THE PRIME MINISTER ---	THE SOCIALIST REPUBLIC OF VIETNAM Independence – Freedom – Happiness ---
No.: 05/2017/QD-TTg	*Hanoi, March 16, 2017*

DECISION

PROVIDING FOR EMERGENCY RESPONSE PLANS TO ENSURE NATIONAL CYBERINFORMATION SECURITY

Pursuant to the Law on Government Organization dated June 19, 2015;

Pursuant to the Law on Cyberinformation Security dated November 19, 2015;

Pursuant to the Government's Decree No. 85/2016/ND-CP dated July 01, 2016 ensuring the security of information systems by security grades;

At the request of Minister of Information and Communications;

The Prime Minister promulgates regulations on emergency response plans to ensure national cyberinformation security.

Chapter I

GENERAL PROVISIONS

Article 1. Scope

This Decision provides for the emergency response plans to ensure national cyberinformation security.

Information systems which are under the management of Ministry of National Defence or Ministry of Public Security shall not be governed by regulations herein.

Article 2. Regulated entities

This Decision applies to agencies, organizations, enterprises and individuals directly involved in or related to emergency response activities to ensure the cyberinformation security in Vietnam.

Chapter II

ASSIGNMENT OF DUTIES TO IMLEMENT EMERGENCY RESPONSE PLANS TO ENSURE NATIONAL CYBERINFORMATION SECURITY

Article 3. National Steering Committee on emergency response to ensure cyberinformation security

1. The National Steering Committee on information security shall perform functions of the National Steering Committee on emergency response to ensure cyberinformation security (hereinafter referred to as the "NSC").

2. The NSC shall instruct Ministry of Information and Communications, Ministry of Public Security, Ministry of National Defence and relevant ministries and local governments to conduct emergency response activities to ensure the national cyberinformation security.

Article 4. Standing Committee on emergency response to ensure national cyberinformation security

1. Ministry of Information and Communications shall be the Standing Committee of the NSC (hereinafter referred to as the "Standing Committee") and have the following duties and rights:

a) Make decisions on selection of response plans and take charge of instructing emergency response activities to ensure the national cyberinformation security;

b) Instruct the National Coordination Center to receive, collect and process information and reports on incidents that cause national cyberinformation insecurity and propose response plans;

c) Convene and instruct the Operations Division for response to national cyberinformation security incidents at the request of the National Coordination Center; instruct and assign duties to units in charge of incident response and members of the Response Network to develop response plans;

d) Take charge or assign the National Coordination Center to act as the national agency for cooperation with regulatory authorities of foreign countries or international organizations in responding to or handling incidents related to such countries;

dd) Inspect the compliance by relevant units and send reports to the NSC on emergency response to national cyberinformation security incidents.

2. Where necessary, Ministry of Information and Communications may take charge of establishing the Coordinating Board for emergency response to ensure national cyberinformation security (hereinafter referred to as the "National Response Coordinating Board") that is comprised of: the head of Ministry of Information and Communications, who shall act as the Head of the National Response Coordinating Board, the National Coordination Center acting as the standing member and other members who are heads of Departments of relevant ministries.

Article 5. Steering Committees on emergency response to cyberinformation security incidents of ministries, ministerial-level agencies, the Government's affiliates and People's Committees of provinces or central-affiliated cities

1. Steering Committees on Information Technology of ministries, ministerial-level agencies, the Government's affiliates and People's Committees of provinces or central-affiliated cities shall perform functions of the Steering Committees on emergency response to cyberinformation security incidents within the scope of their management (hereinafter referred to as "Ministerial/ Provincial-level Steering Committees").

In case of unavailability of the Steering Committee on Information Technology or depending on specific conditions, the ministry, ministerial-level agency, the Government's affiliate or the Provincial-level People's Committee may consider establishing the Ministerial- or Provincial-level Steering Committee on emergency response to cyberinformation security incidents which shall be under the management of the head of Ministry or of the Provincial-level People's Committee.

2. Responsibilities and rights of a Ministerial- or Provincial-level Steering Committee:

a) Instruct coordinating or response activities within the scope of its management; instruct its affiliates to cooperate and comply with orders of the National Coordination Center for coordination and/or response to incidents;

b) Convene and instruct the Incident Response Team or the Operations Division for response to cyberinformation security incidents of same level at the request of the specialized incident response unit;

c) Submit report and ask for instructions from the NSC via the Standing Committee on matters that arise during the implementation of duties beyond its competence; work under the management of the NSC via the Standing Committee and the National Cooperation Office.

