

資通安全事件通報及應變辦法草案總說明

「資通安全管理法」(以下簡稱本法)業於一百零七年六月六日制定公布。為使各受規範對象得妥適辦理資通安全事件之通報及應變，以降低資通安全事件之發生機率，或於發生資通安全事件時可迅速妥適因應，而有效降低損害，本法第十四條第四項及第十八條第四項明定主管機關應訂定資通安全事件之通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項。爰擬具「資通安全事件通報及應變辦法」(以下簡稱本辦法)草案，其要點如下：

- 一、本辦法之授權依據。(草案第一條)
- 二、資通安全事件之分級。(草案第二條)
- 三、資通安全事件之通報項目。(草案第三條)
- 四、公務機關資通安全事件之通報方式、時限及程序。(草案第四條)
- 五、公務機關資通安全事件等級之審核、時限及程序。(草案第五條)
- 六、公務機關資通安全事件之應變方式、時限及程序。(草案第六條)
- 七、公務機關資通安全事件之支援或協助事宜。(草案第七條)
- 八、公務機關資通安全演練作業之規劃、辦理及其內容。(草案第八條)
- 九、公務機關應就資通安全事件之通報及應變訂定作業規範，及其應包括事項。(草案第九條及第十條)
- 十、特定非公務機關資通安全事件之通報方式、時限及程序。(草案第十一條)
- 十一、特定非公務機關資通安全事件等級之審核、時限及程序。(草案第十二條)
- 十二、特定非公務機關資通安全事件之應變方式、時限及程序。(草案第十三條)
- 十三、特定非公務機關資通安全事件之支援或協助事宜。(草案第十四條)
- 十四、特定非公務機關應就資通安全事件之通報及應變訂定作業規範，及其應包括事項。(草案第十五條及第十六條)
- 十五、主管機關對於重大資通安全事件之因應。(草案第十七條)
- 十六、公務機關與特定非公務機關應配合主管機關規劃辦理之資通安全

演練作業及其得包括之內容。(草案第十八條及第十九條)

十七、公務機關或特定非公務機關就資通安全事件之通報及應變，得不適用本辦法規定之例外情形。(草案第二十條)

十八、本辦法之施行日期。(草案第二十一條)

資通安全事件通報及應變辦法草案

條文	說明
第一章 總則	章名。
第一條 本辦法依資通安全管理法（以下簡稱本法）第十四條第四項及第十八條第四項規定訂定之。	明定本辦法訂定之依據。
<p>第二條 資通安全事件分為四級。</p> <p>公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件：</p> <p>一、非核心業務資訊遭輕微洩漏。</p> <p>二、非核心業務資訊或非核心資通系統遭輕微竄改。</p> <p>三、非核心業務或非核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。</p> <p>各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件：</p> <p>一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。</p> <p>二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。</p> <p>三、非核心業務或非核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。</p> <p>各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：</p> <p>一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊</p>	<p>一、考量不同資通安全事件對公務機關或特定非公務機關（以下簡稱各機關）造成之影響或損害程度不同，爰以資通安全事件之性質及業務實際受影響之程度等因素作為判斷標準，將資通安全事件區分為四個等級，於第一項明定資通安全事件之分級，並於第二項至第五項分別規定第一級至第四級資通安全事件之情形。</p> <p>二、所稱核心業務，依資通安全管理法施行細則第七條第一項及同條第二項之規定；所稱核心資通系統，依資通安全管理法施行細則第七條第三項之規定，併予敘明。</p> <p>三、所稱一般公務機密，參考行政院訂定之文書處理手冊第五十一點規定，係指公務機關持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。</p> <p>四、所稱敏感資訊，指包含個人資料等非一般公務機密或國家機密之資訊，如遭洩漏可能造成機關本身或他人之損害或困擾，而具保護價值之資訊。</p> <p>五、所稱國家機密，依國家機密保護法第二條規定，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依該法核定機密等級者。</p>

