Guidelines for National Critical Infrastructure Protection

Promulgated on December 29, 2014
1st revised on February 3, 2015
2nd revised on May 18, 2018
3rd revised on August 19, 2025

Guidelines for National Critical Infrastructure Protection

Table of Contents

Chapter 1 General Provisions

Section 1 Origin

The revision of these Guidelines is based on the resolution adopted by the Homeland Security Policy Committee (hereinafter "the HSPC") of the Executive Yuan and the related meetings, with the aim of strengthening the protection of national critical infrastructure, enhancing national resilience, safeguarding national security, and protecting public interests. In carrying out this revision, the following regulations and acts have been referred to:

I. Cyber Security Management Act and its related subordinate regulations.
II. Disaster Prevention and Protection Act and its related subordinate regulations.
III. All-out Defense Mobilization Readiness Act and its related subordinate regulations.
IV. Civil Defense Act and its related subordinate regulations.
V. Directions for the Establishment and Operation of the Homeland Security Council, Executive Yuan.
VI. Guidelines for Contingency Response Plans and Operations of Homeland Security, Executive Yuan.
VII. Homeland Security Emergency Reporting Regulations.

Section 2 Definition

I. National Critical Infrastructure (hereinafter "CI"): Refers to physical or virtual assets, systems and networks, the disruption or dysfunction of which may negatively impact national security, harm public interests, citizens' livelihood, or economic stability.
II. National Critical Information Infrastructure (CII): Refers to the core information and telecommunications system as well as supervisory control and data acquisition (SCADA), which are also vital components (information and telecommunications assets) of the CI. These systems support the continuous operational needs of a CI, and should be consolidated under the management of the corresponding CI.

III. Classification: CI is classified into three levels, the first level is the sector, the second level is the sub-sector, and the third level consists of core functional facilities and systems under the sub-sector: [1]
    1. Sector: Categorized into nine primary sectors based on functions and attributes. The nine sectors are energy, water resources, communications and transmission, transportation, finance, emergency rescue and hospitals, government agencies, science parks and industrial parks, and food.
    2. Sub-sector: Further categorized under each sector in accordance with functions and tasks. For example, the energy sector is subdivided into electricity, petrol, and natural gas sub-sectors.
    3. Functional facilities and systems: Refer to the facilities and equipment, transmission networks, information and communications systems, control systems, command and management systems, security maintenance systems, and critical technologies which are necessary to ensure the continuous operation of the sub-sectors' core functions and tasks.

IV. The Executive Yuan's CI Security Protection Task Team: The team is composed of representatives from competent authority, coordinating agencies across all sectors, and experts and scholars invited by the Office of Homeland Security, the Executive Yuan. The team communicates and coordinates annual tasks, education and training, drill plans, and revisions to the Guidelines for National Critical Infrastructure Protection and its annexes. Significant measures must be submitted to the HSPC for approval.

V. Competent authority: Refers to the central competent authority of the relevant industry, or municipality, county (city) government directly responsible for, or supporting all or part of a sub-sector.

VI. National critical infrastructure provider (hereinafter "CI provider"): Refers to an entity that is designated by central competent authority and approved by the Executive Yuan (hereinafter "the EY") to maintain or provide all or part of a CI.

VII. All-hazard: Hazards that include natural disasters, cyberattacks, accidents, human-caused attacks, non-conventional attacks, and military threats. Attacks and threats other than natural disasters are divided into three phases: peacetime, gray-zone, and wartime (mobilization and

[1] Refer to Appendix 1: "Sector Classification for National Critical Infrastructure"

implementation phase), which serves as the primary basis for identifying risks and threats to CI.

VIII. Resilience: Refers to the ability to reduce the impact and duration of operational disruptions. Whether a CI possesses effective resilience depends on its capacity to prevent, endure, adjust, and rapidly recover from incidents.

IX. Inter-dependence: Refers to the interdependence and interaction among CIs. If the core function of a specific CI fails, it may trigger a chain reaction, causing other CIs to cease operation.

Section 3 Goals

I. The goals are to ensure the continuity of vital national and societal functions, and to safeguard CI and assets related to national security, governance, public safety, the economy, and public confidence.

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

III. To facilitate partnership by establishing a cross-sector, cross public-private collaboration and information-sharing network to implement practical defense and security protection measures of physical, cyber, and personnel, prevent and respond to the impact of all sorts of hazards, enhance the security and resilience of facilities.