Article 6. Specialized cyberinformation incident response units

1. Specialized cyberinformation incident response units are agencies in charge of information security or information technology of ministries or Provincial-level People's Committees (hereinafter referred to as the "Specialized incident response units").

Telecommunications or Internet enterprises and managing bodies of large-scale information systems shall establish or appoint specialized units to respond to internal cyberinformation security incidents.

2. Specialized incident response units shall propose the establishment of incident response team and organize incident response activities within the scope of their management; participate in the emergency response activities to ensure the national cyberinformation security upon the request of the Standing Committee or the Coordination Center.

Article 7. National cyberinformation security incident response network

1. The national cyberinformation security incident response network (hereinafter referred to as the "Incident Response Network") includes the following members:

a) Units in charge of incident response, information security or information technology of ministries, ministerial-level agencies, the Government's affiliates and central-level agencies; Departments of Information and Communications of provinces or central-affiliated cities;

b) Relevant agencies/ units affiliated to the Ministry of Information and Communications; The Authority of Information Security, Vietnam Computer Emergency Response Team (VNCERT), Vietnam Internet Network Information Center (VNNIC) and the Authority of Central Posts;

c) Relevant agencies/ units affiliated to the Ministry of Public Security: Authority of Cyber Security; Police Department for High-Tech Crime Prevention;

d) Relevant agencies/ units affiliated to the Ministry of National Defence: Department of Information Technology; Governmental Cipher Committee;
dd) Telecommunications infrastructure service providers, Internet service providers (ISP); data center service providers, lessors of digital data storage space; national database managing body; units in charge of information security or information technology of banks, financial institutions, state treasuries, tax agencies and customs agencies;

e) Organizations or enterprises managing or operating important information systems or SCADA systems (industrial control systems) in the following sectors: Energy, industry, healthcare, natural resources and environment, education and training, population and urban management.

2. Voluntary participants in the Incident Response Network are organizations or enterprises which are not specified in Clause 1 of this Article, are capable of information security or information technology and permitted to join the Incident Response Network by the National Coordination Center. Organizations or enterprises operating in information security or information technology; managing bodies of large-scale information systems, or banking or financial information systems, or SCADA systems; and other entities capable of information security are encouraged to join the Incident Response Network.

3. Vietnam Computer Emergency Response Team (VNCERT) that is the National Coordination Center for Incident Response (hereinafter referred to as the National Coordination Center or the Coordination Center) shall assume responsibility to:

a) Coordinate all incident response activities nationwide; have the rights to mobilize and coordinate members of the Incident Response Network and relevant organizations or units to cooperate in preventing, handling and remedying incidents in Vietnam; have the rights to decide the methods of coordinating incident response activities and assume responsibility for coordination orders/ requests;

b) Take charge of formulating operating regulations of the Incident Response Network; organize and manage the operation of the Incident Response Network; apply for and receive and manage contributions or financial aids from members of the Incident Response Network and other organizations or individuals and other legal funding sources in order to cover operating expenditures of the Incident Response Network; act as the national center for cooperation with foreign organizations or enterprises in response to cyberinformation security incidents.

c) Ministry of Information and Communications shall establish the Managing Board of the Incident Response Network, which is comprised of a head of the National Coordination Center who holds the position of the head of the Managing Board and other members being representatives of members of the Incident Response Network, to manage, cooperate and organize operations of the Incident Response Network.

4. Members of the Incident Response Network are responsible for complying with the operating regulations of the Network and coordination orders given by the National Coordination Center, and actively participating in operations of the Network. Telecommunications enterprises and Internet service providers (ISP) shall store and provide information concerning IP address of subscribers, servers, IOT equipment, log files and logs of domain name system (DNS) within the scope of their management; provide spaces for installing monitoring/ sampling equipment and provide data flows on the Internet to serve the supervision and detection of incidents upon request of the National Coordination Center; arrange 24/7 standing team and personnel and material resources to cooperate and develop solutions for responding to and remedying consequences of incidents in cases where the source of cyberattacks is originated from subscriber(s) under the enterprise's management or at the request of the National Coordination Center.

