# Guidelines for National Critical Infrastructure Protection

Promulgated December 29th, 2014

Revised May 18th, 2018

# Table of contents

Chapter 1 General Provisions ..... 3
Section 1 Origin ..... 3
Section 2 Definitions ..... 3
Section 3 Strategies ..... 5
Section 4 Goals ..... 6
Chapter 2 Mission ..... 7
Section 1 Office of Homeland Security ..... 7
Section 2 Competent authority ..... 7
Section 3 Coordinating authority ..... 8
Section 4 National Critical Infrastructure Providers ..... 9
Section 5 Collaborating units for security protection ..... 10
Chapter 3 Security protection management fundamentals ..... 11
Section 1 Set security goals ..... 12
Section 2 Inventory and classification ..... 12
Section 3 Risk assessment ..... 15
Section 4 Determine protection priorities ..... 16
Section 5 Implement protection plans ..... 17
Section 6 Assess implementation effectiveness ..... 17
Chapter 4 Supporting measures ..... 19
Section 1 Classified and sensitive information/Confidentiality requirement ..... 19
Section 2 Notifications, warnings, and press releases ..... 20
Section 3 Partnership with private sectors ..... 21
Section 4 Research and development ..... 22
Annex 1 Sector classification for national critical infrastructure ..... 23
Annex 2 Notice on national critical infrastructure inventory check ..... 23
Annex 3 Security protection plan framework for national critical infrastructures ..... 23

# Chapter 1 General Provisions

## Section 1 Origin

The revision of these Guidelines is based on the resolution passed by the Homeland Security Policy Committee and the Homeland Security Task Meeting in 2013, which demanded the development of critical infrastructure protection plans to strengthen the security protection functions of national critical infrastructure and ensure citizens' safety and interests. In carrying out this revision, the following regulations and acts have been referred to：

I. Provisions for the Establishment and Operations of Homeland Security Policy Committee
II. Operation Direction on Central Emergency Operation Center
III. Guidelines for Contingency Response Plans and Operations of Homeland Security
IV. Operation Guidance Regulations on National Information and Communication Security Notification Response
V. Operation Directions on Homeland Security Contingency Notification
VI. Information and Communication Security Management Act

## Section 2 Definitions

I. National Critical Infrastructure (hereinafter abbreviated as CI): Assets, production systems, and networks- public or private, physical or virtual- that, if disrupted by humans or natural disasters, may negatively impact the proper functioning of the government and society, cause casualties among citizens, bring property losses, inflict economic downturn, bring about environmental changes, or can potentially damage national security or national interests.
II. Critical Information Infrastructure (CII): Vital information and communication systems or supervisory control and data acquisition (SCADA) that deals with core task functions and supports the continuous operation of national critical infrastructures. CII is also a vital component of national critical infrastructures (information category asset) and shall be managed under a single authority according to the CI to which it belongs.

III. Classification: The national CI is classified as a three-level structure, where the first level is called a sector, the second level a sub-sector, and the third level the vital functional facilities and systems that fall under the sub-sector.[1]
    1. Sector: Categorized into eight primary sectors based on functions and attributes. The eight sectors are energy, water resources, telecommunications, transportation, finance, emergency rescue and hospitals, administration and agencies, and science and industrial parks.
    2. Sub-sector: Further categorized under each sector in accordance with functions and tasks. For example, the energy sector is subdivided into electricity, petroleum, and natural gas sub-sectors.
    3. Functional facilities and systems: These are the facilities and equipment, transferring networks, information and telecommunications systems, control systems, command and management systems, security maintenance systems, and critical technologies necessary to ensure the continuous operation of the sub-sectors' vital functions and tasks.

IV. The Executive Yuan's National Critical Infrastructure Security Protection Task Team: Members of this team include experts, scholars, and representatives from coordinating agencies in all sectors invited by the Executive Yuan's Office of Homeland Security (OHS). The team communicates and coordinates on annual tasks, education and trainings, drill projects, and revisions to the Guidelines for National Critical Infrastructure Protection and its appendices. Significant measures must be submitted to the Homeland Security Policy Committee for approval.[2]

V. Coordinating authority[3]：In general, each sector shall establish one authority to be responsible for coordinating the various competent authorities within its sub-sectors in order to achieve resource and information sharing and develop common standards for risk management.

VI. Competent authority[4]：A competent authority is defined as a central authority or municipality or county (city) government directly responsible for, or supporting all or part of, a sub-sector.