<p>遭輕微洩漏。</p> <p>二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。</p> <p>三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。</p> <p>各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件：</p> <p>一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。</p> <p>二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。</p> <p>三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。</p>	
<p>第三條 資通安全事件之通報內容，應包括下列項目：</p> <p>一、發生機關。</p> <p>二、發生時間。</p> <p>三、狀況之描述。</p> <p>四、等級之評估。</p> <p>五、因應事件所採取之措施。</p> <p>六、外部支援需求評估。</p> <p>七、其他相關事項。</p>	<p>為強化資通安全事件之管理、追蹤及加速處理之效率，爰明定各機關辦理資通安全事件通報作業之基本通報項目。</p>
<p>第二章 公務機關資通安全事件之通報及應變</p>	<p>章名。</p>
<p>第四條 公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通</p>	<p>一、第一項明定公務機關辦理資通安全事件之通報，應於知悉後一小時內依主管機關指定之方式及對象為</p>

<p>報。</p> <p>前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。</p> <p>公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。</p> <p>公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。</p>	<p>之。</p> <p>二、考量公務機關可能於辦理完成資通安全事件之通報後，始發現資通安全事件等級須變更，為確保其上級、監督機關或主管機關知悉該情事，並能對之為本辦法所定之審核、複核及提供必要之協助，爰於第二項規定已依第一項規定通報之資通安全事件，如發生等級變更之情事，該公務機關應依第一項規定續行通報。</p> <p>三、考量如有天災、事變或其他事故，可能發生網路或電力中斷等情形，致公務機關無法利用經指定之方式（例如通報應變網站）進行資通安全事件之通報，爰於第三項規定因故無法依指定方式通報時，公務機關應依其他適當方式進行通報，並註記說明阻礙通報之事由。</p> <p>四、第四項規定公務機關於阻礙依指定方式通報之事由解除後，仍應依主管機關指定之方式補行通報。</p>
<p>第五條 主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：</p> <p>一、通報為第一級或第二級資通安全事件者，於接獲通報後八小時內。</p> <p>二、通報為第三級或第四級資通安全事件者，於接獲通報後二小時內。</p> <p>總統府與中央一級機關之直屬機關（構）及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，完成資通安全事件之通報後，依前項規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級。</p> <p>前項機關依規定完成資通安全事件等級之審核後，應於一小時內將審</p>	<p>一、考量公務機關於進行資通安全事件之通報時，因受限於時間急迫或其他因素，就資通安全事件等級之判斷或有不適當之情形，爰於第一項明定主管機關對於其自身之資通安全事件審核，並於第二項規範總統府與中央一級機關之直屬機關（構）及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，通報資通安全事件後，依規定之時限完成對該資通安全事件等級之審核，並得依審核結果變更其等級。</p> <p>二、為使主管機關得掌握資通安全事件之情況，以利適時提供必要協助，爰於第三項規定第二項之機關完成資通安全事件等級之審核後，應於一小時內將審核結果及相關資訊通知主管機關，以利主管機關進行後</p>

<p>核結果通知主管機關，並提供審核依據之相關資訊。</p> <p>總統府、國家安全會議、立法院、司法院、考試院、監察院、省諮議會及直轄市、縣（市）議會，應於其自身完成資通安全事件之通報後，依第一項規定時間完成該資通安全事件等級之審核，並依前項規定通知主管機關及提供相關資訊。</p> <p>主管機關接獲第三項及前項之通知後，應依相關資訊，就資通安全事件之等級進行複核，並得依複核結果變更其等級。但主管機關認有必要，或第二項及前項機關未依規定通知審核結果時，得就該資通安全事件逕為審核，並得為等級之變更。</p>	<p>續之複核。</p> <p>三、第四項明定總統府、國家安全會議、立法院、司法院、考試院、監察院、省諮議會及直轄市、縣（市）議會資通安全事件等級之審核及通知主管機關等程序。</p> <p>四、第五項明定主管機關得就各公務機關資通安全事件之等級進行複核。另考量部分資通安全事件之急迫性與時效性，及避免相關機關未能於規定時限內完成資通安全事件等級之審核致貽誤時效，爰明定主管機關認有必要，或第二項及第四項機關未依規定通知審核結果時，得就該資通安全事件逕為審核，並得為等級之變更。</p>
<p>第六條 公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：</p> <p>一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。</p> <p>二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。</p> <p>公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。</p> <p>前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。</p> <p>上級、監督機關或主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。</p>	<p>一、第一項明定公務機關於知悉資通安全事件後，應視該事件之等級，於時限內完成損害控制或復原作業及通知事宜。</p> <p>二、為使公務機關對於資通安全事件儘速妥適處理，於第二項及第三項明定公務機關完成第一項所定資通安全事件之損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並應於一個月內依主管機關指定之方式，送交調查、處理及改善報告；另得經其上級或監督機關及主管機關同意後延長上開時限。</p> <p>三、為強化公務機關之資通安全管理，爰於第四項規定上級、監督機關或主管機關就第二項之調查、處理及改善報告認為有必要，或認有違法或不當等情事者，得要求該公務機關提出說明及調整。</p>
<p>第七條 總統府與中央一級機關之直屬機關（構）及直轄市、縣（市）政府，就所屬、監督、所轄或業務相關之公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協</p>	<p>一、考量公務機關執行資通安全事件之通報及應變作業時，依其所能使用之資源，或有無法適時完成各項要求之可能；或有數公務機關同時發生類似資安事件，需上級、監督機</p>

