

2026 城鎮韌性(資安防護)演習 實施計畫

壹、依據

- 一、2026 城鎮韌性演習訓令。
- 二、行政院函頒「國家關鍵基礎設施安全防護指導綱領」及附件四「國家關鍵基礎設施防護演習指導手冊」(114 年 11 月 13 日修正版)。
- 三、2025 年行政院全社會防衛韌性工作小組第 6 次會議裁示事項。

貳、演習目的

- 一、檢視縣市政府機關(構)及關鍵基礎設施提供者(下稱 CIP)對外服務系統與連網設備之防護能力，強化政府機關及關鍵基礎設施資安防禦及應變能力。
- 二、驗證縣市政府機關(構)及關鍵基礎設施提供者所轄對外資通系統發生資安事件之緊急應變、系統復原及協調管控等能力。

參、實施構想

- 一、綜合實作階段以實兵演練方式執行：由數位發展部資通安全署(以下簡稱資安署)統籌編成演練團隊，模擬駭客實際攻擊手法，以弱點掃描、滲透測試等方式嘗試取得演練機關內部機敏資料或資通系統控制權限等，在不影響演練機關業務正常運作情況下，檢視機關對外服務系統與連網設備對機密性或完整性之防護能力。
- 二、實際發布資安警訊，並進行通報及應變程序：演練機關於演練期間接獲資安告警訊息，須按資通安全管理法規定，依資通系統受影響程度進行通報與漏洞修補，藉此強化各演練機關資安防護、通報應變及系統復原等各面向能力，檢視各演練機關人員防護意識。

肆、演習編組

依循 2026 城鎮韌性演習訓令之編組體系，區分指導組、統裁部，有關資安防護演習編組及分工說明如下：

一、指導組：

行政院國土安全辦公室(下稱國土辦)訂頒 2026 城鎮韌性(資安防護)演習實施計畫。

二、統裁部：

- (一)配合全民防衛動員演習規劃，指導縣市政府機關(構)城鎮韌性演習資安實兵演練事宜。
- (二)國土辦擇選年度參演縣市及 CIP，指導城鎮韌性演習資安實兵演練事宜。
- (三)由資安署統籌編成資安實兵演練團隊(以下簡稱演練團隊)，召集國安、國防、學術、資安業者等滲透人員組成攻擊手團隊，模擬駭客實際攻擊手法，以弱點掃描、滲透測試等方式，針對直轄市、縣市政府、擇定之 CIP 進行攻擊，檢視機關對外服務系統與連網設備對機密性或完整性之防護能力。

伍、實施方式

- 一、4 月至 8 月間配合參演城鎮韌性(全民防衛動員、關鍵基礎設施防護)演習之 11 個縣市政府機關(構)與 CIP(時程如附件 1)同步辦理演習，另配合城鎮韌性(關鍵基礎設施防護)演習主管機關於各參演縣市指定 1 處 CIP 實施院級檢核(如附件 2)。

二、執行方式：

(一)綜合實作前：

- 1.演習當年度 2 至 3 月，資安署將函請演練機關填報「演練基本調查表」及系統設備、網站清冊等資訊，以確認攻擊範圍。
- 2.綜合實作前，演練攻擊手將開始執行攻擊，蒐集機關弱點；兵棋推演前 1 日行政院國土安全辦公室與資安署共同討