Article 8. Operations Division for emergency response to ensure national cyberinformation security

1. The Operations Division for emergency response to ensure national cyberinformation security (hereinafter referred to as the "Emergency Response Operations Division") is convened and directed by the Standing Committee, and comprised of:

a) The National Coordination Center (Vietnam Computer Emergency Response Team (VNCERT) – standing member);

b) Authority of Information Security affiliated to Ministry of Information and Communications;

c) Authority of Cyber Security and the Police Department for High-Tech Crime Prevention affiliated to Ministry of Public Security;

d) Department of Information Technology and General Staff affiliated to Ministry of National Defence;

dd) Specialized cyberinformation incident response units of ministries, ministerial-level agencies, the Government's affiliates, Provincial-level People's Committees, telecommunications enterprises, Internet service providers and the managing body of the national important information system.

2. The Emergency Response Operations Division shall have the rights to:

a) Implement operational measures, technical equipment and facilities as well as other appropriate measures within the ambit of assigned functions and duties in accordance with regulations of law;

b) Request relevant authorities, organizations and/or individuals to provide information, documents and/or equipment which are discovered relating to the incident in order to facilitate the incident response;

c) Inspect the information systems of authorities, organizations and/or individuals when there are well-grounded to determine that they are related to the incident in order to facilitate the incident response;

d) Request relevant telecommunications agencies/ enterprises and Internet service providers to cooperate in performing works necessary to respond to the incident.

3. The mechanism for cooperation and sharing of information between members of the Emergency Response Operations Division shall be performed in accordance with regulations of the law and decisions by the Prime Minister.

Chapter III

RESPONSE PLANS

Article 9. Classification of cyberinformation security incidents

Cyberinformation security incidents are considered as serious incidents when they meet all of the following criteria:

1. The compromised information system is the grade-4 or grade-5 information system or on the List of national important information systems and encounters one of the following problems:

a) The system is interrupted;

b) The top-secret data or the state secrets may be revealed;

c) The integrity of the important data of the information system is damaged and the recovery of such important data is impossible;

d) The right to control the information system is seized;

dd) The incident may occur on a large scale or cause a line of adverse impacts or harms to other grade-4 or grade-5 information systems.

2. The managing body of the information system is incapable of controlling or responding to the incident.

Article 10. Emergency response plans to ensure national cyberinformation security

1. A national emergency response plan to ensure cyberinformation security is a plan for response to a serious cyberinformation security incident that meets the criteria mentioned in Article 9 and the compromised information system is the grade-5 one or on the List of national important information systems.

2. Emergency response plans to ensure cyberinformation security of state agencies, political organizations or socio-political organizations are the plans for response to serious cyberinformation security incidents that meet the criteria stated in Article 9; the compromised information systems are the grade-4 ones and the managing bodies of the compromised information systems are affiliated to ministries, ministerial-level agencies, the Government's affiliates, state agencies, political organizations or socio-political organizations (hereinafter referred to as “central-level agencies”).

3. Provincial emergency response plans to ensure cyberinformation security are the plans for response to serious cyberinformation security incidents that meet the criteria stated in Article 9, in which, the compromised information systems are the grade-4 ones and the managing bodies of the compromised information systems are affiliated to People’s Committees or Provincial or City Committees of the Communist Party of provinces or central-affiliated cities (hereinafter referred to as “provincial agencies”).

4. Emergency response plans to ensure cyberinformation security of enterprises are the plans for response to serious cyberinformation security incidents that meet the criteria stated in Article 9, in which, the compromised information systems are the grade-4 ones and the managing bodies of the compromised information systems are telecommunications enterprises, state-owned enterprises managing information systems of grade 4 or higher, or any organizations or enterprises managing information systems on the List of national important information systems (hereinafter referred to as enterprises managing important information infrastructures).

Article 11. Cyberinformation security incident report

1. Reporting cyberinformation security incidents:

a) The information system operating unit shall be responsible for reporting the incident to the managing body, the specialized incident response unit of same level, and the National Coordination Center within 05 days from the detection of the incident; if the information system operating unit defines that the incident may be out of its control, it must carry out the emergency report procedures stated in Clause 2-5 of this Article immediately when the incident is detected or it determined that such incident is out of its control.

b) When detecting any signs of cyber attack or cyberinformation security incident, organizations or individuals should promptly report it to the information system operating unit, the managing bodies relevant information systems, the National Coordination Center and specialized incident response unit or relevant member(s) of the Incident Response Network.

