under PNP MC 2018-051 *(Guidelines for brevity),* do not cover other forms of cybercrime case, thus, resulting to a lower statistics and crime solution efficiency.

4. PURPOSE:

a. To provide guidelines and procedures in reporting, recording, monitoring and disposition of cybercrime incidents as addendum to PNP MC 2018-051; and

b. To determine other circumstances that may be considered beyond police control in treating a cybercrime incident as "solved" or "cleared" based on the parameters provided under NAPOLCOM MC No. 94-017.

5. DEFINITION OF TERMS:

a. Beyond police control – reasonable circumstances outside of the control of the police preventing him to arrest the offender or to establish the elements of the crime.

b. Case Solved – a case shall be considered deemed solved with the attendance of any of the following circumstances:
   1) The offender has been identified, arrested, and charged before the prosecutor's office or court of appropriate jurisdiction;

   2) When some elements beyond police control prevent the arrest of the offender, such as when the victim refuses to prosecute after the offender is identified or offender dies or absconds; and

   3) The arrest of one offender can solve several crimes or several offenders maybe arrested in the process of solving a crime **(NAPOLCOM MC No. 94-017).**

c. Cyber – refers to a computer or a computer network, the electronic medium in which online communication takes places.

d. Cybercrime incidents – refers to cybercrime offenses and cyber-related crimes collectively.

e. Cybercrime Offenses – offenses defined and penalized by Sections 4 and 5 of RA No. 10175, under the categories of a) offenses against the confidentiality, integrity, and availability of computer data and systems; b)

computer-related offenses; c) content-related offenses and d) other offenses **(Sections 4 and 5, RA No 10175)**.

f. Cyber-related crimes – violation of the RPC and special laws committed with the use of information and communications technology **(Section 6, RA No. 10175).**

g. Head of office – refers to the Directors, NSUs; Regional Directors; Provincial Directors; Chiefs of Police; Station Commanders for NCRPO; Chiefs of Special Operating Units or Regional Anti-Cybercrime Units of ACG; and Chief, WCPC.

h. Information and Communications Technology (ICT) – refers to a system intended for, and capable of, generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording or storage of electronic data message or electronic document **(IRR, RA No. 10175).**

i. Predicate offense – specific offense defined and penalized by the RPC or special laws, the commission of which are qualified by Section 6 of RA No. 10175 (i.e. Estafa, Threat, Unjust Vexation, Violation of R.A. 9995, and the like).

j. Private cybercrime incidents – private offenses which cannot be prosecuted except upon a complaint filed by the aggrieved party (i.e. RA No.9995 or the Anti-Photo and Video Voyeurism Act of 2009).

k. Public cybercrime incidents – involving the abuse and exploitation of women, children, and other forms of gender-based violence, such as child pornography, child abuse, violence against women and children, and trafficking in persons wherein a case will pursue even without the complainant.

6. CLASSIFICATION OF CYBERCRIMES and CYBER-RELATED OFFENSES

a. The following acts are classified as **cybercrime** offenses pursuant to Sections 4 and 5 of RA No. 10175:
   1) Offenses against confidentiality, integrity, and availability of computer data and systems.
      a) Illegal Access;

      b) Illegal Interception;

      c) Data Interference;

      d) System Interference;

e) Misuse of Devices; and

f) Cyber Squatting.

2) Computer-Related Offenses
   a) Computer-Related Forgery;

   b) Computer-Related Fraud; and

   c) Computer-Related Identity Theft.

3) Content-Related Offenses
   a) Cybersex;

   b) Child Pornography; and

   c) Libel.

4) Other Offenses
   a) Aiding or Abetting in the Commission of Cybercrime; and

   b) Attempt in the Commission of Cybercrime.

b. **Cyber-related offenses** under Section 6 of RA No. 10175 are those defined and penalized by the RPC, as amended, and special laws, if committed by, through and with the use of information and communications technologies.

