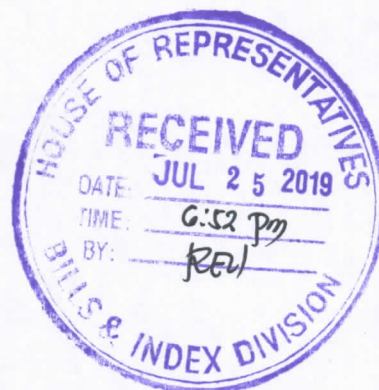


Republic of the Philippines  
**HOUSE OF REPRESENTATIVES**  
Quezon City, Metro Manila

Eighteenth Congress  
First Regular Session

HOUSE BILL NO. 2951



---

Introduced by Representatives Ria Christina G. Fariñas  
and Rudys Caesar G. Fariñas

---

**EXPLANATORY NOTE**

This bill seeks to enhance the nation's security by providing for the electronic surveillance of foreign entities who are known for or suspected of intending to harm the security and interests of the Philippines and its people. It is a complement to Republic Act No. 9372, or the "Human Security Act of 2007," which earlier was passed to provide the country's security agencies the necessary tools and weapons to combat the menace of international terrorism.

The Human Security Act is a landmark piece of legislation that is widely hailed even by our security allies as closing the loopholes which used to prevent our security forces from fully utilizing available resources in the fight against domestic and international terrorists. However, the said Act and all of the country's other laws relating to public order, national security, telecommunications, and cyberspace are still seen as unable to completely equip the country's national security apparatus with what it needs to prevent a catastrophe like another terrorist invasion or even a cyber-attack.

As shown by the recent incident in Marawi City, our security forces need to always be two or three steps ahead of the public's enemies, some of whom have foreign elements or are of foreign origin, and the way to accomplish this is by providing our forces with high-quality, actionable intelligence all the time. It is only when our law enforcers and military are armed with good intelligence that they are capable of fully applying the law's might against those who wish harm on our people.

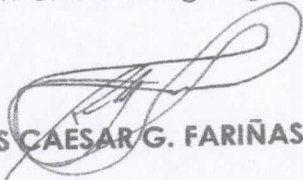
This bill, which is patterned after the Foreign Intelligence Surveillance Act of the United States, augments the features of the Human Security Act by providing for the warrantless surveillance through electronic or mechanical means of foreign entities in domestic and foreign locations in the pursuit of the country's national security goals. For

example, it allows the targeting for surveillance of foreigners outside of the Philippines for up to one (1) year without the need of a court order or warrant. It also provides for safeguards known as "minimization procedures" under which the chances of the surveillance information being misused against a Filipino citizen or any person who is in the Philippines is limited or curtailed. It also provides for the employment of electronic surveillance on any target located anywhere within or outside of the Philippines prior to obtaining a warrant if an emergency situation so warrants. These, in effect, are exceptions to the rule established in our current laws that electronic surveillance may only be done with a warrant.

In essence, the bill legally expands the power of surveillance of security agencies to foreign locations as well as provides for exceptions to the rule that a warrant is necessary to conduct surveillance on Filipino targets or within Philippine jurisdiction. It also protects telecommunications companies, landlords and other service providers, from legal action as a result of their cooperation with the Government in the latter's employment of electronic surveillance for national security purposes.

This measure is a refiled bill from House Bill No. 7111, authored by former Representative Rodolfo C. Fariñas in the 17<sup>th</sup> Congress.

In view of the foregoing, the approval of this bill is highly recommended.