Section 4 Strategies

I. Implement CI risk management based on all-hazard protection concept. CI security protection shall be based on "all-hazard" protection concept, which requires both internal and external risk identification of facilities and the blending of risk management and continuity management methodologies into CI security protection tasks.

II. Develop response tactics and strategies, as well as formulate multiple security protection plans.

To implement CI security protection management effectively, a comprehensive and systematic facility inventory shall be conducted to enable hierarchical management based on facility importance, followed by the establishment and regular update of a complete CI database. All

CI facilities and their competent authorities shall be aware of the inter-dependence among others and the impact caused by facility failures. They shall develop tactics and strategies for prevention (including mitigation and preparedness), response and recovery within their jurisdictions based on the results of risk identification, as well as formulate an actionable security protection plan. During the mobilization and implementation phase, in addition to maintaining existing safeguards, they shall also incorporate operation capacity preservation, transfer or recovery into security protection programs.

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

The competent authorities shall work with CI providers to establish and strengthen cross-sector joint defense mechanisms between the interior and exterior units, as well as between central and local government. 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 establish a threat warning and security protection information-sharing platform 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.

All competent authorities and CI providers shall proactively coordinate and prepare security protection resources to effectively protect and preserve the safety of CIs and critical assets. They should also develop countermeasures to mitigate the impact caused by a sudden suspension of facilities' functions, and enhance the continuity functioning capabilities of government and society, so as to safeguard people's lives, properties and wellbeing as well as homeland and national security.

Chapter 2 Mission

Section 1 Office of Homeland Security

The Office of Homeland Security, the Executive Yuan (hereinafter "OHS") serves as a supporting staff office for the HSPC and implements resolutions on "National Critical Infrastructure security protection" issues adopted by the HSPC. The OHS is responsible for planning the overall direction and missions as well as supervising, inspecting and coordinating security protection goals, missions and resources between various sectors. It should also guide educational training and drills at all facilities.

To integrate the implementation of CI security protection, the OHS convenes project team meetings with all relevant ministries, departments, scholars and experts. Its primary objectives are as follows:

I. Research and draft policies, laws and regulations related to CI security protection.
II. Research and draft risk management and warning mechanism related to CI security protection.
III. Research and draft measures and emergency responses related to CI security protection.
IV. Coordinate and liaise between all intelligence and policing ministries in order to maintain the order of CI security protection.
V. Handle integrated supervision, cooperation and support measures related to CI security protection.
VI. Collect and process information related to CI security protection.
VII. Perform other measures, drills and training related to CI security protection.

Section 2 Competent authority

I. Each competent authority shall appoint deputy chief-level officials or above to act as the convenor of a project team to hold cross-departmental project meetings, establish or designate specific organization and personnel as administrative advisors, inventory any potential vital assets and facilities under its jurisdiction and formulate inventory targets and division of work. They shall also draft budgets and resources to support

security protection management, and implement a system for rewards and penalties.

II. Draft the "National Critical Infrastructure Facilities Sector Security Protection Plan" and submit it to the EY for record. The plan shall cover the general overview of each sub-sector, security protection action visions and goals, risk assessments, facility importance classification and security protection priorities, action plans and implementation, management and coordination, research and development priorities and periodic reviews, etc.[2]

III. Formulate importance classification standards, supervise the inventory and importance classification of the CI under its jurisdiction, compile CI information, prioritize security protection and submit them to the OHS for review.

IV. Based on the characteristics of the CI sectors under its jurisdiction, considering the mutual support and coordination in conjunction with corresponding disaster prevention and relief, all-out national defense mobilization preparation plans and other relevant plans, propose and provide protection operation guidance during the facility mobilization and implementation phase. The contents should include: basis, composition and division of the protective team, evacuation and relocation, protective measures, procedures and measures for resource preservation, transfer and restoration.

V. Guide all levels of CIs under its jurisdiction to implement risk assessment, and examine the "National Critical Infrastructure Facilities Security Protection Plan" drafted by all CI providers complied with risk assessment result and operation guidance specified in preceding subparagraph IV, then submit them to the EY for record.

VI. Supervise, inspect and assist CI providers under its jurisdiction in implementing security protection measures, training and drills as well as coordinate CIs with central, local government and related agencies to establish mutual support and joint defense mechanism.

