Philippines

2014-2015 Cybercrime Report

The Rule of Law in Cyberspace

15 March 2015
Manila
**The Vision**

A just and peaceful society anchored on the principles of transparency, accountability, fairness and truth.

**The Mission**

Towards the effective, efficient and equitable administration of justice.
# Table of Contents

**Messages** ........................................................................................................................................... 1

**About the Department of Justice – Office of Cybercrime** ................................................................. 2
  - Structure .................................................................................................................................................. 3
  - Cybercrime Desk ..................................................................................................................................... 4
  - Prosecution Task Force on Cybercrime ................................................................................................. 3

**Legal Framework** ............................................................................................................................... 6
  - Cybercrime Prevention Act of 2012 ........................................................................................................ 6
  - Rules on Electronic Evidence ................................................................................................................ 6
  - Data Privacy Act of 2012 ....................................................................................................................... 6
  - Anti-Child Pornography Act of 2012 ..................................................................................................... 6

**Current Trends and Challenges** ........................................................................................................ 4
  - Offenses against and by means of computer system ............................................................................. 5
  - Challenges on Electronic Evidence ....................................................................................................... 6

**Authorities under the Cybercrime Prevention Act of 2012** .............................................................. 6
  - Cybercrime Investigation and Coordinating Center ............................................................................. 6
  - Department of Justice – Office of Cybercrime ..................................................................................... 6
  - National Bureau of Investigation – Cybercrime Division ...................................................................... 6
  - Philippine National Police – Anti-Cybercrime Group ......................................................................... 6
  - Cybercrime Investigation Flowchart .................................................................................................... 6

**Priorities** ............................................................................................................................................... 6

**Operational Achievements** .................................................................................................................. 6

**Future Plans and Programs** ............................................................................................................... 6
Message from Secretary of Justice Leila M. De Lima

Greetings!

It is my honor and privilege to present the DOJ Office of Cybercrime’s 2014 Annual Report which details the accomplishments in providing special protection to the public by implementing our cybercrime and cyber-related laws, particularly the Cybercrime Prevention Act of 2012 which is geared for the prevention, investigation, interdiction and prosecution of cybercrime cases.

Since the passage of Republic Act No. 10175, the Department has taken arduous steps in strengthening the government’s capability to implement and enforce the law in order to fight cybercrime in the country. This report outlines not only the milestones of what the Department has achieved but also emphasizes the continuing efforts and expected outputs sought to be attained.

I thank all the men and women who constituted the technical working group that crafted the implementing rules and regulations of the cybercrime law, including all stakeholders – private and public sectors who participated in the public consultations and provided vital inputs, comments, and suggestions.

I also thank our law enforcement authorities, the National Bureau of Investigation Cybercrime Division and the Philippine National Police Anti-Cybercrime Group, who are more than ever vigilant and responsible in protecting our citizenry against cybercrime.

As the government’s principal law agency, the Department vows to give more protection to those who are more vulnerable in our society. I speak of our Filipino children who are ever more acquainted with modern technology, especially in the internet. It is more important that we protect our children against online child abuse and punish those who are treacherously doing harm using anonymity in cyberspace.

In the current pursuit in fighting cybercrime, it is also the continuing directive for the Office of Cybercrime to provide capacity building trainings to our law enforcement authorities, prosecutors,
state counsels, public attorneys, judges, and other government agencies.

Further, we anticipate the designation of special cybercrime courts, and also our country’s accession to the Convention on Cybercrime of the Council of Europe.

Finally, it is the responsibility of the Department to prioritize the fight against online child abuse, internet fraud and network security. Thus, we call on all government agencies, the ICT industry, and the private sector to unite and be one in the fight against cybercrime.

Mabuhay at maraming salamat po!
Message from Assistant Secretary Geronimo L. Sy - Head, Office of Cybercrime

2014 is a year of significant progress for the implementation of the Cybercrime Law. It is a great pleasure to present the 2014 Annual Cybercrime Report and highlight the performance of the Department in carrying out its vision of having a sound, safe, and secure cyberspace.

Though the Cybercrime Law was challenged on constitutional grounds, the Supreme Court upheld its validity on 18 February 2014 which paved the way for further action to disseminate information on its implementation.

As stated in the Report, the Office of Cybercrime (OOC) spearheaded the formulation of the implementing rules and regulations (IRR) and conducted series of meetings and public consultations with stakeholders, industry partners, and concerned government agencies. The envisioned result is a skillful execution of investigating and prosecuting cybercrimes.