VII. National critical infrastructure provider (hereinafter referred to as provider)[5]： An entity that is appointed by the central authority from the related sector and approved by the Executive Yuan to maintain or

[1] Refer to Appendix 1: "Sector Classification for National Critical Infrastructure"
[2] Refer to Chapter 2, Section 1.
[3] Refer to Chapter 2, Section 3.
[4] Refer to Chapter 2, Section 2.
[5] Refer to Chapter 2, Section 4.

provide all or part of the critical infrastructure.

VIII. All-hazard: Hazards that include natural disasters, information security attacks, accidents, artificial disasters, non-conventional attacks, and military threats. All-hazard is the primary basis for identifying the risks and threats to any critical infrastructure.

IX. Resilience: Capability to reduce the degree and duration of impact caused by an incident that suspends functions. The effectiveness of critical infrastructure resilience relies on anticipation, tolerance, adaptation, and speedy recovery in incidents that suspend functions.

X. Interdependency: A relationship between critical infrastructures characterized by mutual dependency and functioning. For example, the failure of a facility's core function will start a chain reaction that makes other facilities cease operation.

## Section 3 Strategies

To achieve CI security protection targets, a risk management procedure is adopted based on the following implementation strategies:

I. Implement CI risk management based on all-hazard protection.

CI security protection shall be based on "all-hazard" protection, which requires both internal and external risk identification of facilities and the blending of risk management and continuous management methods into national critical infrastructure security protection tasks.

II. Develop response tactics and strategies, as well as develop security protection plans on all levels.

To effectively implement CI security protection tasks, a comprehensive and systematic inventory and review of facilities must be performed. Therefore, facilities are classified and managed according to level of importance, and a complete national infrastructure database is created and updated regularly. All management levels for all facilities must be aware of the interdependency between facilities and the impact of such relationship no longer being effective. Management shall also research and develop definite, viable security protection plans based on response tactics and strategies within its jurisdiction on the following four levels: anticipation, preparation, protection, and recovery.

III. Strengthen collaboration and joint defense between sectors and create an information-sharing mechanism.

The competent authorities of all sectors and sub-sectors shall build and strengthen cross-sector joint defense mechanisms between the

interior and exterior units, as well as between central and local government, by working with providers of CI. The authorities should also actively promote cooperation between the public and private sectors and encourage private sector participation. Cross-domain, cross-public and private sectors should share risk information, and a threat-warning and security protection information sharing platform should be established to improve the information sharing mechanism and the integrity of CI security protection.

IV. Effectively prepare and organize security protection resources and enhance continuous functioning capabilities.

Competent authorities and CI providers for all sectors and sub-sectors shall proactively coordinate resources and support to prepare security protection that effectively ensures CIs and assets security. A contingency plan must be established to reduce the impact caused by a sudden suspension of facilities' functions. The relevant authorities shall also establish contingency plans and seek to reduce the impact of facilities' suspension of operations. Doing so will ensure the government's continuous functioning capabilities and safeguard people's lives, properties, and wellbeing, as well as homeland and national security.

## Section 4 Goals

The goals of CI protection (CIP) are:

I. To enable vital functions of the nation and society to continue functioning and ensure the security of infrastructures and assets related to national security, governance, public security, the economy, and public confidence.

II. To be aware of the inter-dependency between facilities based on all-hazard security protection considerations, identify the potential risks and impacts of hazards, reduce facilities' vulnerabilities, minimize the scope and degree of impact from the loss of facilities' effectiveness, increase response efficiency, and speed up recovery.

III. To facilitate partnerships by establishing a sound, cross-sector, public-private collaboration and information-sharing network to perform defense and security protection measures on physical, cyber, and human levels in order to prevent and handle the impact of all sorts of hazards. The security and resilience of facilities also need to be enhanced.

# Chapter 2 The Mission

## Section 1 Office of Homeland Security

The Office of Homeland Security (OHS) acts as a supporting staff office to the Homeland Security Policy Committee and implements resolutions on "CI security protection" issues passed by the committee after consultation and deliberation. The office is responsible for planning the overall direction and missions, as well as supervising, inspecting, and coordinating security protection goals between various sectors. It also promotes missions, gathers resources, and supports educational trainings and drills at all facilities.

To integrate the implementation of CI security protection, the OHS convenes project team meetings with all related ministries and units on CI security protection. Its primary objectives are as follows:

I. To research and draft policies and laws related to CI security protection.
II. To research and draft risk management and early warning systems related to CI security protection.
III. To research and draft measures and emergency responses related to CI security protection.
IV. To coordinate and liaise between all intelligence and policing ministries in order to maintain the order of CI security protection.
V. To handle integrated supervision, coordination, and support measures related to CI security protection.
VI. To collect and process information related to CI security protection.
VII. To perform other measures, drills, and trainings related to CI security protection.