VII. Establish horizontal and vertical notification mechanisms to increase information sharing efficiency within the sector and across sectors.

VIII. Encourage research and development of cost-effective technologies and equipment related to security protection and resilience.

[2] If the competent authority has only one CI under its jurisdiction, then the authority will only be required to formulate its security protection plan, without formulating the sector security protection plan.

IX. Depending on the needs of facility providers under its jurisdiction, complete the mobilization approval or requisition (use) of the required materials in accordance with each category of the all-out defense mobilization readiness regulation, and complete the necessary personnel application, such as civil defense, specialists, substitute services draftees or military service corps, based on the facility essence.

Section 3 National Critical Infrastructure Providers

To ensure CI security and the continuity of its core functions, the head of each CI provider shall appoint a deputy chief or appropriate personnel to act as the convener. The convener shall invite personnel responsible for security maintenance, administration, information security and protection, human resources, accounting, general management, government ethics, and internal control, as well as external collaborating units to hold project meetings. The convener shall designate dedicated organizations and personnel to promote and supervise security protection affairs. The CI providers shall also draft budgets, formulate plans, promote drills, educational training, conduct systematic and continuous research on maintaining facilities' security, continuous functioning, capacity preservation, transfer and recovery. Its primary objectives are as follows:

I. Regularly assess risks, threats and vulnerabilities. Draft a "National Critical Infrastructure Facilities Security Protection Plan", submit it to the competent authority for approval, and regularly check the effectiveness of actual implementation.
II. Establish horizontal and vertical notification mechanism to increase information sharing efficiency within the sector and across sectors.
III. Establish a warning system to promptly alert the public when crisis or emergencies occur.
IV. Cooperate with collaborating security protection units to implement protective drills, improve protective measures and revise protection plans based on reviews and suggestions.
V. Centered around the core tasks of the facilities, establish support protocol related to the professional assistance and support needed during crisis and disaster threats. A detailed list of contact personnel shall be regularly updated.
VI. Develop self-defense and self-rescue preparedness based on operational needs. After conducting an inventory, follow the all-out defense

mobilization readiness regulations set by the competent authorities according to whether the facilities belong to the public or private sector. For public sector facilities, applications should in principle be submitted through the competent authority with jurisdiction; for private sector facilities, applications should in principle be submitted through the competent authority in charge of overseeing the facility, in order to request the necessary personnel and material reserves for operation and sustainment.

Section 4 Collaborating Units for Security Protection

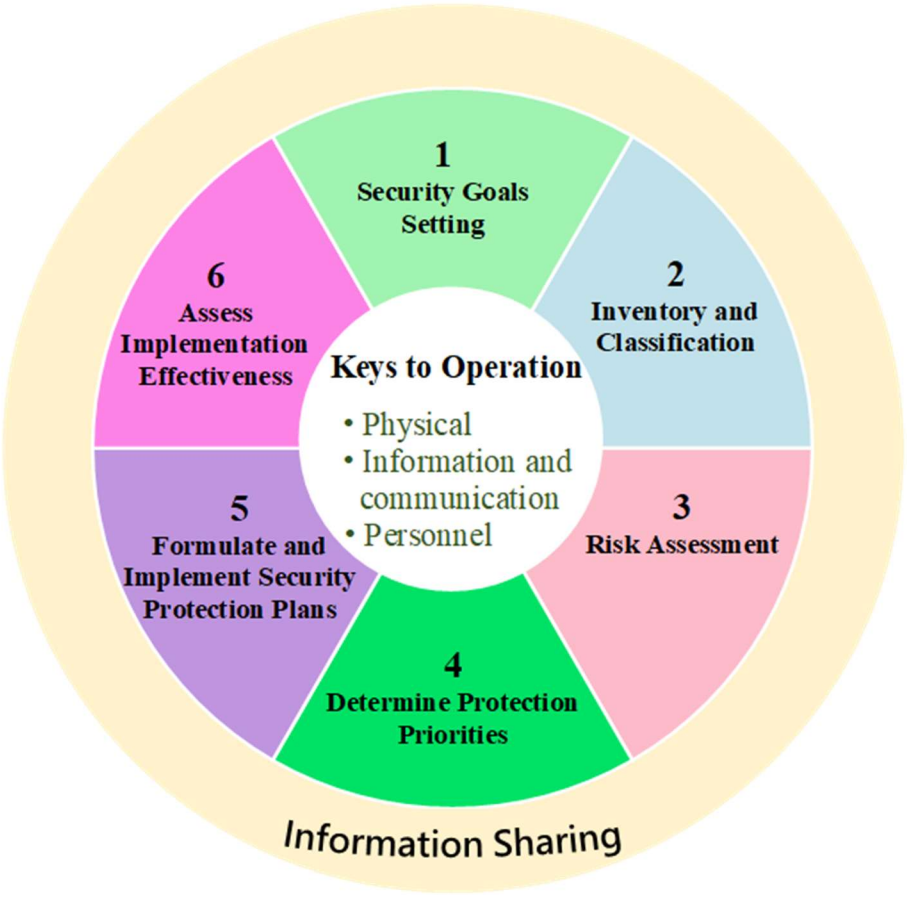
Collaborating security protection units include central and local, public and private sector agencies (units) that support CI providers in security protection, disaster prevention and rescue, continuous functioning, and capacity preservation, transfer and recovery. Collaborating security protection units shall stay in close contact with CI providers during peacetime, engage in training sessions and drills so that they can assist in response and recovery tasks in case of emergency.