論並擇定具有代表性之弱點(至多 3 則)。

(二)綜合實作當日：

- 1.原則於當日上午 9 時(得依狀況調整)實施推演，於下午 5 時前結束，演練結束後視況參與城鎮韌性演習指導官講評會議。
- 2.當日上午 9 時起，由資安署發送「INT-系統入侵」(Intrusion Alert)警訊。
- 3.機關(構)接獲資安警訊後應開始進行事件通報(至國家資通安全通報應變網站)並進行處置，依其機密性、完整性及可用性受影響程度評估資安事件等級，並依資通安全法及其子法等規定，於時間內完成通報作業及損害控制或復原作業。
- 4.機關(構)應於綜合實作當日下午向指揮官說明因應實兵攻防演練之資安防護作為，並說明接獲實兵演練警訊之過程、分析重點、應處結果及針對本件弱點的後續改善精進措施；倘未有弱點遭受攻擊，則須說明機關(構)資安防護作為。有關前開所載須說明之資安防護作為內容包含但不限於資安事件通報及應變組織與程序、營運持續運作計畫(含演練情形)、核心資通系統防護機制、最近一次通報演練與社交工程演練執行情形、委外廠商管理機制。
- 5.若演練機關發現已遭攻擊手團隊攻擊成功，並於資安署發布警訊前即自行通報成功，演練當日機關須說明因應實兵攻防演練資安防護相關作為、如何主動發現遭攻擊手團隊攻擊成功過程、分析重點、應處結果及針對弱點的後續改善精進措施，並納入評核表現。

陸、演練重點：

除配合城鎮韌性(全民防衛動員、關鍵基礎設施防護)演習演練課目共同演練外，演練重點如次：

一、清冊正確率。

- 二、清冊回復時間。
- 三、通報登錄時間。
- 四、資安事件等級正確率。
- 五、建立通報應變組織與程序。
- 六、踐行通報應變程序。
- 七、防護能力。
- 八、營運持續運作計畫(含演練)。
- 九、核心業務防護機制。
- 十、最近一次通報演練與社交工程演練執行情形。
- 十一、委外廠商管理機制。

柒、督導考評：

配合城鎮韌性(全民防衛動員、關鍵基礎設施防護)演習辦理評核，檢核表配合城鎮韌性演習採紅、黃、綠燈評比法(RAG指標)如附件 3 檢核表。

捌、一般注意事項

- 一、實兵攻防演練攻擊手團隊執行遠端攻擊行為，所有攻擊行為皆會被即時監控與記錄。
- 二、攻防演練以不影響演練機關業務正常運作為原則。
- 三、不提供攻擊來源 IP。
- 四、演練機關應與其資安維護廠商共同進行防禦與事件分析，若發現資通系統實兵演練攻擊行為，致使受測目標遭受影響，應至國家資通安全通報應變網站進行通報。
- 五、本演習參與人員(含演習評核委員)應恪遵公務人員廉政倫理規範、利益迴避及保密規定。
- 六、演習機關(構)如接獲非屬上級機關、單位欲觀摩者，應評估該單位特性並排除洩密疑慮，如允許觀摩應請其簽署保密協定，且演習過程限制拍攝、錄音、照相或攜出任何書面資料。
- 七、本實施計畫若有未盡事宜，另函(令)補充修正之。

玖、聯絡窗口：

國土辦資安分組：

一、黃科長筠媛、謝分析師美珍

二、電話：02-3356-7853、02-33567852

三、Email：yyhuang3@ey.gov.tw、mchsieh@ey.gov.tw

拾、附件表單：

附件 1. 2026 城鎮韌性演習日程規劃表

附件 2. 2026 城鎮韌性演習遴選關鍵基礎設施清單（去識別化）

附件 3. 2026 城鎮韌性資安防護實兵演習檢核表單

附件 1：2026 城鎮韌性演習日程規劃表

月	星期一	星期二	星期三	星期四	星期五	星期六	星期日
四月	20	21	22 彰化縣兵推	23 彰化縣實作	24	25	26
	27	28	29	30			
五月					1 勞動節	2	3
	4	5	6	7	8	9	10
	11	12	13 苗栗縣兵推	14 苗栗縣實作	15	16	17
	18	19	20 新竹縣兵推	21 新竹縣實作	22	23	24
	25	26	27 嘉義縣兵推	28 嘉義縣實作	29	30	31
六月	1	2	3 桃園市兵推	4 桃園市實作	5	6	7
	8	9	10	11	12	13	14
	15	16	17	18	19 端午節	20	21
	22	23	24 雲林縣兵推	25 雲林縣實作	26	27	28
	29	30					
七月			1 南投縣兵推	2 南投縣實作	3	4	5
	6	7	8	9	10	11	12
	13	14	15	16	17	18	19
	20	21	22	23	24	25	26
	27	28	29	30	31		
八月						1	2
	3	4	5	6 高雄市、 屏東縣兵推	7 高雄市、 屏東縣實作	8	9
	10	11	12 新北市、 宜蘭縣兵推	13 新北市、 宜蘭縣實作	14	15	16