RUDYS CAESAR G. FARIÑAS I



RIA CHRISTINA G. FARIÑAS

Republic of the Philippines  
**HOUSE OF REPRESENTATIVES**  
Quezon City, Metro Manila

Eighteenth Congress  
First Regular Session

HOUSE BILL NO. **2951**

---

**Introduced by Representatives Ria Christina G. Fariñas  
and Rudys Caesar G. Fariñas**

---

**AN ACT STRENGTHENING NATIONAL SECURITY BY PROVIDING FOR THE ELECTRONIC  
SURVEILLANCE OF FOREIGN ENTITIES UNDER CERTAIN CONDITIONS**

*Be it enacted by the Senate and the House of Representatives of the Philippines in  
Congress assembled:*

**TABLE OF CONTENTS**

- SECTION 1. Short Title
- SEC. 2. Definition of Terms
- SEC. 3. Electronic Surveillance Authorization
- SEC. 4. Emergency Authorizations
- SEC. 5. Emergencies Involving Non-Filipino Citizens
- SEC. 6 Testing of Electronic Equipment; Discovering Unauthorized Electronic Surveillance; Training of Intelligence Personnel
- SEC. 7. Retention of Certifications, Applications and Orders
- SEC. 8. Bar to Legal Action
- SEC. 9. Use of Information
- SEC. 10. Report to Supreme Court Office of the Court Administrator Office and to Congress
- SEC. 11. Report of the Secretary of Justice to Congressional Committees; Limitation on Authority or Responsibility of Information Gathering Activities of Congressional Committees; Report of Congressional Committees to Congress
- SEC. 12. Criminal Sanctions
- SEC. 13. Civil Liability
- SEC. 14. Authorization During Time of War
- SEC. 15. Extra-Territorial Application of this Act
- SEC. 16. Separability Clause
- SEC. 17. Repealing Clause
- SEC. 18. Special Effectivity Clause

SECTION 1. **Short Title.** – This Act shall be known as the "*Foreign Electronic Surveillance Act.*"

SEC. 2. **Definition of Terms.** – As used in this Act:

(a) *Foreign entity* means—

(1) a foreign government or any component thereof, whether or not recognized by the Philippines;

(2) a faction of a foreign nation or nations, majority of whose population is composed of persons who are not Filipino citizens;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based non-government organization, majority of whose members or stockholders are persons who are not Filipino citizens;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of Filipino citizens that is engaged in the international proliferation of weapons of mass destruction.

(b) *Agent of a foreign entity* means—

(1) any person other than a Filipino citizen, who—

(A) acts in the Philippines as an officer or employee of a foreign entity, or as a member of a foreign entity as defined in this Act, irrespective of whether the person is inside the Philippines;

(B) acts for or on behalf of a foreign entity which engages in clandestine intelligence activities in the Philippines contrary to the interests of the Philippines;

(C) engages in international terrorism as defined in Republic Act (RA) No. 9372, also known as the "*Human Security Act of 2007*" or activities in preparation therefor;

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign entity, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign entity, whether the activities involve or may not involve a violation of the laws of the Philippines;

(B) pursuant to the direction of an intelligence service or network of a foreign entity, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign entity, whether the activities involve or may not involve a violation of the laws of the Philippines;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign entity;

(D) knowingly enters the Philippines under a false or fraudulent identity for or on behalf of a foreign entity or, while in the Philippines, knowingly assumes a false or fraudulent identity for or on behalf of a foreign entity; or

(E) knowingly aids or abets any person in the conduct of activities described in this paragraph or knowingly conspires with any person to engage in activities described in this paragraph.

(c) *International terrorism* means activities that involve violent acts or acts dangerous to human life as defined in Section 3 of RA 9372 committed within or outside the jurisdiction of the Philippines.

(d) *Sabotage* means activities that involve a violation of Title Three or Title Four of Book Two of the Revised Penal Code or that would involve such a violation if committed against the Philippines.

(e) *Foreign intelligence information* means—

(1) information that relates to, and if concerning a Filipino citizen is necessary to, the ability of the Philippines to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign entity or an agent of a foreign entity;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign entity or an agent of a foreign entity; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign entity or by an agent of a foreign entity; or

(2) information with respect to a foreign entity or foreign territory that relates to, and if concerning a Filipino citizen is necessary to—

(A) the national defense or the security of the Philippines; or

(B) the conduct of the foreign affairs of the Philippines.

