附件三修正規定

國家關鍵基礎設施安全防護計畫架構

一、設定安全目標

(一)計畫依據、設施等級與設施基本資料(關鍵基礎設施調查表 1.1-1.4)

- 設施基本資料：說明設施發展背景、基本資料及地理環境等。
- 安全防護與監控：說明設施防護與安全監控(安全警戒、資通安全監控與防護等)情形，包括：人力、管制地點、範圍、設備、運作機制等。

(二)設施安全防護目標(關鍵基礎設施調查表 2.1)

- 安全防護目標：說明設施防護的安全目標，如：「功能持續運作」、降低災害風險、提升耐災能力、縮短復原時間、降低災損等。
- 核心功能業務：說明設施的核心功能業務，辨識各項核心功能業務的最大容許中斷時間，說明設施各項核心功能業務的可替代性（如:替代設施、替代方案等）。

(三)關鍵基礎設施防護管理團隊(關鍵基礎設施調查表 3.1-3.2)

- 辨識共同管理單位：在設施範圍內，辨識支持設施核心功能業務運作的共同管理單位，說明各單位所支持的核心功能業務。
- 關鍵基礎設施防護管理團隊：依據所辨識的共同管理單位，建立關鍵基礎設施防護管理團隊名單。
- 辨識外部安全防護支援單位：說明外部安全防護支援單位及所支援事項，例如：地方政府、警消、醫療、國軍、重要供應商、保全公司、資安公司、設備管理公司等，註記支援協定情況，並建立聯絡窗口名單。

(四)設施重要性(關鍵基礎設施調查表 4.1-4.3)

- 政府功能重要性:說明本設施對於國家與社會重要功能任務之重要性,包括:政府部會指管、重要資通訊、維生與運輸機能、金融秩序、疫病系統、治安與防救、國家重要象徵與資產、重要產業與園區、防衛動員等。
- 設施失效對於社會經濟影響:說明設施總價值,設施失效影響人數、經濟損失。
- 設施失效對於民心士氣影響:說明設施失效對於國際形象、政府聲譽、民眾信心的影響程度。

二、辨識設施資產、系統與網絡

(一)外部關鍵資源(關鍵基礎設施調查表 2.2、5.1-5.7)

- 說明支持各項核心功能業務持續運作的外部關鍵資源(電力、供水、供氣、交通、燃料、資通訊)供應者,例如:xx 變電站、xx 淨水場、xx 機房。
- 說明外部關鍵資源(電力、供水、供氣、交通、燃料、資通訊)失效時,或其他設施(次領域)停止運作,設施本身的備援狀態,包括:哪些備援設施、最大備援時間、備援方案等。

(二)內部必要資產(關鍵基礎設施調查表 6.1-6.3)

- 辨識支持各項核心功能業務持續運作的必要資產,以實體、人員、資通訊三大類進行說明。
- 說明各項必要資產(實體、人員、資通訊)的備援狀態,包括:備援設施與替代程度、最大備援時間,以及備援方案說明。

(三)對其他關鍵設施的影響(關鍵基礎設施調查表 2.3)

- 說明當本設施失效後會影響哪些其他關鍵基礎設施與部門。

三、風險評估(威脅、脆弱性以及災害衝擊)

(一)威脅辨識

- 辨識足以對於設施持續運作造成嚴重威脅之內部與外部的危

害項目與全災害風險(天然災害、資安攻擊、意外事件、人為攻擊、新興威脅、非傳統攻擊及軍事威脅等災害)，情境內容說明包括災害規模/程度/強度、發生時間/地點、影響區域範圍/人數等，並評估該情境發生的可能性。

- ■ 天然災害：地震、海嘯、風災、淹水、旱災、坡地災害等。
- ■ 人為災害：疫病/傳染病、火災、爆炸、輻射災害、化學災害、設備管理(例如：設備老舊、人為操作疏失等)、危安事件(例如：殺人、搶奪、竊盜、違法入侵或破壞、所屬員工或委外人員之惡意作為等)、 罷工/勞資爭議、暴動/陳抗事件、恐怖攻擊、軍事威脅等。
- ■ 資安事件：業務服務失效(中斷/無法控制)、系統硬體設施停止運作/無法控制、軟體應用程式執行中斷/無法控制、重要電子資料遭竊取/遺失/毀損、使用危害國家資通安全產品等。
- ■ 新興威脅：無人載具襲擾、人工智慧技術應用威脅、電磁脈衝、灰色地帶行動威脅、原物料供應斷鏈等。

(二)衝擊評估

- ● 依照所建立之各項威脅情境，依序評估對各項內部必要資產(實體、人員、資通訊)、外部關鍵資源(電力、供水、供氣、交通、燃料、資通訊)、內部各項備援設施受影響程度以及所需復原時間，據以建立並說明該項威脅情境對本關鍵基礎設施所造成的災害與衝擊。

(三)關鍵資源中斷影響

- ● 依序評估某項外部關鍵資源中斷下(電力、供水、供氣、交通、燃料、資通訊)，對設施各項必要資產(實體、人員、資通訊系統)的影響程度以及剩餘運作時間，據以建立並說明當該項外部關鍵資源中斷時對本關鍵基礎設施的影響情境。

四、決定防護優先次序

(一)以風險評估結果，辨識各類災害的威脅程度，辨識設施各項核心功能業務、必要資產以及關鍵資源在不同災害類別影響下的失效風險。

(二)分析現有防護程度與備援在各類災害衝擊下是否滿足所設定之安全目標以及復原時間，進而擬定減災策略與優先防護強化項目，如：實體補強、資安防護、人員訓練或是維安強化等。

五、實施防護管理計畫

符合風險評估結果以及防護強化優先次序，分別以預防(含減災、整備)、應變、復原三個階段，依各項災害威脅(天然災害、資安攻擊、意外事件、人為攻擊、新興威脅、非傳統攻擊及軍事威脅等災害)分別表列說明對於內部必要資產(實體、人員、資通訊)與外部關鍵資源的防護管理項目與執行重點，並註明相關防護管理實施計畫。對應各項災害威脅，擬訂之各類計畫可以下列方式依序整理說明:

- 預防階段：營運衝擊分析、風險管理計畫、威脅監控計畫、訓練計畫、各類防護計畫、資安計畫、保密規定、動員整備計畫(含人力、物力申請及整備規劃)、資產維護/改善計畫、各類減災計畫、支援協定等。
- 應變階段：緊急應變計畫、各類危機處理計畫、緊急通報、新聞發布與管制、營運能量保存及移轉計畫等多元防護計畫。
- 復原階段：持續運作計畫、各類復原計畫等。

六、衡量實施成效

說明衡量各類計畫與標準操作程序(SOP)實施成效的演練計畫、工作項目、衡量頻率與依據、檢討與改善項目、改善進度掌握與追蹤，註記相關實施紀錄。