7. GUIDELINES:

a. **General Guidelines:**

1) All violations under Sections 4 and 5 of RA No. 10175 classified as cybercrimes, except Child Pornography and Libel, shall be primarily investigated by the ACG. As such, said unit is mandated to collect cybercrime data and record complaints in their police blotter; Crime Information, Reporting and Analysis System (CIRAS); and other Next Generation Investigation System (NGIS); and

2) For Child Pornography, Libel and cyber-related offenses under Section 6 of RA No. 10175, the ACG and other police units have jurisdiction to conduct an investigation. However, police units that do not have trained personnel in cybercrime investigation may request for technical assistance from the ACG.

b. **Specific Guidelines:**

1) **REPORTING and RECORDING**
   a) All reported cybercrime incidents whether through walk-in, short messaging system (SMS), PNP ACG e-Complaint Desk, PNP ACG

e-Complaint Text/Hotline Number, and referred cases or any means shall be attended to by the desk officer/duty personnel and referred to the duty investigator;

b) Cases received through e-Complaint shall be forwarded to the nearest ACG office, and the Investigator-on-Case (IOC) will directly contact the complainant in order to give guidance as to what pieces of evidence should be presented for the conduct of investigation and filing of appropriate charges;

c) Reporters of cybercrime incidents through SMS shall be advised to proceed to the nearest ACG or police unit concerned for proper recording and validation. They shall also be advised to bring additional pieces of evidence, if necessary;

d) All cybercrime incidents investigated by the IOC shall be recorded and classified as either cybercrime or cyber-related offense, as the case maybe. For cyber-related offenses, only the predicate offense shall be counted although the same may have been qualified by Section 6 of RA No. 10175. To avoid double entry, the police unit that conducted cybercrime investigation of the case is the one responsible to record the same in the blotter and encode in CIRAS and other NGIS;

e) All complaints shall be recorded in the police blotter, encoded in CIRAS and other NGIS and must satisfy the essential elements of investigation which shall answer the five Ws (What, Who, When, Where, and Why) and one H (How); and

f) In cases falling under Item 7 (b.2, sub-paragraph 2.1) of this MC, the IOC shall prepare a corresponding report indicating that the complainant failed to comply with the requirements or refused to pursue the case, as the case may be. He shall recommend that the case be considered as solved subject to the approval of the immediate Head of Office. However, if the complainant later submits the evidentiary requirements needed and decides to file the case, the IOC shall take appropriate action, unless barred by existing laws, rules, and regulations.

2) **DISPOSITION**

a) When a complainant or his/her representative (with SPA and notarized affidavit of complainant) reports a cybercrime/cyber-related incident, he/she will be made to sign an undertaking to comply with the requirements of the IOC in support of the investigation.

b) For purposes of reporting cybercrimes and cyber-related crimes, a case shall be considered solved under the criteria of "beyond police control" when any of the following circumstances is present:

(1) Failure of the complainant to submit evidentiary requirements;
(2) Complainant declines to prosecute the case;

(3) Complainant merely requests to record the incident;

(4) Complainant only requests to deactivate a fake/dummy account or delete pornographic video/picture and/or videos in websites; and

(5) Complainant cannot be found despite diligent and reasonable efforts of the PNP.

(a) Private cybercrime/cyber-related incidents

(a.1) If, without justifiable reasons, the complainant/s in a private cybercrime/cyber-related incident **failed to submit evidentiary requirements** within the three scheduled meetings agreed to by him/her or informing him/her through registered mail, e-mail, private courier (i.e. LBC, FedEx, JRS and the like) by the IOC, he/she will be treated as a disinterested complainant. The IOC shall endeavor to contact the complainant and inquire the circumstances of his/her failure to submit, and if the same is due to his/her disinterest in the case, the IOC shall make an Investigative Report (IR) to that effect.

(a.2) A case shall also be considered solved when the **complainant declines, in writing, to prosecute or pursue the same** despite exhaustion of all means to convince her/him. In case of failure of the complainant to submit a written document or Affidavit despite efforts by the IOC, the latter shall **execute an Affidavit** stating that complainant refused to prosecute or pursue the case.

(a.3) If a **complainant requests to record an incident for future reference but refuses to follow through for whatever reason** to have the case investigated, he/she shall be required to execute a sworn statement indicating the fact of the refusal and the reason/s for such refusal.

