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 survey form 1.1-1.4)
   - ●Basic infrastructure information: Description of the infrastructure's development background, basic information, and geographical environment.
   - ●Security protection and monitoring: Description of the infrastructure's protection and security monitoring status (security alerts, information and communications security monitoring and protection), including human resources, control locations, monitoring scope, equipment, and mechanisms.
2. Infrastructure security protection goals (CI survey form 2.1)
   - ●Security protection goals: Describe the security goals of infrastructure protection, such as continuous operation of functions, reducing disaster risks, enhancing disaster resilience, shortening recovery time, and mitigating disaster and damage impact.
   - ●Core function operations: Describe the core function operations of the infrastructure, identify the maximum tolerable disruption duration (MTPD), and describe the substitutability of all the infrastructure's core functions (such as substitute facility and alternative plans).
3. Critical infrastructure protection management team (CI survey form 3.1-3.2)
   - ●Identify common management units: Identify the common management units within the infrastructure that support the infrastructure's core functional operations and describe the core functional operations supported by each unit.
   - ●Critical infrastructure protection management team: Establish a critical infrastructure protection management team 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, medical teams, national military, important suppliers, security guard companies, information security companies, and equipment management companies. Include notes on the support agreements and develop a liaison/contact list.
4. Infrastructure significance (CI survey form 4.1-4.3)

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

II. Identify facility, assets, systems, and networks

1. External critical resources (CI survey form 2.2, 5.1-5.7)
   - ● Describe the external critical resource providers (such as electricity, water, gas, transportation, fuel, information providers) that enable the continuous operation of various core function operations. For example, this could be XX substation, XX water purification plant, or XX plant.
   - ● Describe the redundancy status of the facility in the event of failure of external critical resource (such as electricity, water, gas, transportation, fuel, information providers) or other facilities (sub-sector) stop operation. This should include backup facilities, maximum backup duration and contingency plans.
2. Internal necessary assets (CI survey form 6.1-6.3)
   - ●Identify the necessary assets that support the continuous operation of various core function operations and categorize them as physical necessities, personnel, or information and communications.
   - ● Describe the backup status of various necessary assets (physical necessities, personnel, and information and communications), including backup facilities and substitution capacity, maximum backup time, and a description of backup plans.
3. Impact on other critical infrastructures (CI survey form 2.3)
   - ● Describe the impact due to functionally ineffective infrastructures on other types of critical infrastructure and sectors.

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

1. Threat identification

- Identify internal and external hazards and risks (natural disasters, cyberattack incidents, accidents, man-made attacks, emerging threats, non-traditional attacks and military threats, etc.) that pose serious threats to the infrastructure's continuous operation. For each scenario, describe the scale/level/intensity of disaster, time/place of occurrence, and impacted region/number of people. Also evaluate the likelihood of such scenarios.
- Natural disasters: Earthquakes, tsunamis, hurricanes, flooding, droughts, and landslides, etc.
- 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., manslaughter, robbery, burglary, illegal intrusion or sabotage, malicious conduct by employees or contractors), strikes/labor disputes, and riots/demonstrations, terror attacks, military threats, etc.
- 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, the use of products endangering national cyber security.
- Emerging attacks: Unmanned vehicle harassment, AI technology application threats, electromagnetic pulses, gray-zone conflict threats, supply chains disruption, etc.

2. Impact assessment
   - Based on the threat scenarios, assess the internal necessary assets (physical necessities, personnel, information and communications), external critical resources (electricity, water supply, gas supply, transportation, fuel, and information and communications), degree of impact on internal backup systems, and required recovery time, in that order. Then describe the hazards and impacts 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 communications) when a given external critical resource is disrupted (electricity, water supply, gas supply, transportation, fuel, information and communications). 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 communications) and external critical resources based on various disaster threats (natural disasters, cyberattack incidents, accidents, man-made attacks, emerging threats, non-traditional attacks and military threats) shall be laid out in three stages: prevention (including disaster mitigation, preparedness), 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:

1. Prevention stage: operation impact analysis, risk management plan, threat monitoring plan, training plan, various protection plans, cybersecurity plan, rules on confidentiality, mobilize and preparation plan (including manpower, material application and preparedness planning,), asset maintenance/improvement plans, various types of disaster reduction plans and support agreements, etc.
2. Response stage: emergency response plans, various types of crises handling plans, emergency notification, and press release and communication, etc.
3. Recovery stage: continuity of operations plan (COOP), various recovery plans, etc.

VI. Assess implementation results

Describe the exercise/drill plans, operation 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).