I. When a CI suffers or is likely to suffer damage, all collaborating security protection units shall provide support and assistance based on the request of the OHS, competent authorities, or CI providers. However, all units shall proactively provide assistance when major hazards and disaster occur.

II. The government of all municipalities, counties (cities) should evaluate the necessary human and material required to support the security, continuous operation, capacity preservation, transfer and recovery of CIs under their jurisdiction and report to the competent authority in accordance with relevant regulations.

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 among goals, plans and actions, but also implementation effectiveness. Competent authorities shall implement correct actions through planning, training, assessment and shall impart a sustainable operation mindset including the duties and management plans to senior executives and personnel. Based on objective assessments from testing and drills, feedback shall be used to revise CI security protection plans, procedures, and training. This will help establish priorities, inform budget decisions, and promote improvement plans and procedures. The fundamentals of such promotion include the following:



Section 1 Security Goals Setting

To achieve CI security protection goals as described in Chapter 1, all competent authorities shall deliberate on protection management goals and priorities. If the risk assessment results indicate that collaboration with other

government partners and with private sectors will be beneficial to achieving the goals of Guidelines, then a specific plan on viability of collaboration shall be drafted and implemented.

All competent authorities and CI providers must follow the protection management goals and priorities required by the sectors to which they belong. They must set security protection goals and priorities for CIs based on core function task, risks environment, available resources, and comply with the following principles:

I. Support and emphasis from authority chiefs
   Each competent authority chief shall supervise the CI security protection management policy and implementation performance, and declare their commitment and determination regarding its promotion. They should also set security protection and continuous operation goals as a major inspection and review targets, offer rewards to the outstanding units and personnel.

II. Establish dedicated promotion teams
   CI inventories, risk assessments, security protection and drills shall be based on inter-ministerial, inter-departmental coordination, cooperation and mutual assistance. The dedicated promotion teams shall be convened by deputy chief-level officers or above.

III. Convey security protection task goals
   All competent authorities shall notify the security protection task goals, implementation strategies and promotion directions to the CI providers within their jurisdiction. They shall also state the risk items, management policies, continuous operation goals and plans, disseminate the proposed operational items pursuant to the Guidelines.

Section 2 Inventory and Classification

The purpose of the CI inventory is to identify the vital nodes, assets, facilities, system networks that affect homeland security, government and social operations, and to understand the inter-dependency within the sector and across sectors to reduce the probability of complex hazards that may occur. Therefore, an importance assessment of facility's systematic functions, assets value, and impact of function loss shall be implemented, and classification management shall be implemented based on the assessment result.

The competent authorities shall first list asset items based on the core functions and mission of the authority, then sort out the vital nodes that cover all

functions or missions of the authority and mutual related nodes, such as buildings and their locations, physical facilities, information systems, telecommunication equipment, technology and human resources. These nodes shall then be organized into a preliminary infrastructure inventory list (including facility providers).