2. Reports on the incident must be made immediately and maintained during the incident response, including: Incident initial report; incident follow-up reports; report on detailed response plan; report to ask for directions; report to ask for support or cooperation; incident final report.

3. Reports may be submitted in the form of official dispatch, by fax, email, MMS (multimedia messaging service) or via the national cyber security incident warning system; templates of reports shall follow regulations on response coordination or guidance by the National Coordination Center.

4. Contents of the incident initial report:

a) Name and address of the information system operating unit; the managing body of the information system; the compromised information system; time of detecting the incident;

b) Personnel in charge of the incident of the operating unit of the compromised information system: Name, position, phone number and email address;

c) Description of the incident: Type of incident, symptoms, preliminary assessment of the severity, spread and impacts of the incident on normal operations of the organization;

d) Provider of information technology/ telecommunications infrastructure services;

dd) List of response actions which have been taken or are being taken to handle the incident;

e) Organizations and/or enterprises supporting or cooperating in incident response, and handling results up to the reporting time;

g) Initial response results;

h) Recommendations for further incident response actions (if any).

5. Principles for reporting and exchanging information involving in incident response:

a) The information system operating unit shall send reports to the managing body of the compromised information system, the specialized incident response unit of the same level and the National Coordination Center;

b) The specialized incident response unit shall send reports to the managing body of the compromised information system, the Steering Committee of higher level and the National Coordination Center;

c) Ministerial- or Provincial-level Steering Committees and the National Coordination Center shall send reports to the Standing Committee and the NSC.

Article 12. Receipt, detection, classification and initial response to cyberinformation security incident

1. Upon the detection or receipt of notification/ report on a cyberinformation security incident within the scope of its management, the specialized incident response unit or the member of the Incident Response Network must:

a) Record or receive the notification or report on the cyberinformation security incident according to process;

b) Promptly notify the incident-related information to the National Coordination Center, the operating unit and the managing unit of the compromised information system and relevant regulatory authorities;

c) Respond to the sender of the incident notification or the incident initial report immediately when receiving it for confirmation purpose;

d) Verify and classify the cyberinformation security incident to select an appropriate response plan or propose the response plan to the Steering Committee of higher level and the National Coordination Center in case the incident occurs out of its control;

dd) Actively give assistance to the operating unit of the compromised information system in responding or handling the incident within the scope of its capacity and responsibility;

e) Supervise the incident response actions and send reports thereof to the Steering Committee of higher level and the National Coordination Center; propose or ask for instructions in case the incident is out of the scope of its competence and responsibility or out of its control;

g) Send periodic reports to the National Coordination Center every 6 months and irregular reports as requested.

2. The National Coordination Center shall assume responsibility to:

a) Publish its phone number, fax number, email address and hotline number on its website, and arrange sufficient staff to maintain the uninterrupted operation of hotline services to receive and respond to incidents;

b) Record or receive the notification or report on the cyberinformation security incident according to process;

c) Respond to the sender of the incident notification or the incident initial report immediately when receiving it for confirmation purpose;

d) Arrange specific staff in charge of communication works in serious incident;

dd) Verify and classify the incident to provide appropriate warnings, coordinate the selection of response plan, organize response activities and prepare reports; request the Standing Committee to make decision on the serious incident and appropriate emergency response plans; report the Standing Committee and the NSC on issues beyond its competence;

e) Organize the cooperation activities with international cyberinformation incident response organizations to receive warnings or information about the cyberinformation security incidents or risks, and cooperate in responding to cross-border incidents or attacks;

g) Fulfill other duties of the National Coordination Center.

3. The information system operating unit, when detecting or receiving the notification of the incident involved in its information system, must:

a) Record or receive the notification or report on the incident and collect information concerning the incident according to process;

b) Respond to the sender of the incident notification or the incident initial report immediately when receiving it for confirmation purpose;

c) Take charge and cooperate with cyberinformation security service providers (if any) and relevant regulatory authorities in performing analysis, verification, preliminary assessment and classification of the incident, conducting incident response actions and reporting in accordance with regulations;

d) Send reports on the incident and response actions, and requests for assistance in responding to the incident or re-assessment of the severity of the incident (where necessary) to the managing body of the compromised information system, the National Coordination Center and specialized incident response unit of the same level.