附件 2：2026 城鎮韌性演習參演關鍵基礎設施提供者清單

所在縣市(演習時間)	院級指定評核 CIP (去識別化)
彰化縣(4/22、23)	醫療照護設施
苗栗縣(5/13、14)	電力設施
新竹縣(5/20、21)	供水設施
嘉義縣(5/27、28)	醫療照護設施
桃園市(6/3、4)	醫療照護設施
雲林縣(6/24、25)	醫療照護設施
南投縣(7/1、2)	醫療照護設施
高雄市(8/6、7)	醫療照護設施
屏東縣(8/6、7)	醫療照護設施
新北市(8/12、13)	醫療照護設施
宜蘭縣(8/12、13)	醫療照護設施

2026 城鎮韌性演習資安防護實兵演習檢核表單		
演習單位類別： ☐ 關鍵基礎設施 ☐ 縣市政府		
檢核人員：		實施日期：115 年 月 日
檢核項目	狀態(RAG)	狀態定義及說明
1. 清冊正確率	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)提供完整對外服務系統與連網設備清冊。 A：機關(構)遺漏 1 筆對外服務系統與連網設備未納入清冊。 R：機關(構)遺漏 1 筆以上對外服務系統與連網設備未納入清冊。
2. 清冊回復時間	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)於數發部資安署指定期限內回復(截止日 24 時前)。 A：機關(構)於數發部資安署指定期限日後 20 個工作日內回復。 R：機關(構)於數發部資安署指定期限日後 20 個工作日以上回復。
3. 通報登錄時間	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)於警訊發布前已自行至通報應變網站進行通報。 A：機關(構)於警訊發布後 1 小時內至通報應變網站進行通報。 R：機關(構)於警訊發布後 1 小時以上至通報應變網站進行通報。
4. 資安事件等級正確率	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)通報之資安事件等級與實際情形相符。 A：機關(構)通報之資安事件等級與實際情形不相符，但經數發部資安署通知後修改為正確之資安事件等級。 R：機關(構)通報之資安事件等級與實際情形不相符，經數發部資安署通知後仍未修改為正確之資安事件等級。
5. 建立通報應變組織與程序	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)有建立資安事件通報應變小組，以及小組分工、事件應變會議、辦理損害控制或復原作業之程序。 A：機關(構)有建立資安事件通報應變小組，以及小組分工、事件應變會議、辦理損害控制或復原作業之程序，前開程序有漏未建立者。 R：機關(構)未建立資安事件通報應變小組，以及小組分工、事件應變會議、辦理損害控制或復原作業之程序。