Next, the facility providers on the list will survey the unit's core tasks, internal assets and external resources to assess their importance and fill out the "CI survey form" before submitting it to the competent authorities for further compilation. The competent authorities will then convene project meetings to review and deliberate on the survey forms, prioritize their importance and consult relevant public administrative agencies, civil groups, experts and scholars before 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, and establish the "CI database" based on the results of the review meeting. The procedure for this is as follows:[3]

I. Facility providers will fill out the "CI Survey Form"

Facility providers will implement necessary check and inventory on nodes, assets, facilities and systematic networks according to the attributes of functions, tasks and scopes. The content of the CI survey form must include:

1. Core function tasks: Identify the core function tasks (including the maximum allowable interruption time), supporting units and target units (recipients).
2. External critical resources: Inventory the external critical resources that support core function operations (such as electricity, water supply, fuel, gas, and communications), their suppliers and the backup plans in the event of a failure of these external critical resources, as well as the maximum operation and switchover time under full load.
3. Internal essential assets: Assess on three categories with physical entities, personnel (critical technologies, leadership, operation), information and telecommunications, to inventory the assets required to support core operations, along with the backup plans, capabilities, maximum operation and switchover time under full load.
4. Importance self-assessment:

[3] Please refer to the "Notice of National Critical Infrastructure Inventory Check Operation" in Annex 2 and the "National Critical Infrastructure Survey Form" provided by OHS.

(1) Function importance: The importance of a facility to the government operation depends on the significance or criticality of its core functions to various government functions.
(2) Impacts on public morale: The extent to which a facility affects intangible aspects such as public morale, public confidence, government reputation, international images, etc.
(3) Failure impacts: Estimate the total value of facility (including assets) and the affected number of people, economic losses and spatial scope when facility operation is degraded.

II. Competent authorities implement preliminary classification assessment
Competent authorities shall compile the CI survey forms submitted by the facility providers within their jurisdiction and review the content to ensure correctness and comprehensiveness. They shall prioritize facilities with the same attributes into "level one, level two, level three" categories, make facility inventory books for all categories and provide reasons for such classifications, then consult related government agencies, civil groups, experts and scholars for their opinions before submitting the aforementioned survey form to the OHS.

III. OHS convenes joint review
The OHS shall convene the National Security Council, the National Security Bureau, Ministry of National Defense, relevant ministries, experts and scholars to jointly review the aforementioned facility lists at all levels, the justification for their classification, appropriateness of the survey forms, whether critical facilities have been omitted, and conduct a comprehensive review to make the final decision on the CI list and classification.

Section 3 Risk Assessment

The CI partners including CI providers, competent authorities and the OHS shall use a series of risk assessment methods to assess risk from aspects of threat, vulnerability and impact consequence, etc. Such risk assessment results should enable leaders and decision-makers to fully understand the most likely and severe incidents that could affect proper functioning, so that they can draw further support and coordinate resources to revise protection plans accordingly. To obtain reliable, operable and timely risk information, competent authorities and CI providers should seek scientific and technological support in

development or usage of methods, techniques or tools to assess related threats, vulnerability and potential consequences.

CI risk assessment must identify the threats, scenarios, severity levels and probability of occurrence regarding impacts on core functions based on the all-hazard concept (threat identification). Assessment on the inter-dependence between the related CIs, the degree of damage (vulnerability) 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 level of threat scenarios that have a low probability of occurrence but are likely to cause massive CI failures, disrupt government and social functions, and serious 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 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, based first on national level and then sector level of threat scenarios, followed by location, environment, spatial scope and facility attributes.

II. Vulnerability and impact assessment
   1. National level: Based on the national level of disaster threat scenarios, assess the degree of impact on CI and sectoral functions, the length of recovery time and evaluate every national level hazard impact scenario.
   2. Sector level: Based on the sector level of disaster threat scenario, assess the degree of impact and recovery time of various CIs, critical external resources, backup strategies within the sector. Assess the impacts if the sector's core functions and tasks are disrupted.
   3. Facility level: Based on the facility level disaster threat scenarios, considering the location, spatial scope and facility attributes, assess the impact on essential internal assets and critical external resources, the extent of the impact on backup facilities, the required recovery time and the overall impact of any disruption to facility operations.

Section 4 Determine Protection Priorities

I. CI providers should prioritize actions to manage facilities according to the importance of facilities, the costs and expenditures of protective actions and the probability of risks mitigation.

II. Competent authorities should 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 specific risk at the sector level.