Concrete accomplishments included trainings and workshops focused on investigations on cybercrimes, handling and analyzing electronic and digital evidence, and cyber incident response, which were attended by judges, law enforcers and other personnel.

Also worth noting is our partnership with foreign agencies and our local law enforcement agencies, which led to the arrest and prosecution of violators of RA 9208, RA 7610, Article 201 of the Revised Penal Code (RPC) and RA 9775.

As we pursue our mission to suppress cybercrime, we are confident that the strategic direction we have chosen is sound as we recognize the need to continue training our law enforcement agencies on computer forensics which is an important part of cybercrime investigations. Indeed, providing them with structured procedures and guidelines consistent with international best practices that will strengthen the protection of the citizenry against cybercrime.
We made considerable progress in 2014, but there is much to be done to institutionalize our fight against cybercrime.

I wish to thank the dedicated efforts of everyone who are involved in the implementation of the Cybercrime Law. I hope that the continued support from various agencies will further improve our performance and enable us to reach our targets for the coming years.

Thank you.
I. About the Office of Cybercrime (OOC)

Section 23 of Republic Act (R.A.) No. 10175 or the Cybercrime Prevention Act of 2012 provides for the creation of an Office of Cybercrime (OOC) within the Department of Justice (DOJ) and is designated as the central authority in all matters related to international mutual assistance and extradition for cybercrime matters\(^1\).

The institution of central authorities is a common feature of modern instruments dealing with mutual assistance in criminal matters, and it is particularly helpful in ensuring the kind of rapid reaction that is so useful in combating computer or computer-related crime.

Primarily, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive request are dealt with properly.

In this regard, to ensure that the technical nature of cybercrime and its prevention is given focus, Section 11 of R.A. No. 10175 specifically mandates the National Bureau of Investigation – Cybercrime Division and the Philippine National Police – Anti-Cybercrime Group (ACG) to submit timely and regular reports including pre-operation, post-operation, and investigation results and such other documents as may be required, to the DOJ-OOC for monitoring and review\(^2\).

To meet the standard of the Council of Europe’s Convention on Cybercrime which calls for a single ‘central authority,’ the duties and responsibilities of the DOJ-OOC as provided in the rules and regulations that implements R.A. 10175 are the following:

---

\(^1\) Section 23, R.A. 10175
\(^2\) Section 11, Ibid.
a. To act as a competent authority for all requests for assistance for investigation or proceedings concerning cybercrimes, facilitate the provisions of legal or technical advice, preservation and production of data, collection of evidence, giving legal information and locating suspects;

b. To act on complaints/referrals, to cause the investigation and prosecution of cybercrimes and other violations of the Act;

c. To issue preservation orders addressed to service providers;

d. To administer oath, issue subpoena and summon witnesses to appear in an investigation or proceedings for cybercrime;

e. To require the submission of timely and regular reports including pre-operation, post-operation and investigation results and such other documents from the PNP and NBI for monitoring and review;

f. To monitor the compliance of the service providers with the provisions of Chapter IV of the Act, and Rules 7 and 8;

g. To facilitate international cooperation with other law enforcement agencies on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;

h. To issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;

i. To prescribe forms and templates including but not limited to preservation orders, chain of custody, consent to search, consent to assume account/online identity, request for computer forensic examination; and

j. To undertake the specific roles and responsibilities of the DOJ related to cybercrime under the Implementing Rules and Regulation of Republic Act No. 9775 or the Anti-Child Pornography Act of 2009;

k. To perform such other acts necessary for the implementation of the Act.
Cybercrime Desk for MLAT-EXTRAT

For immediate attention that is essential for the effective implementation and enforcement of the Cybercrime Prevention Act of 2012, Department Order No. 814 established the Cybercrime Desk – a task force that handles Mutual Legal Assistance and Extradition request was constituted which is comprised of State Counsels from the Office of the Chief State Counsel and Office of Cybercrime.

Chief State Counsel Ricardo V. Paras III and Assistant Secretary Geronimo L. Sy serves as the Chair and Vice-Chair, respectively, and five State Counsels complete the Desk.

Assistance and support that may be required by the Cybercrime Desk will be provided by the Office of Cybercrime, in consideration of the technical nature which will accompany requests for cooperation to and from this jurisdiction.
Prosecution Task Force on Cybercrime

The National Prosecution Service - Prosecution Task Force on Cybercrime was constituted in the DOJ central office to handle high-profile and sensational cases. Said Task Force is chaired by Senior Deputy State Prosecutor Theodore M. Villanueva and vice-chaired by Senior Assistant State Prosecutor Lilian Doris S. Alejo.