## Section 2 Competent authority

I. Senior personnel, or chiefs, familiar with facilities in the sub-sectors shall form project teams, convene cross-departmental project meetings, and install or appoint dedicated organization and personnel to be responsible for administrative and advisory tasks. These chiefs shall inventory and review all possible vital assets and facilities within the organization's jurisdiction and determine inventory targets and division of labor. They shall also draft budgets and resources that can be used to support tasks related to security protection and

management. Lastly, they shall implement a merit system.

II. The competent authority shall supervise facilities within its jurisdiction and perform inventory reviews on CIs. Furthermore, it shall categorize its facilities into various levels, compile CI data in the sub-sectors, prioritize security protections, and submit plans for a comprehensive assessment to be carried out at the sector level.

III. Competent authorities shall support, mentor, and approve risk assessments on national infrastructures of all levels. They shall also draft a "CI security protection plan" and submit it to the sector's coordinating ministry.

IV. Competent authorities are responsible for supervising, inspecting, and assessing national CI providers, as well as providing them with assistance, when they implement security protection measures and trainings and drills.

V. Competent authorities shall encourage the research and development of cost-effective technologies and equipment related to security protection and anti-disaster resilience.

VI. Competent authorities shall compile data of facility providers based on the actual demand of military task forces before the end of April each year and submit such data to the Ministry of National Defense for application.

## Section 3 Coordinating authority

I. In the case that a sector has many sub-sectors and each sub-sector has more than one competent authority, the attributes and core functions of such sectors must be considered under the "Principles on Appointment of Central Competent Authority for Certain Tasks." These principles can be found in the Executive Yuan's Guidelines for Contingency Response Plans and Operations of Homeland Security and must be referred to before appointing an agency whose tasks are closest to the core functions as the coordinating authority for that sector. (For example, certain transportation sector has several competent authorities, including the Ministry of National Defense, Ministry of Transportation, Council of Agriculture, and local governments; in this case, since the core function and attributes of the Ministry of Transportation is closest to the sector of transportation, it shall become both the competent authority and the coordinating authority of such sector. Likewise, the National Communications Commission would oversee the sector for telecommunications.)

II. Each coordinating authority shall appoint deputy chief-level officials to act as the convener and install or appoint ad hoc organization and

related personnel to serve as administrative advisors. Furthermore, the authority needs to invite cross-sub-sector ministries to create coordinating teams that will hold regular meetings to discuss drafting risk management standards, classifying facilities, approving plans, promoting drills and trainings, using resources, exchanging information, and mutual support related to the indicated sectors.

III. Coordinating authorities shall compile the protection plans submitted by the competent authorities of the sub-sectors and comprehensively analyze them prior to drafting a sector-level security protection plan.[6] This sector-level security protection plan, along with the level-one CI protection plan, shall be sent to the OHS as a notification.

IV. Sector-level security protection plans shall include a general overview of the status, visions, goals, risk assessments, prioritizations, security protection action plans, and implementation measures. The plans shall further include management and coordination concerning legal levels, between systems, constructing public-private collaboration, and assistance for achieving efficient information sharing between sectors, as well as horizontal and vertical notification systems, drills, and educational training.

V. Coordinating authorities shall assist all levels of national CIs to establish a mutual support and cooperative defense system with related ministries and local governments and promote the use of security maintenance and disaster resilience technologies and equipment.

VI. Coordinating authorities shall establish audit frequencies based on the importance of national CIs and collaborate with competent authorities and local governments at sub-sectors to implement protection drills before a review of results and make subsequent improvement recommendations.

VII. The authority shall establish a Computer Emergency Response Team (CERT), Information Sharing and Analysis Center (ISAC), and Security Operation Center (SOC).