<p>助。</p> <p>主管機關就公務機關執行資通安全事件之應變作業，得視情形提供必要支援或協助。</p> <p>公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。</p>	<p>關或主管機關協助資通安全事件應變之可能；爰於第一項規定總統府與中央一級機關之直屬機關（構）及直轄市、縣（市）政府，應視情形提供資通安全事件通報及應變作業必要支援或協助，並於第二項規定主管機關得視情形提供資通安全事件通應變作業必要支援或協助，以利各公務機關順利完成相關作業。</p> <p>二、考量第三級或第四級資通安全事件影響層面、可能發生之損害皆較嚴峻，爰於第二項明定公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。</p>
<p>第八條 總統府與中央一級機關之直屬機關（構）及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關、前開鄉（鎮、市）、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。</p> <p>前項演練作業之內容應至少包括下列項目：</p> <p>一、每半年辦理一次社交工程演練。</p> <p>二、每年辦理一次資通安全事件通報及應變演練。</p> <p>總統府與中央一級機關、省諮議會及直轄市、縣（市）議會，應依前項規定規劃及辦理資通安全演練作業。</p>	<p>一、考量資通安全演練作業係屬資通安全事件應變機制之一環，為使公務機關於資通安全事件發生時得妥適進行相關應對措施，爰於第一項規定總統府與中央一級機關之直屬機關（構）及直轄市、縣（市）政府應規劃並辦理其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關、前開鄉（鎮、市）、直轄市山地原住民區民代表會之資通安全演練作業，並於第二項明定資通安全演練作業之基本內容。</p> <p>二、總統府與中央一級機關、省諮議會及直轄市、縣（市）議會，亦應辦理資通安全演練作業，以利資通安全事件發生時得妥為應對，爰為第三項規定。</p>
<p>第九條 公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：</p> <p>一、判定事件等級之流程及權責。</p> <p>二、事件之影響範圍、損害程度及機關因應能力之評估。</p> <p>三、資通安全事件之內部通報流程。</p> <p>四、通知受資通安全事件影響之其</p>	<p>為確保公務機關於知悉資通安全事件後，得依本辦法規定迅速進行通報及適當之處置，爰為本條規定。各公務機關訂定資通安全事件之通報作業規範時，應考量其機關特性、資源及其他需求等因素，依本條規定為之。</p>