The Cybercrime Prosecution Task Force in the National Capital Region Prosecution Offices was also established which will handle cybercrime and cybercrime related cases within their respective jurisdiction which are punishable under the following laws:

a. RA 10175 – Cybercrime Prevention Act of 2012
b. RA 9995 – Anti-Photo and Voyeurism Act of 2009
c. RA 9775 – Anti-Child Pornography Act of 2009
d. RA 8792 – E-Commerce Act of 2000
e. RA 8484 – Access Devices Regulation Act of 1998
f. RA 4200 – Anti-Wiretapping Law of 1965

The OOC coordinates with law enforcement agencies and the foregoing Task Force to monitor cybercrime and cybercrime related cases for the effective implementation and enforcement of the said laws.

II. Current Trends and Challenges

There are around 177 Internet Service Providers (ISPs) in the country today with the major providers offering services at an average rate of P25.00 per hour. Digital subscriber line (DSL), wireless and fixed broadband, cable, satellite Internet facilities are now being offered to the public making access to the internet easily serviceable. The number of Philippine Internet users range to 33.6 million.\(^3\) Contributing heavily to its growth are Internet cafes that allow Filipinos who do not own computers to gain access to the facility at an affordable price. An increasing number of schools and small and medium enterprises (SMEs) accessing the Internet contributed to this growth as well.

\(^3\) PNP Cybersecurity, Research and Analysis Division Report (30 June 2012)
The Philippines has been regarded as a haven of crime committed online for many years while other countries have developed cyberwarfare. It has only begun its stand when the country received recognition in 2000 as the source of “LOVE BUG” or the “I love you” virus. It has been 13 years since the virus bolstered the insufficiency of the government’s policies on cybercrime suppression, investigation and prosecution when the author of the virus was released from jail and no case was filed against him for lack of legislation defining the act as a crime and imposing penalty for such commission.

On 12 September 2012, the Philippine Congress enacted the Cybercrime Prevention Act to govern crimes committed in the cyberspace. The new law specifies several new acts of cybercrime. Among those prohibited under the law are cybersex, online child pornography, illegal access to computer systems or hacking, online identity theft, and spamming. It increases the penalty for computer-related crimes. However, the law could not take its course in attaining its aim due to the indefinite restraining order issued by the Supreme Court for its implementation until the petitions challenging constitutionality of the law were resolved last February 2014.

Offenses against and by means of computer system

Cyberespionage attacks or intellectual property theft is considered as the major threat that increasingly hits the manufacturing sectors as well as small businesses with 42% surge during 2012 compared to 2011. Thirty one percent of these attacks are directed to small businesses that are attractive targets. Consumers remain vulnerable to ransomware and mobile threats, particularly on the Android platform.

From rank 35th in 2012, Philippines has moved to rank 39 among countries globally on internet threat activities, according to the annual Symantec Internet Security Threat Report (ISTR). According to this year’s ISTR, the top growing trends that organizations in the country should watch out for in today’s threat landscape includes advanced targeted attacks, mobile threats, malware attacks and data breaches. Targeted attacks are growing, with the number of daily targeted attacks increasing from 7 per day to 82 per day by the end of 2011.

Targeted attacks use social engineering and customized malware to gain unauthorized access to sensitive information. Meanwhile, the report cited that the most frequent cause of data breaches that could facilitate
identity theft or loss of a computer or other medium on which data is stored or transmitted, such as smartphone, USB key or backup device.

From January to December of 2014, the Philippine National Police (PNP) – Anti-Cybercrime Group (ACG) recorded six hundred fourteen (614) cybercrime incidents, compared to 2013 where there were only two-hundred and eighty-eight (288) incidents.
Crimes against Children

The online platforms of social engagement brings a number of benefits to children but it can also be a source of threat to their safety and protection. Children use it as a tool for education thus making them prone to online predators usually disguised as “virtual friends” or “virtual mentors. Globally, sexual abuse and exploitation on children online is alarming, and in response to this, fifty four (54) countries around the world have gathered in a Global Alliance against Child Sexual Abuse Online and which was launched on 5 December 2012.

The Philippines is a signatory to this global alliance and is committed to contribute to the meeting of the four (4) policy targets set, such as:

- Enhancing efforts to identify victims and ensuring that they receive the necessary assistance, support and protection;
- Enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders;
- Increasing awareness among children, parents, educators and the community at large about the risks; and
- Reducing the availability of child pornography online and the re-victimization of children.