(f) *Electronic surveillance means—*

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known Filipino citizen who is in the Philippines, if the contents are acquired by intentionally targeting that Filipino citizen, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the Philippines, without the consent of any party thereto, if such acquisition occurs in the Philippines, but does not include the acquisition of those communications of computer trespassers that would be permissible under the law;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the Philippines;



(4) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication via the Internet or other electronic communications network, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the Philippines; or

(5) the installation or use of an electronic, mechanical, or other surveillance device in the Philippines for monitoring to acquire information, other than from a wire, radio or any electronic communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) *Secretary of Justice* means the Secretary of the Department of Justice of the Philippines (or Acting Secretary of Justice), or, upon the designation of the Secretary of Justice, the appropriate Undersecretary of Justice.

(h) *Minimization procedures*, with respect to electronic surveillance, means—

(1) specific procedures, which shall be adopted by the Secretary of Justice, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting Filipino citizens consistent with the need of the Philippines to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that non-publicly available information, which is not foreign intelligence information, as defined in this section, shall not be disseminated in a manner that identifies any Filipino citizen, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding the above paragraphs, procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding the above paragraphs, with respect to any electronic surveillance approved pursuant to this Act, procedures that require that no contents of any communication to which a Filipino citizen is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72

hours unless a court order is obtained or unless the Secretary of Justice determines that the information indicates a threat of death or serious bodily harm to any person.

(i) *Filipino citizen* means a citizen of the Philippines, either by birth or naturalization, or a corporation, partnership, cooperative, or association a majority of the stock or membership of which is of citizens of the Philippines and which were formed in accordance with Philippine laws.

(j) *Philippines*, when used in a geographic sense, means all areas under the territorial sovereignty of the Philippines as defined in the Constitution.

(k) *Surveilled person* means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) *Wire communication* means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of domestic or foreign communications.

(m) *Person* means any individual, including any officer or employee of the government, or any group, entity, association, corporation, or foreign entity.

(n) *Contents*, when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) *Internet or electronic communication* means any communication made through the use of the Internet, or any similar electronic communications network regardless of whether transmission is made by satellite, wired or wireless means or via access that is free or for a fee through a public network, commercial provider or common carrier.

(p) *Weapon of mass destruction* means—

(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;

(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;



(3) any weapon involving a biological agent, toxin, or vector that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or

(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

SEC. 3. **Electronic Surveillance Authorization.** – (a) (1) Except as otherwise provided in this Act, electronic surveillance conducted anywhere in the Philippines or on targets at least one of whom is located in the Philippines or on a target Filipino citizen located outside the Philippines shall be upon a court order obtained in accordance with RA 9372.

The Secretary of Justice and the Director General of the National Intelligence Coordinating Agency (NICA) may authorize jointly, for a period of up to one (1) year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the Philippines to acquire foreign intelligence information, subject to the limitations that the acquisition:

- (A) may not intentionally target any person known at the time of acquisition to be located in the Philippines;
- (B) may not intentionally target a person reasonably believed to be located outside the Philippines if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the Philippines;
- (C) may not intentionally target a Filipino citizen reasonably believed to be located outside the Philippines;
- (D) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the Philippines; and
- (E) may not be conducted in a manner contrary to Section 2, Article III of the Constitution.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Secretary of Justice's certification of compliance with the foregoing paragraph and the minimization procedures adopted by the Secretary. The Secretary of Justice shall assess compliance with such

procedures and shall report such assessments to the House of Representatives Committee on National Defense and Security under the provisions of this Act.

(3) The Secretary of Justice shall immediately transmit under seal to the Court of Appeals a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Secretary of Justice, in consultation with the Director General of NICA, and shall remain sealed unless—

(A) an application for a court order with respect to the surveillance is made under RA 9372 or this Act; or

(B) the certification is necessary to determine the legality of the surveillance.