Article 13. Procedures for response to normal cyberinformation security incidents

Procedures for response to normal cyberinformation security incidents shall be performed in accordance with written guidance or regulations of Ministry of Information and Communications and the National Coordination Center.

Article 14. Procedures for response to serious cyberinformation security incidents

The following procedure for emergency response to serious cyberinformation security incidents shall be applied to the four emergency response plans stated in Article 10 herein. It includes the following steps:

1. Detection of the incident or receipt of incident report

Unit in charge: The information system operating unit; the National Coordination Center.

Coordinating units: The specialized incident response unit; the managing body of the compromised information system.

Working contents: The information system operating unit shall continuously monitor and detect sources of attacks and the incident occurring on the information system under its management. The National Coordination Center shall take charge of organizing activities of monitoring and detecting incidents, and receiving notifications of cyberinformation security incidents from various sources.

2. Verification, analysis, assessment and classification of the incident

Unit in charge: The National Coordination Center.

Coordinating units: The managing body of the compromised information system; specialized incident response units; the information system operating unit. Working contents:

a) The National Coordination Center shall cooperate with the managing body of the compromised information system (or its authorized unit such as the specialized incident response unit or the information system operating unit) to verify the incident in terms of: The incident status; the severity of incident; the extent of incident impact; target and location of the incident.

b) After the incident is verified, the National Coordination Center shall classify the incident and perform the following works:

- If the incident is classified as a normal incident (it fails to meet the criteria mentioned in Article 9 herein), the National Coordination Center shall notify the incident classification result to relevant parties so as to develop the procedure for response to a normal cyberinformation security incident;

- If the incident is classified as a serious incident (it meets the criteria mentioned in Article 9 herein), the National Coordination Center shall notify the incident classification result to the Standing Committee with the following recommendations: Response plan; units participating in the response plan; resources necessary to respond to the incident; plan for convening the Emergency Response Operations Division and performance of works stated in the following Clause 3 of this Article.

3. The Standing Committee’s decision on selection of response plan and members of the Emergency Response Operations Division.

Unit in charge: The Standing Committee.

Working contents:

a) The Standing Committee shall make decision on selection of the emergency response plan and members of the Emergency Response Operations Division according to the report made by the National Coordination Center. Based on the actual situation, the Emergency Response

Operations Division is comprised of the units prescribed in Article 8 herein in conformity with the selected response plan and particulars of the incident.

b) Principles for assigning duties of the emergency response plan to ensure national cyberinformation security:

- Managing response actions and supervising cooperation and information sharing activities: Ministry of Information and Communications, the National Response Coordinating Board;

- Collecting information and sharing, reporting: The National Coordination Center, the managing body of the compromised information system (via the information system operating unit and the specialized incident response unit);

- Analyzing information: The National Coordination Center, the information system operating unit, the specialized incident response unit and members of the Emergency Response Operations Division;

- Preventing and handling incident: The information system operating unit, the specialized incident response unit, the National Coordination Center and members of the Emergency Response Operations Division;

- Remedying, removing and restoring data and normal activities: The managing body of the information system and its authorized units;

- Handling consequences: The managing body of the information system and members of the Emergency Response Operations Division;

- Publishing and handling information crisis: The Standing Committee and the National Coordination Center.

4. Implementation of initial response plan

Unit in charge: The National Coordination Center, the managing body of the compromised information system.

Working contents: The National Coordination Center shall cooperate with the managing body of the compromised information system to immediately perform initial response actions, consisting of:

a) Determination of the scope, objects and targets requiring response actions:

- Relevant incidents occurred;

- Affected objects;

- Scope of incident impact;

- Targets prioritized in the response plan (restore operation, ensure the data confidentiality; ensure the integrity);

- Developments and methods/ strategies of attack;

- Foreseen developments that may occur.

b) Coordination of initial response actions: The Standing Committee shall direct the National Coordination Center to coordinate and share information and documents related to the incident to members of the response plan according to their assigned functions and duties.

c) Warning of the incident on the incident response network: The National Coordination Center shall give warnings of the incident to members of the Incident Response Network and relevant entities or those may face similar incidents.

d) Implementation of temporary recovery measures:

Based on prioritized targets in incident response plan, the managing body of the compromised information system shall cooperate with the National Coordination Center, relevant service providers and other regulatory authorities to recover the most necessary functions, data or connections to minimize damage to the information system, or the prestige of the managing body of the information system as well as mitigate the adverse influence on the society, if any.