In compliance to the commitment to the Global Alliance, the DOJ Convergence of Councils and Committees for Child Protection held a small roundtable dialogue with relevant and critical public and private stakeholders. The dialogue format is deemed to be a balanced and civil forum to stimulate dialogue and collaboration, to help build trust and transparency among stakeholders, and to provide a venue to discuss areas of cooperation and partnerships to intensify the fight against alarming increase in the number of cases of abuse and exploitation of Filipino children online.

At present, the alarming issues of child pornography locally and globally, citing a three hundred forty-five (345%) increase in child pornography sites from year 2001, and more than twenty thousand (20,000) child pornographic images on the internet every week. 2005 data

---

4 Convergence of Councils and Committees for Child Protection
from computer and IT magazine Top Ten Reviews noted that child pornography is a three billion dollar ($3 Billion) industry.\(^5\)

**Challenges on Electronic Evidence**

On the advent of accessibility and affordability of internet connection, communications have shifted peoples’ medium of interactions. These interactions using electronic gadgets have spawned legal controversies as to the use of the electronic writings and its admissibility in court. With the ever-growing demand to regulate transactions in the Internet, legislators enacted Republic Act No. 8792, otherwise known as the "E-Commerce Law". This law was subsequently followed by the issuance of the Supreme Court of A.M. No. 01-7-01-SC, otherwise known as the "Rules on Electronic Evidence".

The admissibility of electronic evidence becomes a major issue of the citizens due to its unreliability and doubtful authenticity having internet technology involvement. Taking advantage of the complex technology offered nowadays, electronic documents by all means could be changed and altered and used as evidence to prove allegations to the point of making false accusations and unjust judgment. Citizens, law enforcement officers and judiciary’s inability to understand the divergence in technology will hamper the applicability and practicability of the Rules. Electronic documents without electronic signatures and proper authentication will have no credit on court cases. With such issues and the continuing struggles of some people deprived of justice, electronic evidence could also be an avenue to enhance the divisions between the rich and the poor.

At present, the PNP-ACG Digital Forensics Laboratory recorded that they were able to examine eight hundred fourteen (814) phones with nine hundred ninety-three (993) SIM cards, and three hundred forty-four (344) memory cards.

\(^5\) DSWD-ITMS
Mobile Phone Examined

<table>
<thead>
<tr>
<th></th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>49</td>
<td>56</td>
<td>47</td>
<td>66</td>
<td>82</td>
<td>87</td>
<td>51</td>
<td>126</td>
<td>47</td>
<td>113</td>
<td>47</td>
<td>43</td>
<td>814</td>
</tr>
<tr>
<td>Sim Card</td>
<td>53</td>
<td>59</td>
<td>68</td>
<td>83</td>
<td>92</td>
<td>126</td>
<td>67</td>
<td>150</td>
<td>56</td>
<td>132</td>
<td>56</td>
<td>51</td>
<td>993</td>
</tr>
<tr>
<td>Memory Card</td>
<td>21</td>
<td>29</td>
<td>17</td>
<td>31</td>
<td>35</td>
<td>39</td>
<td>25</td>
<td>40</td>
<td>20</td>
<td>41</td>
<td>26</td>
<td>20</td>
<td>344</td>
</tr>
</tbody>
</table>

On the part of computer examined, PNP ACG received and examined one hundred thirty two (132) Hard disk Drives and ten (10) laptops. While sixty-five (65) USB, fifty-two (52) CD, thirty-nine (39) DVD, seven (7) CCTV footage, six (6) IPads and five (5) cameras were examined.

Computer Examined

<table>
<thead>
<tr>
<th></th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDD</td>
<td>1</td>
<td>17</td>
<td>21</td>
<td>15</td>
<td>36</td>
<td>5</td>
<td>18</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>10</td>
<td>5</td>
<td>132</td>
</tr>
<tr>
<td>LAPTOP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
</tbody>
</table>
### III. Legal Framework


#### Cybercrime Prevention Act of 2012

The Philippines was invited to accede to the Budapest Convention on 15 June 2011 without objection from member countries and annually invited to join the Octopus Conferences. The Philippines substantially adopted the international definition of cybercrimes by the Council of Europe and assisted the decision-maker to uphold the same by enacting a cybercrime law.
On 12 September 2012, the Philippine Congress enacted Republic Act (R.A.) No. 10175 or “Cybercrime Prevention Act of 2012” which completely addresses crimes committed against and by means of computer system. The law focuses on the pre-emption, prevention and prosecution of cybercrimes such as offenses against the confidentiality, integrity and availability of computer data and systems, computer-related offenses, and content-related offenses.