## Section 4 National Critical Infrastructure Providers

To ensure that the CI maintains security and the continuous functioning of its core competencies, the head of each provider shall

[6] Also known as Sector-Specific Plan (SSP). Please refer to the plans submitted for all sectors (departments) from the commissioned research cases done for the Executive Yuan's CI security protection services (2010-2013). However, note that these results were intended for the system in place prior to implementing the national CI protection system; therefore, some revisions and modifications may be required based on the national CIs that are inventoried and the practical experience obtained after 2013.

appoint a deputy chief or appropriate personnel to simultaneously act as the convener. He/she shall invite personnel responsible for security maintenance, administration, human resources, accounting, general management, and security protection, as well as external collaborating units, to hold project meetings, where he/she shall designate ad hoc organizations and personnel to promote and supervise security protection affairs. He/she shall also allocate funds, make plans, promote drills and educational training, and conduct systematic and continuous research on maintaining facilities' continuous functioning and security. Its primary objectives are as follows:

I. Regularly assess risks, threats, and vulnerabilities. Draft a "CI security protection plan" and submit it to the competent authority for compilation. Regular checks on the effectiveness of actual implementation shall also be performed.
II. Establish horizontal and vertical notification systems and enhance the efficiency of information sharing across sectors.
III. Establish a warning system that warns the public in times of crisis or emergencies.
IV. Work with local governments to carry out protective drills improve protective measures based on feedback from reviews, and revise protection plans.
V. With the core tasks of the facilities as the foundation, establish support protocol related to the professional assistance and support needed in times of crisis and threats from disasters. A detailed list of contact personnel shall be regularly updated.

## Section 5 Collaborating units for security protection

Collaborating security protection units shall stay in close contact with CI providers during regular times and engage in training sessions and drills so that they can assist in response and recovery tasks in case of emergency.

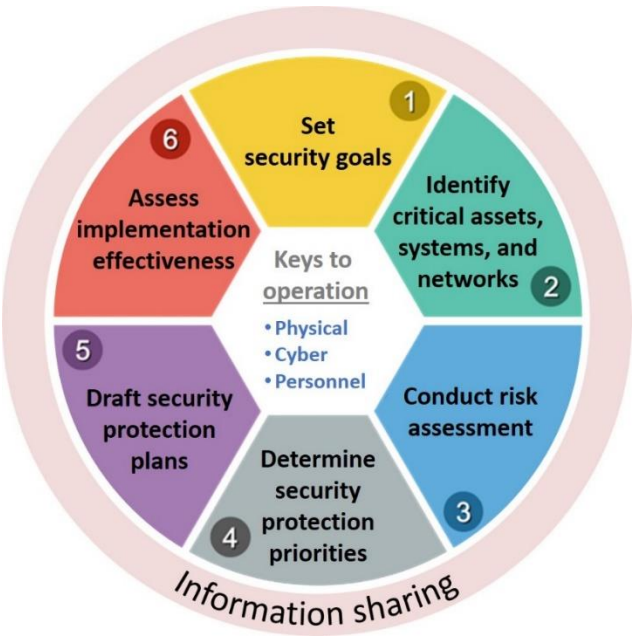
I. Municipalities and counties (cities) shall provide support and assistance in accordance with the demands of the Office of Homeland Security, competent authorities, and CI providers when CIs suffer or are likely to suffer damage. However, in times of major hazards and disasters, municipalities and counties (cities) shall provide proactive assistance.
II. All competent authorities shall assess risks and compile the needs of the infrastructure providers under their jurisdiction. If a military task force is needed, an application for such support shall be submitted to

the Ministry of National Defense before the end of April each year. During times of war or emergency (such as major disasters), military task forces can support public administrative agencies' emergency response and support local security, self-defense, and anti-air attacks in order to meet citizens' basic living demands. Such support shall not affect predetermined military missions.

III. Competent authorities can apply for national military support if an emergency response demands it. However, during times of major hazards and disasters, the national military can proactively provide hazard rescue assistance without being requested to do so.

# Chapter 3 Security protection management fundamentals

Tasks at various stages of security protection management for CIs shall follow the circular steps of "Plan, Do, Check, Action" to ensure not only consistency between goals, plans, and actions, but also implementation effectiveness. Competent authorities shall implement correct actions through planning, training, and assessment and shall teach senior managers and personnel continuous operation concepts. Such individuals shall also learn about the duties and objectives related to implementing continuous operation management plans. Through testing, drills, and objective assessment, CI protection plans, procedures, and training can be revised based on feedback. They will be able to set priorities, allocate funds, and promote improvement plans and procedures. The fundamentals of such promotion include the following:



## Section 1 Set security goals

To achieve CI security protection goals, as described in Chapter 1, all coordinating authorities of each sector shall discuss and research protection management goals and priorities with their sub-sector's competent authorities. If the risk assessment results show that collaborations with other government partners and with private sectors are beneficial to achieving the guidelines' goals, then a specific plan on the viability of collaboration shall be drafted and implemented.

