**「現存機關安全威脅及應有防處作為」課程重點摘要**

**講座：國家安全會議郭諮詢○○**

**一、建立工作方法與防護機制：**

推動與做好機關安全維護工作，應先考量以何種觀念檢視需要處理的問題，要注意哪些事項，涵蓋面相有多廣，進而建立工作方法與防護機制。

**二、進行「風險評估」與檢視「威脅圖像」：**

1. **風險評估：**面對安全威脅應先進行「風險評估」，包括整體架構、面臨何種威脅、知悉本身弱點及規劃防護工作等。
2. **威脅圖像：**首先整理流程，再檢視每個環節面臨的威脅，透過「威脅圖像」（哪些行為態樣可能危害「國家安全」、「經濟發展」與「社會穩定」）來思考安全維護風險控制。

**三、安全維護工作要守護什麼？**

除建立威脅圖像外，其次要瞭解機關安全維護要守護的重點資產是什麼？「有形」資產，包括人員、功能、服務、網路系統、硬體設施或重要財產等；更重要的是「無形」資產（包含：政府形象、民眾信心、設施功能之韌性、核心機密之維護等。）如今網路發達，倘機密遭竊，將嚴重影響機關形象，若系統功能喪失將無法即時提供民眾服務等，這都是安全維護工作要守護的目標。

**四、「多層次安全防禦」觀念：**

機關安全三環節包括人員、實體及網路，三環節間緊緊相扣，缺一不可，如突破一環節，安全皆失守，因此內外部人員、實體防護及資安系統應相互整合，並瞭解哪個部分需設置偵測機制以防禦風險。

1. **人員安全：**
2. **掌握機密維護基本資訊：**

機密核定與分級應有明確標準，倘發現洩密案件，得據以迅速判斷是否涉及機密；其機密等級、接觸或保管人員，係機密維護須基本掌握之資訊。

1. **人員安全查核：**

人員有權限傳遞資訊者，是否經過安全查核，權限清單應進行列管，及協調權管單位加強檢視得接觸機密之人員，並應思考有關「接密權限」之授權是否適當？權限之後續管理是否落實？辦理機敏性資訊採購時，對投標廠商資格與背景應明確規範，避免承包商洩漏機關通訊網路架構，致生機關資安漏洞，並注意其專案與派遣人員管理，及包商人員接觸核心機密之陪同與管理機制。

1. **人員與海外風險：**

對外交人員派駐海外高風險區域，應適時告知可能遭遇之風險，注意機敏性訊息之保密措施，避免遭刺探國家機密；人員赴海外開會或旅宿，連接WIFI或使用3C電子用品，易遭偷竊公務資料，應加強宣導注意資訊安全，以避免機密外洩。

1. **實體安全**：

機關安全維護工作實體面，如機關安全、機密文件存放等，需檢視是否符合相關政策防制與規定；以機場安全維護為例，美國政府在911事件後，建置許多關卡以強化飛航安全，機關安全維護亦可區分多層次，形成滴水不漏堅固防護網絡。

1. **網路與資訊系統安全**：
2. 政府機關面臨最大的安全威脅是網路，應獨立網路安全加以防範，釐清哪些人員有權限存取資料？或注意是否有員工離職前大量備份資料等可疑行為，各機關務必要重視網路安全。
3. 現今工業控制系統遭入侵事件頻傳，各公營事業機構需重視關鍵基礎設施控制系統之安全性。

**五、反思與策進：**

1. **我們對於威脅有無共識?**

透過本次講習提醒大家去檢視對於威脅要有共識。

1. **各單位是否掌握安全圖像?**

各機關、單位之安全圖像都不同，如何加以拼湊，並解決各單位間資訊共享的問題。

1. **有無建置緊急應變流程?**

除機關首長掌握緊急應變流程外，應瞭解負責應變計畫的單位與如何落實執行。

1. **利用多元系統工具:**

利用大數據分析、輿情媒體資訊及新科技等克服人力不足，以解決機關安全問題。

1. **爭取長官支持：**

需爭取長官支持，方可取得各單位資訊，順利推動機關安全維護工作。

1. **情報整合、分享:**

可請長官召集各單位分享整合資訊，或考量如何建立機制使資訊相互分享，才能圓滿完成維護工作。