Annex 3

Security Protection Plan Framework for National Critical Infrastructure Facilities

I. Propose security goals

1. Plan basis, infrastructure level, and basic infrastructure information (CI basic information and risk assessment form 1.1)

- Basic infrastructure information: Description of the infrastructure's development background, basic information, and geographical environment.
- Security protection and monitoring: Description of infrastructure protection and security monitoring status (security alert and information and telecommunication security monitoring and protection), including human resources, control locations, scope, equipment, and mechanisms.

2. Infrastructure security protection goals (CI basic information and risk assessment form 1.2)

- Security protection goals: To describe the security goals of infrastructure protection, such as the "continuous operation of functions", reducing disaster risks, enhancing disaster resilience, shortening recovery time, and decreasing disaster and damage impact.
- Core function tasks: To describe the core function tasks of the infrastructures, identify the maximum tolerable disruption durations of the various core functions, and describe the substitution ability of all the infrastructure's core functions (such as substitution facility and alternative plans).

3. Critical infrastructure protection management team (CI basic information and risk assessment form 1.3)

- Identify common management units: Identify the common management units within the infrastructure scope that support the infrastructure's core function tasks and describe the core function tasks supported by various units.
- Critical infrastructure protection management team: Establish a critical infrastructure protection management team list based on the common management units identified.
- Identify external security protection supporting units: Describe the

external security protection supporting units and the matters they support, such as local government, police and fire rescue squads, medical teams, the military, important suppliers, security guard companies, information security companies, and equipment management companies. Make notes on the protocol support status and develop a liaising/contact list.

4. Infrastructure significance

(CI basic information and risk assessment form 1.3)

- Importance of governmental functions: Describe the infrastructures' importance for achieving crucial national and social functions and missions, including government/agencies command and control, important information and telecommunications, life maintenance and transport functions, financial order, disease management systems, security protection and disaster prevention/rescue, vital national symbols and assets, vital industries and industrial parks, and defense and mobilization.
- Social and economic impact caused by functionally ineffective infrastructure: Describe the total infrastructure value, the number of people affected, and the economic losses.
- Impact on morale caused by functionally ineffective infrastructure: Describe the impact level of functionally ineffective infrastructure on international image, government prestige, and public confidence.

II. Identify infrastructure, assets, systems, and networks

1. External critical resources (CI basic information and risk assessment form 2.1)

- Describe the external critical resource providers that enable the continuous functioning of various core functions and tasks (such as electricity, water, gas, transportation, fuel, and information and telecommunications providers). For example, this could be XX substation, XX water purification plant, or XX plant).
- Describe the infrastructures' backup status if external critical resources (such as electricity, water, gas, transportation, fuel, and information and

telecommunications) are disrupted. This may include a description of the types of backup facilities, maximum backup time, and backup options.

2. Necessary internal assets (CI basic information and risk assessment form 2.2)
   - Identify the necessary assets that support the continuous functioning of various core functions and tasks and then categorize them as physical necessities, personnel, or information and telecommunications.
   - Describe the backup status of various necessary assets (physical necessities, personnel, and information and telecommunications), including backup facilities and substitution capacity, maximum backup time, and backup plan description.
3. Impact on other critical infrastructures (CI basic information and risk assessment form 2.3)
   - Describe the impact due to functionally ineffective infrastructures on other types of critical infrastructure and sectors.

III. Risk assessment (threats, weaknesses, and disaster impact)

1. Threat identification (CI basic information and risk assessment form 3.1)
   - Identify internal and external hazards and risks (natural disasters, man-made disasters, and information security incidents) that pose serious threats to the infrastructure's functioning. For each scenario, describe the scale/level/intensity of disaster, time/place of occurrence, and region scope/number of people impacted. Also evaluate the likelihood that such a scenario could occur.
     - Natural disasters: Earthquakes, tsunamis, hurricanes, flooding, draughts, and landslides.
     - Man-made disasters: Diseases/contagious diseases, fires, explosions, radioactive disasters, chemical disasters, equipment management (e.g., old equipment, faulty operation), security hazard incidents (e.g., man-slaughter, robbery, burglary, illegal intrusion, or sabotage), terrorist attacks, strikes/labor disputes, and riots/demonstrations.
     - Information security incidents: Service disruption/ loss of control,

system hardware facilities shut down/loss of control, software application disruption/loss of control, stolen/loss/damage of vital electronic data.

2. Impact assessment (CI basic information and risk assessment form 3.2)
   - Based on the threat scenarios, assess the internal necessary assets (physical necessities, personnel, information and telecommunications), external critical resources (electricity, water supply, gas supply, transportation, fuel, and information and telecommunications), degree of impact on internal backup systems, and necessary recovery time needed, in that order. Then establish and describe the hazards and impact on critical infrastructures caused by such threat scenarios.
3. Impact caused by disrupting critical resources
   - Assess the degree of impact on and remaining functioning duration of the necessary assets (physical necessities, personnel, information and telecommunications) when a given external critical resource is disrupted (electricity, water supply, gas supply, transportation, fuel, information and telecommunications). Then establish and describe the impact scenario on the critical infrastructure in such a case.

IV. Determine protection priorities

1. Based on risk assessment results, identify various disaster threat levels and the risks of facilities' core functions, necessary assets, and critical resources becoming ineffective.
2. Analyze whether existing protection levels and backups meet the security needs and recovery times established for various types of impact. Then use such analysis to draft a disaster reduction strategy and establish protection priorities, such as strengthening physical necessities, protecting information security, training personnel, or improving security.

V. Implement protection management plan

In accordance with the risk assessment results and protection strengthening priorities, a series of protection, management, and implementation key points related to internal necessary assets (physical necessities, personnel, information and telecommunications) and external assets based on various disaster threats (natural, man-made, information security) shall be laid out in

four stages: prevention, disaster reduction, response, and recovery. Furthermore, additional notes on relevant protection management implementation plans shall be included. The following is a recommendation for plans drafted to counter various disaster threats:

- Prevention stage: operation impact analysis, risk management plan, threat monitoring plan, training plan, various protection plans, information and telecommunications plan, rules on confidentiality.
- Disaster reduction stage: assets maintenance/improvement plans, various types of disaster reduction plans, and support protocols.
- Response stage: emergency response plans, various types of crisis handling plans, emergency notification, and press release and control.
- Recovery stage: continuous operation plan, various recovery plans.

VI. Assess implementation results

Describe the drill plans, task items, assessment frequencies and references, review and improvement items, and improvement status and tracking that are used to assess the implementation results of various plans and standard operating procedures (SOPs).