The law provides procedural measures to be undertaken by law enforcement authorities mandated by the law to enforce and implement its provisions. To ensure that the technical nature of cybercrime and its prevention is given focus and the procedures involved for international cooperation considered, law enforcement authorities specifically the computer or technology crime divisions responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.

**Rules on Electronic Evidence**

The Philippine Supreme Court issued and adopted the Rule on Electronic Evidence or A.M. No. 01-7-01-SC pursuant to its rule-making power and consistent with Republic Act No. 8792 or the “E-Commerce Act of 2000” which gives credence to admissibility of evidence in electronic form and to secure legal framework and environment for electronic commerce. The Rule took effect on 1 August 2001 which was initially applicable only to all civil actions and proceedings, as well as quasi-judicial and administrative cases and amended to include criminal cases on 12 October 2002.

The E-Commerce Act of 2000 is basically patterned from United Nations Commission on International Trade Law Model Law on Electronic Commerce to maintain uniformity and harmony with the other member-states of the United Nations. The salient features of the Act are as follows:

1. Provision on legal recognition of electronic documents or data messages, electronic signatures, and electronic contracts;
2. Require all government agencies to, among others, transact government business and perform government functions using
electronic data messages or electronic documents within two (2) years from the date of effectivity of the Act;  
3. Require the government to install an electronic network known as the RP Web within two years (2) years from the date of effectivity of the Act; and  
4. Penalize the offenses of hacking, cracking and piracy.

**Data Privacy Act**

On 15 August 2012, Republic Act No. 10173 or the Data Privacy Act of 2012 was enacted which was significantly influenced by Directive 95/46/EC of the European Union and the Asia Pacific Economic Cooperation Information Privacy Framework. The introduction of the Act follows a series of developments in the expansion of data privacy laws in the Asia Pacific region and adds to an increasingly complex data privacy environment, particularly for organizations using business process outsourcing services based in the region. The salient features of the Act are as follows:

1. Require all personal information controllers to comply with a raft of requirements before any collection, holding, processing or use of the personal information takes place;  
2. Secure personal information handled by employees of BPO companies based in the Philippines;  
3. Attract more investors in the information and communication technology and BPO industry in the Philippines; and  
4. Impose stronger sanctions on offenders.

The Act also created the National Privacy Commission (NPC), an independent privacy regulator, to administer and implement the Act. It is an agency attached to the Department of Information and Communications Technology and headed by a Privacy Commissioner. The NPC will be responsible for the enforcement and administration of the Act. The NPC's powers include handling privacy-related complaints, conducting investigations, issuing orders for compliance and issuing temporary or permanent bans on data processing by named Controllers.

**Anti-Child Pornography Act**

In order to guarantee the fundamental rights of every child from all forms of neglect, cruelty and other conditions prejudicial to his
development, the Philippine Congress enacted Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009". The Act declares the following acts unlawful:

(a) To hire, employ, use, persuade, induce or coerce a child to perform in the creation or production of any form of child pornography;
(b) To produce, direct, manufacture or create any form of child pornography;
(c) To publish offer, transmit, sell, distribute, broadcast, advertise, promote, export or import any form of child pornography;
(d) To possess any form of child pornography with the intent to sell, distribute, publish, or broadcast: Provided. That possession of three (3) or more articles of child pornography of the same form shall be prima facie evidence of the intent to sell, distribute, publish or broadcast;
(e) To knowingly, willfully and intentionally provide a venue for the commission of prohibited acts such as, but not limited to, dens, private rooms, cubicles, cinemas, houses or in establishments purporting to be a legitimate business;
(f) For film distributors, theaters and telecommunication companies, by themselves or in cooperation with other entities, to distribute any form of child pornography;
(g) For a parent, legal guardian or person having custody or control of a child to knowingly permit the child to engage, participate or assist in any form of child pornography;
(h) To engage in the luring or grooming of a child;
(i) To engage in pandering of any form of child pornography;
(j) To willfully access any form of child pornography;
(k) To conspire to commit any of the prohibited acts stated in this section. Conspiracy to commit any form of child pornography shall be committed when two (2) or more persons come to an agreement concerning the commission of any of the said prohibited acts and decide to commit it; and
(l) To possess any form of child pornography.

The Act defines and punishes syndicated child pornography. It also requires Internet Service Provider (ISP) to notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Furthermore, an ISP shall preserve such evidence for purpose of investigation and prosecution by relevant authorities. An ISP shall, upon the request of proper authorities, furnish the particulars of users who gained or
attempted to gain access to an internet address which contains any form of child pornography.