The managing body of the information system must closely cooperate with and provide sufficient information to the National Coordination Center in order to supervise and monitor the recovery process and attacks or effects while the incident is still not yet handled thoroughly.

dd) First steps for dealing with consequences: The managing body of the information system should promptly emergency measures to deal with consequences or damage of cyberattacks which cause adverse impacts on the people, society, other authorities and/or organizations at the request of the Standing Committee.

e) Prevention and control of detected attack attempts: The Standing Committee shall coordinate or instruct the National Coordination Center to coordinate relevant regulatory authorities to perform actions to detect and handle sources of attacks and prevent external attacks against the compromised information system. The Standing Committee shall provide or instruct the provision of information and/or evidence relating illegal acts having constituents of a crime (if any) to regulatory authorities affiliated to the Ministry of Public Security so that they can investigate, verify and prevent crimes.

5. Implementing the emergency response plan

a) Directing incident response actions

Unit in charge: The Standing Committee, the Ministerial- or Provincial-level Steering Committees on emergency response to cyberinformation security incidents.

Working contents: Based on the selected response plan, the Standing Committee shall direct the managing body of the compromised information system, the National Coordination Center and the Emergency Response Operations Division to perform duties of the response plan. During the implementation of the response plan, the Standing Committee may, depending on the actual developments of the incident, make decisions on selection of additional members to the Emergency Response Operations Division.

b) Coordinating response actions

Unit in charge: The National Response Coordinating Board, the National Coordination Center.

Working contents: Based on the selected response plan, the National Response Coordinating Board or the National Coordination Center shall coordinate response actions within the ambit of assigned functions and duties and supervise the cooperation and information sharing activities.

c) Statements and information disclosure

The Standing Committee shall assume responsibility to appoint spokespersons to declare statements and provide related information; make decision on location, contents and time of declaring statements and providing related information to mass media agencies, individuals and organizations involved in the incident.

d) Information collection

Unit in charge: The National Coordination Center, the managing body of the information system.
Working contents: Based on requests for information submitted by members of the Emergency Response Operations Division, the National Coordination Center shall cooperate with the managing body of the information system to collect, gather and provide information as requested.

dd) Analysis and supervision of incident-related issues

The National Coordination Center shall take charge and cooperate with the managing body of the information system to conduct continuous supervision of incident developments and send notices thereof to the members of the Emergency Response Operations Division.

Members of the Emergency Response Operations Division shall base on obtained information, resources and facilities and adopt operational procedures to analyze the incident. Results of the analysis of incident shall be reported to the Standing Committee and the National Coordination Center, and shared among members of the Emergency Response Operations Division so as to effectively handle the incident.

e) Handling of incident and malware removal

Unit in charge: The managing body of the information system

Coordinating units: The National Coordination Center, other members of the Emergency Response Operations Division. Working contents:

- Back up the system prior to and after implementing actions to handle the incident;

- Delete malcode or malware;

- Restore the system, data and connections;

- Configure security systems;

- Test the entire system after completing incident response actions;

- Handle information security vulnerabilities;

- Supplement or replace equipment, hardware and software to ensure information security of the system;

- Monitor, supervise and prevent the incident or similar incidents from occurring in the future.

g) Prevention and handling of impacts

The managing body of the information system is responsible for handling the negative impacts of the incident on the people, and other authorities and organizations.

Based on results of analysis of the incident, members of the Emergency Response Operations Division shall use their available resources, facilities and operational techniques to prevent acts that may cause security incidents and assist in handling impacts of the incident.

h) Finding out and verifying the causes of incident

After completing the analysis of incident or consulting results of analysis of incident provided by other units, members of the Emergency Response Operations Division shall take advantage of available information and implement their operational procedures to find out the root causes of the incident, and send report thereof to the Standing Committee/ the National Coordination Center so as to verify and send consolidated report thereof to the NSC with the following contents:

- Targets of security attacks;

- Attack methods/ strategies (processes, techniques, malcode or malware);

- Time of attack;

- Damage suffered;

- Attackers;

- Predicted similar attack activities and potential damage.