All competent authorities and CI providers at the sub-sector level must follow the protection management goals and priorities required by the sectors to which they belong. They must set security goals and priorities for CIs based on the core functions, risks, environment, and collectable resources.

I. Support and respect from agency chiefs
   The heads of each sub-sector competent authorities shall supervise the security protection management policies and implementation performance of CIs. They shall also set such security protection and continuous functioning goals as major inspection and review targets.
II. Establish dedicated promotion teams
   CI inventories, reviews, risk assessments, protection, and drills shall be performed across ministries and agencies through coordination and collaboration. Therefore, dedicated promotion teams shall be convened and established by senior chiefs.
III. Announce security protection task goals
   All sub-sector competent authorities shall announce security protection goals and implementation and promotion strategies to the CI providers within their jurisdiction. They shall also explain the risk items, management policies, and continuous operation targets and plans. They shall announce drafted task items pursuant to this guideline.

## Section 2 Inventory and classification

Inventorying a CI means having a proper understanding of the vital nodes, assets, facilities, and systematic networks that affect national security, government, and society. Understanding the inter-dependency within sectors and across sectors also helps to lower the probability that a complex hazard may occur. Therefore, an importance assessment on facilities' systematic functions, the value of facilities and assets, and the

impact of ineffectiveness shall be carried out, and classification management based on the results of such importance assessments.

The sub-sector competent authorities shall first make a list of assets based on the core functions and missions of each authority before sorting out the vital nodes that are important or can cover the authorities' functions or missions, such as buildings, physical (non-virtual) facilities, information systems, telecommunications equipment, and technology and human resources; these nodes shall then be organized into an infrastructure candidate list (including facility providers).

Next, the infrastructure providers on that list shall survey the unit's core tasks, internal assets, and external resources to assess their importance and fill out the "CI basic data survey form"[7] before submitting it to the sub-sector competent authorities for further compilation. The competent authorities shall then convene project meetings to review and deliberate on such data survey lists, prioritize importance, and consult relevant public administrative agencies, civil groups, and experts/professionals for their opinions before finally proposing a preliminary classification recommendation. This will then be submitted to the OHS, which will convene another expert team to hold a review meeting to make a final decision on the classification. Based on that meeting's result, a "CI database" will be created. The procedure for such is as follows:

I. Facility providers shall fill out the "CI basic data survey form".
   With the goal of maintaining core functions, facility providers shall perform necessary inventory checks on nodes, assets, facilities, and systematic networks according to the attributes of functions, tasks, and scopes. The content of the facility inventory and investigation report shall include:
   1. Core function tasks: identify core function tasks, their tolerable discontinuity duration (Recovery Time Objective), and options for continuous operation (Recovery Point Objective).
   2. External critical resources: perform inventory checks on external critical resources and their providers that support core function operations. Furthermore, perform inventory checks on the backup plans and backup time in the case of critical external resources failure.
   3. Internal necessary assets: Perform inventory checks on the necessary assets that support core function operations based on 3 categories - physical necessities, personnel (critical technologies, leadership), and information telecommunications. Moreover, perform inventory checks on the backup plans and maximum

[7]The "National Critical Infrastructure Basic Data Survey Form" shall be provided by the Executive Yuan's Office of Homeland Security. Please also refer to the "Notice on National Critical Infrastructure Inventory Check" in Appendix 2.

backup times for each category. For example, if sabotage or destruction from hazards in the information and telecommunication category has been determined to affect core function tasks and no other temporary alternatives are available, then they shall be listed as information telecommunication assets within the critical infrastructure.

4. Importance self-assessment by facility providers: Analyze the possibility of impact from facility failure on the functions of CIs in other sectors. The importance assessment shall include the following items:
   (1) Demographic impact: Whether an incident or disaster of the facility may cause significant casualties or emergency fleeing.
   (2) Importance on government and social functions: Assess the importance of said facility in supporting the proper government and social functions, such as the command and management of government agencies, information and telecommunications functions, life maintenance and transportation functions, national financial order, health and disease system, security and disaster prevention/rescue, national vital symbols and assets, critical technologies and industries, and defense and mobilization.
   (3) Economic impact from an ineffective facility: This includes total facility value, number of people impacted by the ineffectiveness, and any economic losses.
   (4) Impact on public morale from facility failure: Assess the degree of impact on international image, government prestige, and public confidence due to facility failure.