III. The OHS should 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 serve as the foundation for formulating protection strategy and the overall allocation of protective resources.

IV. The CI classification list is essential for allowing central control of limited protective resources during peacetime and ensures that core 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 for disaster periods.

V. In times of military crisis, national security units shall assist in maintaining vigilance and protecting CIs deemed critical for warfare. Competent authorities shall adjust protective resources and ensure the proper functioning of facilities during military crisis.

Section 5 Formulate and Implement Security Protection Plans

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

II. Objectives of security protection plan:
    1. To ensure sustainable and stable protection of CIs with regard to physical, telecommunications and personnel aspects.
    2. To plan necessary actions during peacetime, grey zone and wartime based on the all-hazard concept. Actions shall include prevention, response, recovery and reconstruction steps.

3. To coordinate, allocate responsibilities and resources among partners according to the inter-dependency and substitutability of facilities.
4. To effectively utilize resources to establish disaster resilience and maximize the reduction and mitigation of risks and threats.

III. The Security protection plan shall include an overview of the CI, its core function, facility importance, security protection goals, protection management team, internal necessary assets, external critical resources and other inter-dependency facilities, risk assessment, determine protection priorities, formulate and implement three protection management phases of prevention, contingency and recovery (including continuous operation, capacity preservation and transferring), the drill way, the supporting measures for assessing implementation effectiveness, etc.[4]

Section 6 Assess Implementation Effectiveness

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

I. Drills and educational training

1. The OHS and each competent authorities shall provide resources and necessary measures to promote CI security protection management concepts, and carry out staff educational training on risk management, continuous operation management, drills and audits. Assist CI providers in establishing and enhancing professional skills related to risk management and response capabilities through educational training and organization learning.
2. To verify whether the identified risks can be effectively controlled as well as the security protection plans successfully reduce hazard losses and shorten recovery time, every competent authority shall supervise CI providers to hold drills or supporting anti-hazard and information security drills.
3. Drills may take the combination of table-top exercises, war games or full-scale exercises. The aforementioned kind of drills shall integrate all related authorities (units) to participant, and should be based on

[4] Please refer to the "Security Protection Plan Framework for National Critical Infrastructure" in Annex 3.

real people, real place, real objects, real actions, real scenarios without scripts (with a scenario but no script).

4. Plans shall be formulated before drills take place and hold coordinating meeting to explain the details. Drill procedures shall be accurately recorded in detail, including drill ways, time, place, purpose, personnel list, evaluations and suggestions. After the drill, they should immediately review and plan follow-up improvement measures as a reference for future drafting and revision of protection plans.
5. The drill items deemed as requiring further improvements shall be prioritized for funding allocation and incorporated into training courses.
6. The utmost emphases of all competent authorities' educational training and drill are learning effectiveness and providing feedback to the CI security protection system. Agencies or individuals should be rewarded with incentives as appropriate.
7. Based on the classification results, OHS should consider the current state of affairs and environmental requirements before selecting vital CIs and recommending that the HSPC incorporate such CIs into the annual homeland security drill. OHS should also require that agencies for the selected CIs submit detailed risk assessments and drill plans.

II. Audits and rewards

1. The OHS has the authority to invite experts and scholars to draft a review list to cooperate on the Office of Disaster Management's disaster prevention and rescue visiting assessment projects and cyber security audits of the Administration for Cyber Security, Ministry of Digital Affairs, then incorporate the review list into all competent authorities' internal control systems. Furthermore, the OHS has the authority to visit all agencies to check the risk management and contingency plan implementation status of CIs. All competent authorities shall incorporate the security protection status of these facilities into their own internal audits.
2. Security protection plans of all-level CIs shall be submitted to their competent authorities for approval, then submitted by the competent authority to the EY for record. The OHS will select plans as the subjects of annual visits, evaluations, and exercises by the EY depending on the circumstances. The assessment results of annual

drill shall be submitted to the HSPC which will make recommendations regarding rewarding well-performing agencies.

3. Competent authorities shall conduct annual ministerial-level inspections and exercises at all levels under their jurisdiction and stipulate operational regulations for annual self-inspection and drills of facilities, compile the results of the aforementioned work, review common deficiencies, formulate and promote measures to be implemented in parallel on CIs under their jurisdiction. The implementation plans, performance reports, and summaries of key security protection research and development achievements of the competent authorities and CI providers shall be submitted to the OHS for record, and the OHS may submit recommendation list for rewards.