(a.4) If the **complainant only wants to deactivate a fake/dummy or similar social media account or delete pornographic picture/s and/or videos in websites** on a valid and verified complaint, but will not pursue any case, he/she is also required to

execute a sworn statement indicating the reason/s thereof.

(a.5) Provided however, despite the aforementioned circumstances, if the complainant later submits the evidentiary requirements needed and decides to file the case, the IOC shall take appropriate action, unless barred by existing laws, rules, and regulations.

(b) Public cybercrime incidents

(b.1) In cases of public cybercrime incidents involving the abuse and exploitation of women, children, and other forms of gender-based violence, such as child pornography, child abuse, violence against women and children, and trafficking in persons, the cases shall be investigated by trained women and children investigators or, in the absence of such investigator, the case shall be endorsed to the WCPC, CIDG or ACG, despite the refusal of the victim to pursue a case.

3) MONITORING

The status of all cybercrime and cyber-related incidents investigated by Police Regional Offices (PROs), Police Provincial Offices (PPOs), Police Stations, Criminal Investigation and Detection Group (CIDG) and ACG, as the case may be, should be regularly updated by the units concerned for assessment and analysis.

8. RESPONSIBILITIES:

a. **Crime Research and Analysis Center (CRAC)**
1) Monitor the implementation of this MC;

2) Designate personnel to monitor all cybercrime/cyber-related cases; and

3) Perform other tasks as directed.

b. **School for Investigation and Detective Management (SIDD)**
1) Ensure that this MC is included in the syllabus and include the same during the conduct of investigation courses; and

2) Perform other tasks as directed.

c. **Information and Technology Division (ITD)**

1) Make adjustments on the Crime Information, Reporting, and Analysis System (CIRAS) in order to cater cybercrimes and cyber-related crimes;

2) Ensure that cybercrime and cyber-related crime cases and statistics can be generated from CIRAS for analysis; and

3) Perform other tasks as directed.

d. **Women and Children Protection Center (WCPC)**

1) Monitor all cybercrime incidents involving women and children;

2) Ensure that all handled cybercrime incidents involving women and children are reported and updated in CIRAS; and

3) Perform other tasks as directed.

e. **Anti-Cybercrime Group (ACG)**

1) Act as the OPR of this MC;

2) Assist for policy formulation on cybercrime investigation;

3) Formulate guidelines in investigation, forensic examination, evidence recovery, and forensic date, consistent with industry standard practices of the PNP;

4) Conduct orientation/briefing to this Directive to all concerned personnel or first responders of cyber-related incidents of PROs and other NSUs with investigative capabilities;

5) Ensure that all handled cybercrimes and cyber-related crimes are recorded and updated in CIRAS;

6) Monitor all cybercrime incidents;

7) Maintain necessary and relevant databases for statistical and/or monitoring purposes;

8) Provide cybercrime and cyber-related analysis as needed;

9) Coordinate with the WCPC on the monitoring of cybercrime incidents involving women and children; and

10) Perform other tasks as directed.

f. **PROs, Other National Support Units with Investigative Capabilities**

1) Ensure that all handled cyber-related crimes are recorded and updated in CIRAS;

2) Refer all violations of Sections 4 and 5 of RA No. 10175 to ACG; and

3) Perform other tasks as directed.

9. PENAL CLAUSE:

Any violation of this MC shall constitute a cause of action against the erring PNP personnel in accordance with NAPOLCOM MC No. 2016-002 and other applicable laws, rules, and regulation.

10. REPEALING CLAUSE:

Any provision of issuances, memoranda, rules, and regulations pertaining to the recording, reporting, and monitoring of cybercrime incidents, inconsistent with any of the provisions of this Directive are deemed repealed or amended accordingly.

11. EFFECTIVITY:

This MC shall take effect after 15 days from filing a copy thereof at the UP-Law Center in consonance with Section 3, Chapter 2, Book VII of Executive Order 292, otherwise known as the "Revised Administrative Code of 1987," as amended.

GUILLERMO LORENZO T ELEAZAR
Police General
Chief, PNP

Distribution:
Command Group
IG, IAS
Cmdr, APCs
D-Staff
P-Staff
D, NSUs
RD, PROs
SPA to the SILG

CPNP *Ltrs'21* S086869
S086869