(4) With respect to electronic surveillance authorized by this section, the Secretary of Justice may direct a specified communication common carrier to —

(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

(B) maintain under security procedures approved by the Secretary of Justice and the NICA Director General any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

(b) Applications for a court order are authorized if the President has, by written authorization, empowered the Secretary of Justice to approve applications under RA 9372 to the Court of Appeals and the latter may, notwithstanding any other law, grant an order, in conformity with this Act, approving electronic surveillance of a foreign entity or an agent of a foreign entity for the purpose of obtaining foreign intelligence information.

#### SEC. 4. **Emergency Authorizations.** —

(1) Notwithstanding any other provision of this Act, the Secretary of Justice may authorize the emergency employment of electronic surveillance on any target if he —

(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this Act to approve such electronic surveillance exists;

(C) informs, either personally or through a designee, the designated division of the Court of Appeals under RA 9372 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

(D) makes an application in accordance with this Act to the designated division of the Court of Appeals under RA 9372 as soon as practicable, but not later than seven (7) days after the Secretary of Justice authorizes such surveillance.

(2) If the Secretary of Justice authorizes the emergency employment of electronic surveillance under paragraph (1), the Secretary of Justice shall require that the minimization procedures required by this Act for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of seven (7) days from the time of authorization by the Secretary of Justice, whichever is earliest.

(4) A denial of the application made under this Act may be reviewed by the Supreme Court.

(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, department, office, agency, regulatory body, legislative committee, or other authority of the National Government, local government unit, or their political subdivision, and no information concerning any Filipino citizen acquired from such surveillance shall subsequently be used or disclosed in any other manner by government officers or employees without the consent of such person, except with the approval of the Secretary of Justice if the information indicates a threat of death or serious bodily harm to any person.

(6) The Secretary of Justice shall assess compliance with the requirements of paragraph (5).

**SEC. 5. *Emergencies Involving Non-Filipino Citizens.* –**

(1) Notwithstanding any other provision of this Act, the lawfully authorized targeting of a non-Filipino citizen previously believed to be located outside the Philippines for the acquisition of foreign intelligence information may continue for a period not to exceed 72 hours from the time that the non-Filipino citizen is reasonably believed to be located inside the Philippines and the acquisition is subject to this Act, the Rules of Court and other laws, provided that the head of an element of the intelligence community—

(A) reasonably determines that a lapse in the targeting of such non-Filipino citizen poses a threat of death or serious bodily harm to any person;

(B) promptly notifies the Secretary of Justice of a determination under the foregoing paragraph; and

(C) requests, as soon as practicable, the employment of emergency electronic surveillance under the previous section or the employment of an emergency physical search, as warranted.

(2) The authority under this subsection to continue the acquisition of foreign intelligence information is limited to a period not to exceed 72 hours and shall cease upon the earlier of the following:

(A) The employment of emergency electronic surveillance under the previous section or the employment of an emergency physical search.

(B) An issuance of a court order under RA 9372 or this Act.

(C) The Secretary of Justice provides direction that the acquisition be terminated.

(D) The head of the element of the intelligence community conducting the acquisition determines that a request under this section is not warranted.

(E) When the threat of death or serious bodily harm to any person is no longer reasonably believed to exist.

(3) Nonpublicly available information concerning unconsenting Filipino citizens acquired under this subsection shall not be disseminated during the 72 hour time period under paragraph (1) unless necessary to investigate, reduce, or eliminate the threat of death or serious bodily harm to any person.

(4) If the Secretary of Justice declines to authorize the employment of emergency electronic surveillance under the previous section or the employment of an emergency physical search, or a court order is not obtained, information obtained during the 72 hour acquisition time period under paragraph (1) shall not be retained, except with the approval of the Secretary of Justice if the information indicates a threat of death or serious bodily harm to any person.

(5) Paragraphs (5) and (6) of the previous section shall apply to this section.