6. Assessing results of the emergency response plan to ensure national cyberinformation security

Unit in charge: The National Steering Committee (NSC)

Working contents: The Standing Committee shall consolidate reports on analytical activities relating the emergency response plan to ensure national cyberinformation security so as to report to the NSC and organize a meeting for analyzing the causes of the incident and learning experience in incident response and propose appropriate measures for dealing with similar incidents.

7. Finalization of response actions

Unit in charge: The National Coordination Center

Coordinating units: The managing body of the information system, and members of the Emergency Response Operations Division. Working contents: The National Coordination Center shall base on the assessment results of the NSC to fulfill the following duties and finalize the emergency response actions:

- Store relevant documents and records;

- Prepare teachings of experience;

- Propose recommendations on techniques and/or policies to minimize damage caused by similar attack activities;

- Send reports to the authorities of higher level, organize press conferences or provide information to mass media agencies, where necessary.

Chapter IV

MEASURES TO ENSURE THE IMLEMENTATION OF RESPONSE ACTIONS AGAINST NATIONAL CYBERINFORMATION SECURITY INCIDENTS

Article 15. Requisition of property and suspension of operation of means of communication to serve emergency response to national cyberinformation security incidents

In course of implementation of the emergency response plan to ensure national cyberinformation security and at the request of the Standing Committee, regulatory authorities shall, within the competence prescribed by law, discharge the following duties:

1. Postpone or suspend the operation of electronic forms of contract or other activities originated from the information system when these activities are determined to cause extremely serious harms to the public interests or serious harms or extremely serious harms to the national defense and security.

2. Requisition means of communications, means of transport and other means as well as the users or operators of such means in emergency cases so as to fulfill emergency response tasks or prevent harms or potential harms to the society.

3. Mobilize resources within the scope of their management to conduct incident response actions.

Article 16. Formulation and implementation of response plans to cyberinformation security incidents

1. Agencies and units shall formulate and implement response plans to cyberinformation security incidents (hereinafter referred to as the "incident response plan") to ensure human, material and financial resources and other necessary conditions to implement such incident response plans. To be specific:

a) The National Coordination Center shall formulate and submit the incident response plan to ensure national cyberinformation security and the operating plan of the Incident Response Network to the Ministry of Information and Communications for approval.

b) Specialized incident response units of ministries or central-level agencies shall formulate and submit incident response plans to ensure cyberinformation security for information systems of state agencies, political organizations or socio-political organizations within the scope of their management to the heads of managing bodies of such information systems for approval.

c) Specialized incident response units affiliated to People's Committees of provinces or central-affiliated cities shall formulate and submit incident response plans to ensure local cyberinformation security to Chairpersons of Provincial-level People's Committees for approval.

d) Members of the Incident Response Network, organizations or enterprises managing the information systems on the List of national information systems, large-scale information systems or SCADA systems shall formulate, approve and implement incident response plans to ensure cyberinformation security for their information systems.

2. Relevant agencies and units shall formulate incident response plans to ensure cyberinformation security according to the outlines provided in the Appendix II herein with paying special importance to the following contents: Attack scenarios, risks and incidents that might occur, response plans according to attack scenarios, estimated circumstances and training activities. Where necessary, Ministry of Information and Communications shall consider adjusting certain contents of the outlines in conformity with the actual situation and requirements for response to cyberinformation security incidents.

3. The National Coordination Center shall instruct the formulation and implementation of incident response plans and backup plans for responding or handling cyberinformation security incidents; organize training or drilling activities on the regional, national and international scale; conduct regular inspection and assessment of the implementation of incident response plans by ministries, local governments and organizations/ enterprises.

Article 17. Funding

1. Funding for implementing coordination, response and recovery plans against cyberinformation security incidents is provided by: The central-government budget, local-government budgets, budget of enterprises and other legal sources of funding as regulated by law.