All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered. The National Telecommunications Commission (NTC) shall promulgate within ninety (90) days from the effectivity of this Act the necessary rules and regulations for the implementation of this provision which shall include, among others, the installation of filtering software that will block access to or transmission of any form of the child pornography.

However, the Act does not require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person which gives loophole for possible violation of the Act and it further provides that no ISP shall be held civilly liable for damages on account of any notice given in good faith in compliance with this section.

To date, the National Telecommunication Commission (NTC) issued Memorandum Circular No. 01-01-2014 that provides guidelines for ISPs for the installation of filtering softwares that will block access to or transmission of any form of child pornography.

IV. Authorities under the Cybercrime Prevention Act of 2012

a. Cybercrime Investigation and Coordination Center (CICC)

The CICC is an inter-agency body created by virtue of the Philippine Cybercrime Prevention Act of 2012, and is under the administrative supervision of the Office of the President which was established for policy coordination among concerned agencies and for the formulation and enforcement of the national cyber security plan.

It is headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson; the Director of the NBI as Vice-Chairperson; and the Chief of the PNP, the Head of the DOJ Office of Cybercrime, and one (1)
representative each from the private sector, non-governmental organizations, and the academe as members.

b. **Department of Justice (DOJ) - Office of Cybercrime (OOC)**

The OOC is an office within the DOJ created under Republic Act 10175 or the “Cybercrime Prevention Act of 2012” and is designated as the Central Authority in all matters relating to international mutual assistance and extradition for cybercrime cases.

The OOC is also tasked to monitor and review cybercrime and cyber-related cases being handled by the NBI and PNP.

c. **National Bureau of Investigation (NBI) – Cybercrime Division (CCD)**

The NBI-CCD is tasked to investigate all cyber related crimes punishable under CPA and related laws, and to establish and maintain an Incident Response Team and Digital Forensic Section that will be responsible for responding to the current and emerging cyber threats, and conducting digital forensic examination and analysis.

At present, NBI-CCD has eight (8) agents and five (5) special investigators, and regional operatives nationwide. It is manned by a Chief, Operations Officer, Section Team Leaders, Cybercrime Investigators, Regional Laboratories, Digital Forensic Technicians, and other Support Staff.

d. **Philippine National Police (PNP) – Anti-Cybercrime Group (ACG)**

The PNP-ACG investigates all cybercrimes and other crimes in which Information and Communications Technology (ICT) is used in the commission of criminal acts or the object of attack, conduct data recovery and forensic analysis on all computers, computer peripherals and storage devices, and other digital evidence seized by PNP units and any other law enforcement agencies within the country.
It provides operational support to investigating units within the PNP, including the search, seizure, evidence preservation, forensic examination and analysis of all digital evidence from crime scenes, and conducts security vulnerability assessment of Information and Communications Technology (ICT) systems in both public and private infrastructures.

In addition, the PNP-ACG maintains Cyber-Patrolling and Terror Response Team for the monitoring and production of social media exploitation made by Persons of Interest (POI); and Project AngelNet specifically focuses on an information dissemination campaign for the protection of women and children from the menace of online abuse.

Currently, there are 110 police officers who serve as special investigators in PNP-ACG who shall ensure the citizens safety online and these officers are detailed to different units of PNP-ACG such as Child Protection, Economic Crimes, Financial Intelligence, Organized Crimes and other units.
V. Priorities

**Online Child Abuse**

Considering that most of the cases received by the office pertains to child pornography, in April 2014, OOC was provided access to the Virtual Private Network (VPN) of the National Center for Missing and Exploited Children (NCMEC), and was designated as its point-of-contact for the Philippines. OOC gets notified when NCMEC receives a report that has a Philippine nexus through its CyberTipline which operates as a national clearinghouse in the United States for tips and leads relating to child sexual exploitation.

The CyberTipline is authorized by U.S. Congress to create a reporting mechanism for members of the public, law enforcement, and certain corporate entities, including U.S. electronic service providers (ESPs) that have statutory reporting obligations to report to NCMEC instances of child sexual exploitation, including child pornography. From April 2014 to December 2014, OOC was notified by NCMEC with Twelve Thousand Three Hundred Seventy Four (12,374) reports of child exploitation where either the offended party or the offender is in the Philippines. All these NCMEC reports were shared with the Inter-Agency Council against Trafficking (IACAT) and Inter-Agency Council against Child Pornography.