**SEC. 6 *Testing of Electronic Equipment; Discovering Unauthorized Electronic Surveillance; Training of Intelligence Personnel.*** – Notwithstanding any other provision of this Act, officers, employees, or agents of the government are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Secretary of Justice, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:

(D) *Provided, That* the test may exceed ninety days only with the prior approval of the Secretary of Justice;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce Republic Act No. 4200 or the "Anti-Wiretapping Act" or Republic Act No. 10175 or the "Cybercrime Prevention Act," or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

i. obtain the consent of the persons incidentally subjected to the surveillance;

ii. train persons in the course of surveillances otherwise authorized by this subchapter; or

iii. train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

SEC. 7. **Retention of Certifications, Applications and Orders.** – Certifications made by the Secretary of Justice pursuant to Section 4 of this Act and applications made and orders granted under this Act shall be retained for a period of at least ten years from the date of the certification or application.

SEC. 8. **Bar to Legal Action.** – No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance.

SEC. 9. **Use of Information.** –



(a) **Compliance with Minimization Procedures; Privileged Communications; Lawful Purposes.** – Information acquired from an electronic surveillance conducted pursuant to this Act concerning any Filipino citizen may be used and disclosed by officers and employees of the government without the consent of the Filipino citizen only in accordance with the minimization procedures required by this Act. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this Act shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this Act may be used or disclosed by officers or employees of the government except for lawful purposes.

(b) **Statement for Disclosure.** – No information acquired pursuant to this Act shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Secretary of Justice.

(c) **Notification by the Government.** – Whenever the government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the Philippines, against a surveilled person, any information obtained or derived from an electronic surveillance of that surveilled person pursuant to the authority of this Act, the government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the surveilled person and the court or other authority in which the information is to be disclosed or used that the government intends to so disclose or so use such information.

(d) **Motion to Suppress.** – Any person against whom evidence obtained or derived from an electronic surveillance to which he is a surveilled person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the government, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

- (1) the information was unlawfully acquired; or
- (2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(e) ***In Camera and Ex Parte Review by Trial Court.*** – Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (d), or whenever any motion or request is made by a surveilled person pursuant to any other statute or rule before any court or other authority of the government to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the trial court shall, notwithstanding any other law, if the Secretary of Justice files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the Philippines, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the surveilled person was lawfully authorized and conducted. In making this determination, the court may disclose to the surveilled person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(f) ***Suppression of Evidence; Denial of Motion.*** – If the trial court pursuant to subsection (e) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the surveilled person or otherwise grant the motion of the surveilled person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the surveilled person except to the extent that due process requires discovery or disclosure.

(g) ***Finality of Orders.*** – Orders granting motions or requests under subsection (f), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the trial court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be executory except when restrained by the Court of Appeals or the Supreme Court.

(h) ***Destruction of Unintentionally Acquired Information.*** – In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances

in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the Philippines, such contents shall be destroyed upon recognition, unless the Secretary of Justice determines that the contents indicate a threat of death or serious bodily harm to any person.

**(i) Notification of Emergency Employment of Electronic Surveillance: Contents: Postponement, Suspension or Elimination.** – If an emergency employment of electronic surveillance is authorized under Sections 4 or 5 of this Act and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any Filipino citizen named in the application and on such other Filipino citizens subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

- (1) the fact of the application;
- (2) the period of the surveillance; and
- (3) the fact that during the period information was or was not obtained.

On an *ex parte* showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety (90) days. Thereafter, on a further *ex parte* showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

**(j) Coordination with Law Enforcement on National Security Matters. –**

(1) Government officers who conduct electronic surveillance to acquire foreign intelligence information under this Act may consult with law enforcement or military officers or personnel to coordinate efforts to investigate or protect against—

(A) actual or potential attack or other grave hostile acts of a foreign entity or an agent of a foreign entity;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign entity or an agent of a foreign entity; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign entity or by an agent of a foreign entity.

(D) Coordination authorized under this paragraph shall not preclude the certification required by Section 3 of this Act or the entry of an order under R.A. No. 9372.

**SEC. 10. Report to Supreme Court Office of the Court Administrator Office and to Congress.** – In April of each year, the Secretary of Justice shall transmit to the Supreme Court Office of the Court Administrator and to the Senate and House of Representatives a report setting forth with respect to the preceding calendar year—

(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this Act; and

(b) the total number of such orders and extensions either granted, modified, or denied.