II. Preliminary classification assessment to be carried out by sub-sector competent authorities

Sub-sector competent authorities shall compile the facility survey forms submitted by the facility providers within their jurisdiction and review the content to ensure their correctness and comprehensiveness. They shall prioritize facilities with the same attributes into “level one, level two, and level three” categories, make facility inventory books for all categories, and provide reasons for such classifications. Competent authorities shall then consult related government agencies, civil groups, and experts/professionals for their opinions before submitting the aforementioned survey form to the OHS.

III. Joint review by the OHS

The OHS shall convene the National Security Council, the National

Security Bureau, coordinating authorities, the Ministry of National Defense, relevant ministries, and private sector organizations to jointly review the facility lists of the aforementioned facilities at all levels, the reasons for their classification, and the appropriateness of the survey forms. Furthermore, they need to check whether critical facilities have been omitted and deliberate based on all kinds of data to make final decisions on the CI list and classification.

## Section 3 Risk assessment

The partners of CIs, including facility providers, competent authorities, coordinating authorities, and the OHS shall all assess risks based on a series of risk assessment methods including aspects on threats, vulnerability, and impact consequences. Such risk assessments must enable leaders and decision-makers to have a sufficient understanding of the most likely and most serious incidents that may affect proper functioning, so that they can draw further support and coordinate resources to revise protection plans based on such assessment's results and information.

To obtain reliable, operable, and timely risk information, coordinating authorities shall coordinate competent authorities and CI providers to seek scientific and technological support in the development or usage of products to assess related threats, vulnerability, and potential consequences.

The CI risk assessment shall identify the threats, scenarios, degree levels, and possibility of occurrence of impact on core functions based on the concept of all-hazards. Assessment on the degree of damage (fragility) and recovery time of necessary assets, resources, and backups under different threat levels shall also be carried out, and the degree of protection and backup capacity under various threats should be analyzed.

I. Threat identification
   1. National level: National threat scenarios that have a low probability of occurrence but are likely to cause massive CI failures, disrupt government and social functions, and seriously impact homeland security if they occur.
   2. Sector level: Based on the national level of threat scenario, assess the attributes, environment, scope, and latest trends of the core functions within the sector. Furthermore, identify the internal and external hazard threat scenarios that may disrupt tasks at the sector level.
   3. Facility level: Identify internal and external hazard threats that may disrupt facility operation, first on national-level and then sector-level threat scenarios, followed by location and environment, space

scope, and facility attributes.

II. Impact assessment
    1. National level: Establish various national hazard impact scenarios based on the degree of impact and recovery time from national-level hazard and threats on CIs.
    2. Sector level: Assess the degree of impact and recovery time of various CIs, critical external resources, and backup strategies within the sector. Assess the impact from disruption of the sector's core functions and tasks.
    3. Facility level: Assess the degree of impact and recovery time on various necessary internal assets, critical external resources, and backup facilities based on the location and environment, space scope, and facility attributes. Further assess the impact on the disruption of facility functions.

## Section 4 Determine protection priorities

I. CI providers shall prioritize actions to manage facilities according to the importance of facilities, the costs and expenditures of protective actions, and the possibility of lowering risks.
II. Coordinating authorities shall coordinate available protective resources to draft sector protection plans based on the sector environment and attributes, as well as a facility list that demands priority protection under certain risks at the sector level.
III. The OHS shall establish a CI list that requires priority protection from specific risks at the national level based on the importance of CI and risk assessment results. The list shall then be used as a protection strategy and serve as the foundation for the overall allocation of protective resources.
IV. The CI classification list is essential in allowing central control of limited protective resources at normal times and ensures that important functions do not fail when disasters occur. Nevertheless, other important facilities that are not listed shall still conduct voluntary risk management and foster recovery capabilities in disaster periods.
V. In times of military crisis, national security units shall assist in maintaining vigilance and protecting CIs deemed critical for warfare. Sub-sector competent authorities shall support such actions to adjust protective resources and ensure the proper functioning of facilities during military crises.

## Section 5 Implement protection plans

I. Based on the risk assessment results, the CI providers shall determine whether security protection goals and recovery times are satisfied and prioritize risk-lowering and protection-strengthening tasks according to the possibility of threats occurring, as well as the degree of impact on facilities. Providers shall also regularly review and revise security protection plans.

II. The objectives of the protection plans are:
    1. To ensure sustainable and stable protection of CIs with regard to physical, information and telecommunications, and personnel aspects.
    2. To plan necessary actions in normal times and emergencies based on the all-hazard concept. Actions shall include early warning, response, and recovery and reconstruction stages.
    3. To coordinate and allocate responsibilities and resources between partners according to the inter-dependency and level of substitution between facilities.
    4. To effectively utilize resources to establish disaster resilience and maximize the reduction and mitigation of risks and threats.