In May 2014, the OOC was introduced to INTERPOL’s International Child Sexual Exploitation (ICSE) image database. Said database is equipped with tools to extract digital information from images and check it against existing data, and with numerous other features designed to aid investigators and enhance their investigations.

INTERPOL also invites the Philippines to become a member of the international community of specialized units to save children from
sexual exploitation, and requests OOC to identify the appropriate national unit in the Philippines to be connected to ICSE.

In this regard, the Inter-Agency Council against Child Pornography (IACACP) has recommended that the OOC be the national unit in the Philippines to be connected to ICSE.

**Online Fraud and Network Security**

The OOC has conducted Basic Cybercrime Ethical Hacking Trainings for law enforcers as counter-measure to hacking and network security issues of government and business firm sites. It was attended by the NBI-CCD operatives and PNP-ACG officers. Further, OOC committed to place digital forensic equipment, surveillance equipment and other equipment to enhance the capabilities of the Cybercrime Division of the NBI and Anti-Cybercrime Group of the PNP.

The OOC also participated in the Cybersecurity Forum conducted by the National Defense College of the Philippines entitled “How Safe is Your Money?: Rethinking Cybersecurity”. The said forum provided a venue for various stakeholders, including representatives from government agencies, the banking sector, remittance centers, and other financial institutions, to discuss and exchange best practices in enhancing cybersecurity.

VI. Operational Achievements

a. Implementing Rules and Regulations

In February 2014, immediately after the Supreme Court upheld the constitutionality of the controversial Cybercrime Prevention Act of 2012, the OOC spearheaded the formulation of the implementing rules and regulations (IRR) by convening all the government agencies concerned and thereby created a technical working group (TWG).
The final draft of the Implementing Rules and Regulations has been recommended for approval by the Secretaries of the Interior and Local Government, of Science and Technology and of Justice. Members of the technical working group (TWG) include representatives from the following agencies:

1. Department of Justice (DOJ) – Office of Cybercrime;
2. DOJ – National Prosecution Service;
3. DOJ – Office of the Chief State Counsel;
4. Department of Science and Technology – Information and Communications Technology Office (DOST-ICTO);
5. Department of Foreign Affairs (DFA);
6. Department of Local and Interior Government (DILG);
7. Philippine National Police (PNP); and

The TWG conducted series of meetings and public consultations with stakeholders and industry partners from business, media, academe, ICT organizations, legal profession, non-government organizations, internet service providers, and all national government agencies.

b. Ratification of the Budapest Convention on Cybercrime

The DOJ has already prepared a platform agenda paving the way to subsequent ratification while awaiting concerned agencies for their respective concurrence certificates.
The Philippine Cybercrime Law adopted almost all substantial provisions of the Budapest Convention, which shows our readiness to comply with the international standards provided under the Convention.

c. Capacity Building

a. Global Action against Cybercrime (GLACY) Project

In January 2014, the OOC started formulating the Global Action on Cybercrime (GLACY) project country report and work plan in partnership with the Council of Europe (CoE). This project aims to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention.

On November 24-28, 2014, the OOC, in partnership with the Council of Europe (CoE) and European Union (EU), conducted a Judicial and Law Enforcement Training Workshop on Cybercrime. This is a unique workshop that integrates the tasks of the OOC in the context of the COE-EU Global Action against Cybercrime (GLACY) project of which the Philippines is a priority country. The said training, which was attended by Judges and law enforcers, focused on the handling of electronic evidence in Court.
b. Cybercrime Training for Investigators, Prosecutors, State Counsels, Public Attorneys and Judges

The OOC continuously conducts series of trainings for designated personnel on topics such as conducting investigations on cybercrimes, handling and analyzing electronic and digital evidence, and cyber incident response.

More than 300 investigators and prosecutors nationwide are trained in conducting cybercrime investigation.

c. Inter-Council Coalition against Online Child Abuse

Considering that there exists overlapping of functions and to ensure that efforts are consolidated and resources are maximized, the Office of Cybercrime hosted a three-day workshop to coordinate and consolidate the respective efforts of the IACAT, IACACP, CSPC, and OOC in combating child sexual abuse online. The moderator for the said workshop will submit a consolidated proposal to the working group that would serve as the country action plan in combating child sexual abuse online.
d. DOJ-NU partnership

The Department of Justice signed of a Memorandum of Agreement (MOA) between the DOJ Office of Cybercrime (OOC) and the National University (NU) for a Digital Forensics degree program to build a corps of anti-cybercrime professionals.