**SEC. 11. Report of the Secretary of Justice to Congressional Committees; Limitation on Authority or Responsibility of Information Gathering Activities of Congressional Committees; Report of Congressional Committees to Congress.** –

(1) On a semiannual basis the Secretary of Justice shall fully inform the Committee on National Defense and Security of the House of Representatives and the Committee on Justice and Human Rights of the Senate concerning all electronic surveillance under this Act. Nothing in this Act shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(2) Each report under the first sentence of paragraph (1) shall include a description of—

(A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this Act where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;

(B) each criminal case in which information acquired under this Act has been authorized for use at trial during the period covered by such report;

(C) the total number of emergency employments of electronic surveillance under Sections 4 and 5 this Act and the total number of subsequent orders approving or denying such electronic surveillance; and

(D) the total number of court authorizations under RA 9372 and the total number of subsequent emergency employments of electronic surveillance under Sections 4 and 5 of this Act.

On or before October 30 of each year, the Committee on National Defense and Security of the House of Representatives and the Committee on Justice and Human Rights of the Senate shall report to their respective chambers concerning the implementation of this Act. Said reports shall include but not be limited to an analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

SEC. 12. **Criminal Sanctions.** –

(a) **Prohibited Activities.** – A person is guilty of an offense if he intentionally—

(1) engages in electronic surveillance under color of law except as authorized by this Act or other laws;

(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act nor other laws.

(b) **Defense.** – It is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) **Penalties.** – Offenses described in this section are punishable under any of the crimes defined in Republic Act No. 10175 or the Cybercrime Prevention Act in their maximum periods.

SEC. 13. **Civil Liability.** – A surveilled person, other than a foreign entity or an agent of a foreign entity, as defined in Section 2(a) or (b)(1)(A) of this Act, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of Section 12 of this Act shall have a cause of action against any person who committed such violation and shall be entitled to civil damages as may be defined in the Civil Code.

SEC. 14. **Authorization During Time of War.** – Notwithstanding any other law, the President, through the Secretary of Justice, may authorize electronic surveillance without a court order under RA 9372 or this Act to acquire foreign intelligence information for a period not to exceed fifteen (15) calendar days following a declaration of war by the Congress.

SEC. 15. **Extra-Territorial Application of this Act.** – Subject to the provision of an existing treaty of which the Philippines is a signatory and to any contrary provision of any law of preferential application, the provisions of this Act shall apply: (1) to individual persons who commit any of the crimes defined and punished in this Act within the terrestrial domain, interior waters, maritime zone, and airspace of the Philippines; (2) to individual persons who, although physically outside the territorial limits of the Philippines, commit, conspire or plot to commit any of the crimes defined and punished in this Act inside the territorial limits of the Philippines; (3) to individual persons who, although physically outside the territorial limits of the Philippines, commit any of the said crimes on board Philippine ship or Philippine airship; (4) to individual persons who commit any of said crimes within any embassy, consulate, or diplomatic premises belonging to or occupied by the Philippine government in an official capacity; (5) to individual persons who, although physically outside the territorial limits of the Philippines, commit said crimes against Philippine citizens or persons of Philippines descent, where their citizenship or ethnicity was a factor in the commission of the crime; and (6) to individual persons who, although physically outside the territorial limits of the Philippines, commit said crimes directly against the Philippine government.

SEC. 16. **Separability Clause.** – If for any reason any part or provision of this Act is declared unconstitutional or invalid, the other parts or provisions hereof which are not affected thereby shall remain and continue to be in full force and effect.

SEC. 17. **Repealing Clause.** – RA 9372 and all laws, decrees, executive orders, rules or regulations or parts thereof, inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

SEC. 18. **Special Effectivity Clause.** – After the bill shall have been signed into law by the President, the Act shall take effect after its publication in three (3) newspapers of national circulation.

Approved,