III. Protection plans shall include an overview of the CI, including an assessment on the facilities' locations, warning systems, human resource allocation, contact methods, internal and external rescue resources (fire rescue and emergency rescue planning), notification and response mechanisms, recovery goals and procedures, and drill methods.[8]

## Section 6 Assess implementation effectiveness

The effectiveness of risk management tasks on CI protection shall be assessed based on the sector system concept, partnership function collaboration, risk assessment, training exercises and drills, and actual hazard responses. The results of such assessments shall be used for further review and improvement.

### I. Drills and educational training

[8] Please refer to the "national critical infrastructure security protection plan structure" in Annex 4. Furthermore, according to Chapter 2, Section 3 of these guidance regulations, sector coordinating authorities shall compile a security protection plan for the national critical infrastructures within the sector to draft additional sector security plans.

1. The OHS, coordinating authorities, and competent authorities shall provide resources and necessary measures to promote the concept of security protection management for CIs and shall carry out staff educational training on risk management, continuous operation and management, drills and training, and audits. Such agencies and authorities shall assist CI providers in establishing professional skills related to risk management and response to enhance risk management and response capabilities.[9]
2. To verify whether the identified risks can be effectively controlled, as well as the protection plans are effective in reducing hazard losses and shortening recovery time, all competent authorities shall supervise facility providers to hold drills or support anti-hazard and information security drills.
3. Drill methods can include a combination of table-top exercises (issue exploration and situation simulation), war games (hypothetical situation responses), or full-scale exercises (drills conducted in the field with real objects and live actions based on war game details). All drills may involve and integrate related agencies/parties.
4. Plans shall be made before drills take place and shall hold coordinating meetings to explain the details. Drill procedures shall be accurately recorded in detail, including drill methods, time, location, purpose, personnel list, judges and their review opinions, and any correctional and preventive measures. These records will serve as a reference for future drafting and revisions of protection plans.
5. Failure drill items deemed as requiring further improvements during such drills shall be prioritized in training courses.
6. The utmost emphasis of all sub-sector competent authorities' educational training shall be learning effectiveness and providing feedback to the CI protection system. Agencies or individuals shall be rewarded with incentives as appropriate.
7. Based on the classification results, OHS shall consider the current state of affairs and the environment before choosing vital CIs and recommending that the Homeland Security Policy Committee incorporate such CIs into the annual homeland security drill. OHS shall also require that agencies for the selected CIs submit detailed risk assessments and drill plans.

## II. Audit and rewards

1. The OHS has the authority to invite experts and scholars to draft a

[9] Please refer to the "National Critical Infrastructure Protection Drill Manual" for details on drill preparation and implementation.

review list to support the Office of Disaster Management's disaster prevention and rescue visiting assessment projects, the Department of Cyber Security's security audit on the government's administrative agencies, or the Directorate-General of Budget, Accounting and Statistics' audit of internal control systems. The review list shall then be incorporated into all agencies' internal control systems. Furthermore, the OHS has the authority to visit all agencies to check on the risk management and contingency plan implementation status of the CIs. All agencies shall perform reviews based on this list prior to the visit from the OHS. They are required to incorporate the security protection status of such facilities into their own internal audits.

2. The OHS shall review and audit sector-level security protection plans and tasks undertaken by sector-level coordinating agencies. Level-one CIs' security protection plans shall be submitted to the Executive Yuan for approval and reference and shall serve as options for the EY's annually appointed drills. Level-two CIs' security plans shall be submitted to the competent authorities for approval and reference. The competent authorities shall then carry out annually appointed drills on level-two CIs, as well as requesting a visit from the OHS. Level-three CIs' security protection plans shall be submitted to the competent authorities for approval and reference. Security protection drills shall be carried out by the agencies and units responsible for their own infrastructures; competent authorities on the sub-sector level shall make on-site visits to review the drills.
3. The annual drill's assessment results shall be submitted to the Homeland Security Policy Committee, which will make recommendations regarding rewarding well-performing agencies.

# Chapter 4 Supporting measures

## Section 1 Classified and sensitive information/ confidentiality requirement

I. In response to a reasonable range of requests, the Executive Yuan and competent authorities shall transmit and share the information collected, in possession, kept, or stored with each other for matters concerning the security protection of CIs.