6. 踐行通報應變程序	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)依通報應變處理作業程序成立通報應變小組，與召開事件應變會議、辦理損害控制或復原作業。 A：機關(構)依通報應變處理作業程序成立通報應變小組，與召開事件應變會議、辦理損害控制或復原作業，前開程序有漏未辦理者。 R：機關(構)未依通報應變處理作業程序成立通報應變小組，與召開事件應變會議、辦理損害控制或復原作業。
7. 防護能力-重大衝擊弱點	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)對外服務系統無重大衝擊弱點。 A：機關(構)對外服務系統有 1 筆重大衝擊弱點。 R：機關(構)對外服務系統有 2 筆(含)以上重大衝擊弱點。
8. 防護能力-高中低衝擊弱點	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)對外服務系統無任何高、中、低衝擊弱點。 A：機關(構)對外服務系統僅有 1 筆低衝擊弱點。 R：機關(構)對外服務系統有 2 筆(含)以上低衝擊弱點，或有 1 筆(含)以上高、中衝擊弱點。
9. 營運持續運作計畫(含演練)	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)針對核心資通系統擬定營運持續運作計畫並定期進行演練，營運持續計畫內容至少包含人員職責應變、作業程序、資源調度機制及檢討改善措施等。 A：機關(構)針對核心資通系統應擬定營運持續運作計畫並定期進行演練，營運持續計畫內容至少包含人員職責應變、作業程序、資源調度機制及檢討改善措施等，前開事項缺漏一項者。 R：機關(構)針對核心資通系統未擬定營運持續運作計畫且未定期進行演練，營運持續計畫內容至少包含人員職責應變、作業程序、資源調度機制及檢討改善措施等。 備註：營運持續運作計畫演練頻率為 A 級機關每年 1 次；B、C 級機關每 2 年 1 次。
10. 核心業務防護機制	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：針對核心業務訂定最大可容忍中斷時間(MTPD)，並至少針對防護需求為中等級以上之資通系統，訂定從中斷後至重新恢復服務之可容忍時間要求(RTO)，及可容忍資料損失之時間要求(RPO)，並針對防護需求為中等級以上資通系統之備份資訊，定期測試備份資訊；且於可容忍時間內，由備援設備或其他方式取代並提供服務。 A：針對核心業務訂定最大可容忍中斷時間(MTPD)，並至少針對防護需求為中等級以上之資通系統，訂定從中

		斷後至重新恢復服務之可容忍時間要求(RTO)，及可容忍資料損失之時間要求(RPO)，並針對防護需求為中等級以上資通系統之備份資訊，定期測試備份資訊；且於可容忍時間內，由備援設備或其他方式取代並提供服務。前開事項缺漏一項者。 R：針對核心業務訂定最大可容忍中斷時間(MTPD)，並至少針對防護需求為中等級以上之資通系統，訂定從中斷後至重新恢復服務之可容忍時間要求(RTO)，及可容忍資料損失之時間要求(RPO)，並針對防護需求為中等級以上資通系統之備份資訊，定期測試備份資訊；且於可容忍時間內，由備援設備或其他方式取代並提供服務。前開事項缺漏兩項(含)以上者。
11. 最近一次通報演練與社交工程演練執行情形	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)演練範圍涵蓋全部所屬單位，且演練結束針對結果檢討、訂出改善計畫並確實管考執行進度 A：機關(構)演練範圍涵蓋全部所屬單位，惟演練結束未針對結果檢討、訂出改善計畫或確實管考執行進度 R：演練範圍未涵蓋全部所屬單位。
12. 委外廠商管理機制	☐ G(綠燈) ☐ A(黃燈) ☐ R(紅燈)	G：機關(構)針對資訊系統委外廠商管理有建立資通安全管理機制，並亦將委外廠商納入營運持續運作演練範圍。 A：機關(構)針對資訊系統委外廠商管理有建立資通安全管理機制，並亦將委外廠商納入營運持續運作演練範圍，前開事項缺漏一項者。 R：機關(構)針對資訊系統委外廠商管理未有建立資通安全管理機制，亦未將委外廠商納入營運持續運作演練範圍。
綜合建議		
檢核說明	一、倘未有弱點遭受攻擊之機關(構)於項目 3、4、5、6 皆以綠燈計。 二、項目分類：關鍵項目—第 1、3、4、5、6、7、8、9、11 項；必要項目—第 2、10、12 項。 三、評核等級區分： (一)優良：關鍵項目均為綠燈(G)，必要項目未有紅燈(R)。 (二)合格：總燈數黃燈(A)最多 <u>2</u> 個。 (三)待改進：紅燈(R)具 <u>1</u> 個以上，或皆為黃燈(A)。	