The NU is the first educational institution approved by the Commission on Higher Education to offer a four year bachelor degree program in digital forensics. The MOA provides for an exchange of expertise and sharing of resources. For example, the DOJ shall provide lecturers and resource speakers on the cybercrime law and cyber-related laws and jurisprudence.

d. Investigation and Enforcement Highlights

Online Child Abuse Case

In February 2014, the Department of Justice (DOJ) – Office of Cybercrime (OOC) received an investigative lead from the United States Homeland Security Investigations (USHSI) Manila Attaché about an individual in
the Philippines who produces child pornography online.

Said lead was based from the results of computer forensic examination conducted by USHSI in connection to an arrest of an online sexual predator in the United States. Several chats and electronic payments were revealed to be in relation to child pornography activities of the subject in the Philippines.

Investigation was conducted in coordination with the National Bureau of Investigation and the Inter-Agency Council against Trafficking. Subject, one of the minor victims, and the target area were identified. A search warrant was requested and subsequently granted.

Before implementing the search warrant, agents were able to confirm that subject was online and in control of the victims. Operatives rushed to the subject area and there caught subject in flagrante delicto, in a room with four (4) other female individuals who were all later confirmed to be of minor age, ranging from ages 9 to 14, in front of a laptop computer negotiating the price and cyber sexual shows they would perform.
Subject was placed under arrest and immediately apprised of his constitutional rights, and charged for violations of RA 9208, RA 7610, Article 201 of the Revised Penal Code (RPC) and RA 9775.

**Sextortion Case: Operation Strikeback**

“Sextortion” is a form of sexual exploitation that employs non-physical forms of coercion to extort money from the victim in exchange of the non-posting of the victim’s sexual video online.

On Nov 11, 2013, Police Senior Superintendent Gilbert C. Sosa, Director of the PNP-ACG, attended the *1st Eurasian Working Group Meeting for Heads of Cybercrime Units* in Singapore. It was found out that the Philippines is the number one country with the highest recorded cases of “sextortion”.

In February 2014, the DOJ – OOC received an investigative lead from the Scotland Police and U.S. Homeland Security Investigations regarding a case of “sextortion” wherein the minor victim in UK committed suicide.

An INTERPOL meeting was immediately convened on March 2014 to assess the situation and consolidate all information gathered by concerned law enforcement agencies worldwide. The meeting was attended by U.K. Child Exploitation Online Protection (CEOP), Scotland Police, Hong Kong...
Police Force, Singapore Police Force, Australian Federal Police (AFP), DOJ-OOC, PNP-ACG, and private entities such as Facebook, Google, and Western Union.

Based on the information gathered, there were more or less nine thousand (9,000) suspected accounts related to sextortion activities. Two thousand eight hundred (2,800) of which were traced to be from the Philippines.

During investigation, the PNP-ACG was able to identify the subjects and the fifteen (15) target locations. Search warrant operations were simultaneously conducted in the 15 identified target areas. Fifty seven (57) subjects were arrested and more than two hundred (200) digital evidence were seized.
VII. Future Plans and Programs

a. National Computer Forensics Training Program

In all cybercrime investigations, computer forensics is mostly, if not always, placed as its heart. It is a complicated science with its own history, implications, and future. We acknowledge that it is just getting more and more complicated.

In light of this, a National Computer Forensics Training Program (NCFTP) will be launched to train and capacitate our law enforcers in computer forensics jointly. The main purpose is to have a consolidated training for all Law Enforcement Agencies in computer forensics and provide them with a structured procedures and guidelines consistent with international best practices.

b. First cyber-responders training

Nowadays, all types of criminal investigations involve electronic evidence. It is therefore imperative to train our law enforcers, even those who are not involved in cybercrime investigation, especially the usual first responders, in cyber-incident response.

The OOC will start conducting First Cyber-Responders training to the usual crime scene incident responders to ensure that the volatile nature of electronic evidence is preserved and are collected in accordance with rules and regulations, and international best practices.

c. CPA v2

In its effort to strengthen the Cybercrime Prevention Act of 2012, this Department has submitted a working draft to Congress of a new version of cybercrime law that would supplement and enhance the existing law.
The new version will delete the provisions of cyber-squatting, libel, restricting or blocking access, and will focus on priority areas such as online child abuse, online fraud, and network security.

d. Cybercrime Courts

The DOJ has submitted a proposal to the Supreme Court for the creation of Cybercrime Courts nationwide and a specialized division in the Court of Appeals to handle cybercrime cases.

This is in line with Section 21 of R.A. No. 10175 which states that “There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.”

---

6 Section 21, R.A. 10175