<p>他機關之方式。</p> <p>五、前四款事項之演練。</p> <p>六、資通安全事件通報窗口及聯繫方式。</p> <p>七、其他資通安全事件通報相關事項。</p>	
<p>第十條 公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：</p> <p>一、應變小組之組織。</p> <p>二、事件發生前之演練作業。</p> <p>三、事件發生時之損害控制機制。</p> <p>四、事件發生後之復原、鑑識、調查及改善機制。</p> <p>五、事件相關紀錄之保留。</p> <p>六、其他資通安全事件應變相關事項。</p>	<p>為確保公務機關於發生資通安全事件後，得依本辦法規定迅速且確實進行資通安全事件之應變，爰為本條規定。</p>
<p>第三章 特定非公務機關資通安全事件之通報及應變</p>	<p>章名。</p>
<p>第十一條 特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。</p> <p>前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。</p> <p>特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。</p> <p>特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。</p>	<p>一、第一項明定特定非公務機關辦理資通安全事件通報之方式與時限。</p> <p>二、考量特定非公務機關可能於辦理完成資通安全事件之通報後，始發現資通安全事件等級須為變更，為確保中央目的事業主管機關知悉該情事，並能對之為本辦法所定之審核及提供必要之協助，爰於第二項規定已依第一項規定通報之資通安全事件，如發生等級變更之情事，該特定非公務機關應依第一項規定續行通報。</p> <p>三、考量如因天災、事變或其他因素，可能發生網路或電力中斷之情形，致特定非公務機關無法依經指定之方式（例如通報應變網站）進行資通安全事件之通報，爰於第三項規定，因故無法依指定方式通報時，特定非公務機關應依其他適當方式通報中央目的事業主管機關，並註記說明阻礙通報之事由。</p> <p>四、第四項規定特定非公務機關於阻礙依指定方式通報之事由解除後，仍應依中央目的事業主管機關指定之方式補行通報。</p>

<p>第十二條 中央目的事業主管機關應於特定非公務機關完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：</p> <p>一、通報為第一級或第二級資通安全事件者，於接獲通報後八小時內。</p> <p>二、通報為第三級或第四級資通安全事件者，於接獲通報後二小時內。</p> <p>中央目的事業主管機關依前項規定完成資通安全事件之審核後，應依下列規定辦理：</p> <p>一、審核結果為第一級或第二級資通安全事件者，應定期彙整審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。</p> <p>二、審核結果為第三級或第四級資通安全事件者，應於審核完成後一小時內，將審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。</p> <p>主管機關接獲前項資料後，得就資通安全事件之等級進行複核，並得為等級之變更。</p>	<p>一、考量特定非公務機關於進行資通安全事件之通報時，因受限於時間急迫或其他因素，就資通安全事件等級之判斷或有不適當之情形，爰於第一項明定中央目的事業主管機關於特定非公務機關完成資通安全事件之通報後，應於規定時限內完成資通安全事件等級之審核。</p> <p>二、為使主管機關得掌握資通安全事件之情況，以利適時提供必要協助，爰於第二項明定資通安全事件經中央目的事業主管機關判斷為第三級或第四級事件者，中央目的事業主管機關應於審核完成後一小時內將審核結果、依據及其他必要資訊送交主管機關；如判斷屬第一級或第二級事件者，則應定期彙整審核結果、依據及其他必要資訊送交主管機關，無須立即為之。</p> <p>三、第三項明定主管機關接獲中央目的事業主管機關送交之資通安全事件審核資料後，得就資通安全事件之等級進行複核，並為等級變更。</p>
<p>第十三條 特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜：</p> <p>一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。</p> <p>二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。</p> <p>特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。</p> <p>前項調查、處理及改善報告送交</p>	<p>一、第一項明定特定非公務機關於知悉資通安全事件後，應視該事件之等級，於時限內完成損害控制或復原作業及通知事宜。</p> <p>二、為使特定非公務機關及其中央目的事業主管機關對於資通安全事件儘速妥適處理，於第二項及第三項明定特定非公務機關完成第一項所定資通安全事件之損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並應於一個月內依中央目的事業主管機關指定之方式送交調查、處理及改善報告；另得經中央目的事業主管機關同意後延長上開時限。</p> <p>三、為強化特定非公務機關之資通安全管理，爰於第四項及第五項規定，</p>