II. The aforementioned information, except for data classified as national secrets, shall be kept confidential as official secrets. No prying,

collecting, disclosure, or handover is allowed without proper cause.

III. The Executive Yuan shall have the authority to prescribe the security management and other rules for transmission and protection of the information described in I. and II.

IV. The security protection tasks and information related to the CIs shall be kept classified and sensitive. Therefore, if the security protection plans, drills, and audit data drafted by the agencies are classified and sensitive, they shall follow the rules required by the Classified National Security Information Protection Act and other relevant regulations.

## Section 2 Notifications, warnings, and press releases

I. If the core functions of the CIs are damaged or suffer from major man-made hazard incidents or terrorist attacks, infrastructure providers shall notify the related organizations according to the "Operation Directions on Homeland Security Contingency Notification" and initiate response mechanisms. The providers shall also be responsible for such tasks as making emergency repairs, recovering, and ensuring continuous operations. At the same time, supporting agencies shall support providers in rescue operations and evacuations.

II. If the aforementioned functions become damaged or suffer from attacks and may cause hazards to civilian lives and business operations, the CI providers shall initiate warning mechanisms to the public in times of crisis or emergencies.

III. CI providers shall coordinate with the competent authorities and establish a press release mechanism that drafts rules for media control at the incident field; the content, methods, frequency, and procedures of press releases; the methods and principles for interaction with the media; and press release samples. Such mechanisms can enable parties responsible for the affairs to regularly explain disasters to the public; as a result, sectors, sub-sectors, operating units, the media, and the public can stay informed of incident updates.

IV. Competent authorities shall establish vertical and horizontal notification mechanisms that assist CI providers and external units in establishing security joint defense and notification response mechanisms. Therefore, the latest security protection goals and risk information can be communicated so that additional supervision and improvements can take place.

## Section 3 Partnership with private sectors

I. Since protecting CIs still partially relies on the efforts of private businesses (known as the private sector), insufficient protection by private sectors on their own critical infrastructures can cause protection loopholes for the nation's homeland security. Therefore, public and private sectors shall work hard on collaborating CI protection and supporting each other with their own resources. All sub-sector competent authorities shall proactively encourage businesses to put efforts into security protection through the following measures:
    1. Provide instantaneous early warning information to encourage private critical infrastructure providers to voluntarily participate in information-sharing mechanisms.
    2. Invite the private sector to participate in disaster prevention and rescue drills, held by the government or national enterprises, to enhance learning effectiveness.
    3. Forming an in-depth response system with resources from private critical infrastructure providers that are inter-dependent or substitutive is recommended.
    4. When drills take place for all levels of infrastructures according to the protection plans, their superior authorities shall perform reviews on the collaboration between infrastructures and the private sectors to ensure sufficient levels of protection from the private sector that will not result in homeland security loopholes.

II. Regarding private sector participation and support, various ministries are recommended to take an encouragement approach. However, chartered businesses may be requested to make further implementation through supervision and support policies. During the annual comprehensive assessment by the Homeland Security Policy Committee, a point and merit system may be introduced to reward private sector industries that participate in risk management and ministries that participate in response mechanisms.

III. The long-term goal of promoting CI protection shall be the establishment of safety norms and standards for the private sector's critical infrastructures. Necessary supervisory measures should be taken to ensure that the public interest is served. In the short-term, measures such as executive orders may be considered for handling urgent matters.

## Section 4 Research and development

I. To reduce the risks and threats on CIs, infrastructure providers and competent authorities shall encourage employees to research and develop security maintenance and disaster-resilient technologies and equipment that are cost-effective or incorporate risk assessment results into R&D plans.

II. Sector-level coordinating authorities may promote the security maintenance and disaster-resilient technologies, as well as equipment researched and developed by the infrastructure providers based on their sector attributes and environmental restrictions. In addition, agencies may incorporate common sector needs into the R&D plan.

III. Some recommended R&D topics are as follows:
- Testing and sensor system
- Security protection and prevention system
- Analysis and decision support system
- Response and recovery tools
- Security threat and loophole blocking tools
- Advanced infrastructure structure and system design
- Coordinated protection or warning measures with the public

IV. The outcomes of research and development, along with a personnel list to be rewarded, shall be submitted to the Homeland Security Policy Committee.

**Annex 1 Sector Classification for National Critical Infrastructure**

**Annex 2 Notice on National Critical Infrastructure Inventory Check**

**Annex 3 Security Protection Plan Framework for National Critical Infrastructures**