2. Funding for conducting response actions against cyberinformation security incidents is included in the estimates of state budget expenditures of ministries, central-level agencies and local governments (including development investment expenditure and recurrent expenditure), managed, used and recorded into accounts according to state budget levels as prescribed in the Law on State Budget and its instructional documents. Funding shall be allocated according to the following principles: Regulatory authorities shall their own sources of funding to cover expenditures for their activities or personnel. To be specific:

a) The central-government budget shall allocating funding for:

- The activities of directing, managing and inspecting incident response actions of the NSC, the National Coordination Center and the National Standing Committee;

- Funding for activities of the National Coordination Center consists of: Funding for performing relevant activities within the scope of responsibility of the National Coordination Center as prescribed in Articles 7, 11, 12, 13, 14 and 16 herein; funding for ensuring regular operations; detecting and warning activities; training and drilling activities; purchasing, upgrading and extending software copyright, equipment, facilities and tools for performing international cooperation for cyber security; funding for formulating and implementing incident response plans; provisions for responding to national serious incidents; funding for assisting ministries and local governments in coordinating and handling incidents; funding for hiring technical services, organizing and maintaining operation of incident response specialists team and incident response operations division; funding for managing and organizing operation of the Incident Response Network; disseminating, training, organizing conferences of the network, doing specialized research and maintaining technical specialists team, improving and developing operation of incident response teams; funding for inspecting, scanning and assessing information security; collecting, analyzing and sharing incident-related information; assisting in formulation and application of ISO 27xxx standards and international standards on cyberinformation security; performing specific operations to ensure cyberinformation security for the important information systems of the Government;

- Ministries and central-level agencies shall, pursuant to regulations herein, prepare annual estimates of expenditures for performing relevant activities within the scope of their management as prescribed in Articles 7, 11, 12, 13, 14 and 16 herein; funding for formulating and

implementing their incident response plans; provisions for responding or handling incidents occurring on the information systems under their management; funding for training and drilling activities, and operations of the incident response teams; funding for monitoring, supervising, scanning and assessing the information security; funding for assisting in formulation and application of ISO 27xxx standards and performing specific operations to ensure cyberinformation security for the information systems under their management.

b) Local-government budget shall provide funding for activities of the Steering Board, specialized incident response units and local incident response teams, consisting of: Funding for performing relevant activities under the management of local governments as prescribed in Articles 7, 11, 12, 13, 14 and 16 herein; funding for implementing local incident response plans; provisions for responding or handling incidents occurring on the information systems under the management of local governments; funding for training and drilling activities, and operations of the local incident response teams; funding for monitoring, supervising, scanning and assessing the information security; funding for assisting in formulation and application of ISO 27xxx standards and performing specific operations to ensure cyberinformation security for the information systems under their management.

c) Enterprises shall provide funding for performing relevant activities within the scope of their management as prescribed in Clause 4 Article 7, Articles 11, 12, 13, 14 and 16 herein; funding for implementing enterprises' incident response plans and backup plans for response to incidents attacking the information systems under their management; supervision activities, providing information and participating in incident response plans; organizing training and drilling activities and maintaining operations of incident response teams and other duties assigned to enterprises. These spending items may be accounted as the enterprises' business expenses. Telecommunications enterprises and Internet Service Providers must arrange funding for monitoring and handling incidents to ensure cyberinformation security on their Internet connections and may aggregate this funding into their business expenses.

d) The managing bodies of information systems must arrange funding for implementing incident response plans as well as backup plans for handling incidents, remedying impacts, restoring data and continuing normal operations of their information systems.

dd) The Vietnam Public-utility Telecommunication Service Fund (VTF) shall provide funding for performing coordination or response actions to ensure cyberinformation security, which are not supported or partially supported by state budget, including operations of the National Coordination Center, incident response operations divisions convened by the Standing Committee, operations of the national incident response network, hiring technical services, organizing and maintaining incident response specialists teams affiliated to the National Coordination Center, covering losses of telecommunications enterprises or Internet Service Providers from the handling, prevention or response to national serious incidents, and other relevant activities which are not supported or partially supported by state budget.

e) Ministry of Finance shall take charge and cooperate with Ministry of Information and Communications in instructing allocation of funding for performing the activities of coordination and response to ensure cyberinformation security in accordance with regulations of this Article.

Chapter V

IMPLEMENTATION

Article 18. Entry into force

This Decision shall come into force as from the date on which it is signed.

Article 19. Organization of implementation

Ministries, ministerial-level agencies, central-level agencies, People's Committees of provinces or central-affiliated cities, and relevant organizations shall implement this Decision.

Difficulties that arise during the implementation of this Decision and require amendments to this Decision should be reported to the Ministry of Information and Communications so as to submit a consolidated report to the Prime Minister for consideration./.

THE PRIME MINISTER

Nguyen Xuan Phuc