Chapter 4 Related Supporting Measures

Section 1 Confidentiality and Confidential Requirements

I. To implement CIs security protection, the EY and competent authorities shall, to the extent necessary and upon request, provide access to transmit or exchange the information they collect, keep or store.

II. The aforementioned information, except for the information legally classified as national security information, shall be kept confidential as official classified information. No prying, collecting, disclosure or handover is allowed.

III. The transmission and protection principles of the information stated in the preceding two subparagraphs are as follows:

1. Confidential information range: Information once disclosed, may endanger national security, social stability, economic development and people's lives, or trade secrets of facility operation. Information that may impair facility availability, integrity, reliability or safety.
2. Information provision practices: Facilities (including critical assets) with their locations, vulnerabilities and specific-event information are not appropriate to be explicitly stated. Whether information is provided depends on the purpose, contents, providing organization (or personnel), recipients and way of provision, etc.

IV. The security protection tasks and information related to the CIs shall remain confidential. Therefore, any security protection plans, drills and audit data formulated by the responsible authorities shall be handled in accordance with the Classified National Security Information Protection Act and other relevant regulations.

V. All agencies and facility providers shall implement measures for the handover and supervision of personnel in charge of sensitive information to ensure facility security protection and task operations.

VI. To reduce the risk for hiring personnel with security concerns, CI providers shall, in accordance with relevant laws and regulations, conduct special or qualification checks on key internal maintenance personnel or vendors (including personnel performing relevant tasks), and maintain tracking management.

VII. Regarding the confidential and sensitive information protection of competent authorities, relevant agencies and CI providers, the OHS has

compiled related laws and regulations, formulated reference guidelines for internal measures to the aforementioned agencies (providers) to fulfill confidentiality mechanisms.

Section 2 Notifications, Warnings and Press Releases

I. If the core functions of the CIs are damaged or suffer from major human-caused security incidents or terror attacks, CI providers shall notify the related organizations in accordance with the "Operation Directions on Homeland Security Contingency Notification" and initiate response mechanisms. The providers shall also be responsible for emergency repairs, recovering and ensuring continuous operations. At the same time, collaborating security protection units shall support providers in rescue operations and evacuations.

II. If the aforementioned functions are damaged or suffer attacks and may cause hazards to civilian lives and business operations, the CI providers shall initiate warning mechanisms to promptly alert the public when crisis or emergencies occur.

III. CI providers shall coordinate with competent authorities to establish a press release mechanism that standardizes media control at the incident scene; 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 the disaster to the public, ensuring the relevant sectors, facilities, operating units, media and the public stay informed of latest updates and to clarify false information or misinformation.

IV. Competent authorities shall establish vertical and horizontal notification mechanisms to assist CI providers and external related units in establishing joint security defense and notification response mechanisms. Therefore, the latest security protection goals and risk information can be communicated as well as further supervision and improvement can take place.

Section 3 Partnership with Private Sectors

I. Since CI security protection also relies on the participation of private sector, insufficient protection by private sectors can cause CIs protection

loopholes in homeland security. Therefore, public and private sectors should be dedicated to collaborating on CI protection and supporting each other with their respective resources. All competent authorities shall proactively encourage private sector to put efforts into security protection through the following measures:

1. Provide instantaneous early warning information to encourage private CI 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 state-owned enterprises to enhance learning effectiveness.
3. Forming an in-depth response with resources from private CI providers that are inter-dependent or substitutive is recommended.
4. When drills take place for all sectors of infrastructures according to the protection plans, their superior authorities shall perform reviews on the collaboration between infrastructures and the private sectors to prevent insufficient protection by the private sector from creating security loopholes in homeland security.

II. Regarding the private sector attendance 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 HSPC, a point and merit system may be introduced to reward ministries that successfully invite private sector participation in risk management and 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 alleviate the risk threats on CI, CI providers and their competent authorities shall encourage employees to research and develop security maintenance, disaster-resilient technologies and equipment that may meet their cost-effective requests or incorporate risk assessment results into R&D plans.

II. Each competent authority can promote the security maintenance and disaster-resilient technologies as well as equipment researched and developed by the CI providers based on their sector attributes and environmental restrictions. In addition, agencies can incorporate common sector needs into the R&D plans.