<p>之時限，得經中央目的事業主管機關同意後延長之。</p> <p>中央目的事業主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。</p> <p>特定非公務機關就第三級或第四級資通安全事件送交之調查、處理及改善報告，中央目的事業主管機關應審查後交主管機關；主管機關就該報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。</p>	<p>中央目的事業主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整；就第三級或第四級資通安全事件之調查、處理及改善報告，應於審查後送交主管機關，主管機關認有必要，或有違法或不當等情事者，得要求該特定非公務機關提出說明及調整。</p>
<p>第十四條 中央目的事業主管機關就所管特定非公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。</p> <p>主管機關就特定非公務機關執行資通安全事件應變作業，得視情形提供必要支援或協助。</p> <p>特定非公務機關知悉第三級或第四級資通安全事件後，應召開會議研商相關事宜。</p>	<p>一、考量特定非公務機關執行資通安全事件之通報及應變作業時，依其所能使用之資源，或有無法適時完成各項要求之可能；或有數特定公務機關同時發生類似資安事件，需中央目的事業主管機關或主管機關協助資通安全事件應變之可能；爰於第一項規定中央目的事業主管機關，應視情形提供資通安全事件通報及應變作業必要支援或協助，並於第二項規定主管機關得視情形提供資通安全應變作業必要支援或協助，以利各特定非公務機關順利完成相關作業。</p> <p>二、考量第三級或第四級資通安全事件影響層面、可能發生之損害皆較嚴峻，爰於第二項明定特定非公務機關應召開會議研商相關事宜；主管機關就該等事件，亦得視情形提供必要支援或協助。</p>
<p>第十五條 特定非公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：</p> <ol style="list-style-type: none"> 一、判定事件等級之流程及權責。 二、事件之影響範圍、損害程度及機關因應能力之評估。 三、知悉資通安全事件之內部通報流程。 四、通知受資通安全事件影響之其他機關之時機及方式。 	<p>為確保特定非公務機關於知悉資通安全事件後，得依本辦法規定迅速進行事件之通報及適當之處置，爰為本條規定。</p>

<p>五、前四款事項之演練。</p> <p>六、資通安全事件通報窗口及聯繫方式。</p> <p>七、其他資通安全事件通報相關事項。</p>	
<p>第十六條 特定非公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：</p> <p>一、應變小組之組織。</p> <p>二、事件發生前之演練作業。</p> <p>三、事件發生時之損害控制及向中央目的事業主管機關請求技術支援或其他必要協助之機制。</p> <p>四、事件發生後之復原、鑑識、調查及改善機制。</p> <p>五、事件相關紀錄之保留。</p> <p>六、其他資通安全事件應變相關事項。</p>	<p>為確保特定非公務機關於知悉資通安全事件後，得依本辦法規定迅速且確實進行資通安全事件之應變，爰為本條規定。</p>
<p>第四章 附則</p>	<p>章名。</p>
<p>第十七條 主管機關就各機關之第三級或第四級資通安全事件，得召開會議，邀請相關機關研商該事件之損害控制、復原及其他相關事宜。</p>	<p>考量第三級與第四級資通安全事件之影響範圍及資訊洩漏之情形較鉅，爰規定主管機關得針對各機關之第三級與第四級資通安全事件（即重大資通安全事件），邀集相關機關召開會議，就事件之損害控制、復原及其他相關事宜進行研商，以提升各機關對於重大資通安全事件之處理成效，避免類似事件再次發生。</p>
<p>第十八條 公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：</p> <p>一、社交工程演練。</p> <p>二、資通安全事件通報及應變演練。</p> <p>三、網路攻防演練。</p> <p>四、情境演練。</p> <p>五、其他必要之演練。</p>	<p>考量資通安全演練作業為資通安全事件應變之一環，為使公務機關對於資通安全事件之預防與應變更臻完備，爰規定公務機關應配合主管機關規劃、辦理之資通安全演練作業及相關項目。</p>
<p>第十九條 特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：</p> <p>一、網路攻防演練。</p> <p>二、情境演練。</p> <p>三、其他必要之演練。</p> <p>主管機關規劃、辦理之資通安全演練作業，有侵害特定非公務機關之權利或正當利益之虞者，應先經其書</p>	<p>一、考量資通安全演練作業為資通安全事件應變之一環，為使特定非公務機關對於資通安全事件之預防與應變更臻完備，爰規定特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業及相關項目。</p> <p>二、考量部分資通安全演練作業可能影響特定非公務機關之業務運作或造成資通系統損壞，而侵害其權利或</p>

<p>面同意，始得為之。</p> <p>前項書面同意之方式，依電子簽章法之規定，得以電子文件為之。</p>	<p>正當利益，為保護特定非公務機關之權益，爰於第二項明定主管機關規劃、辦理該等演練作業，應先經特定非公務機關之書面同意，始得為之。</p> <p>三、為提升行政效率，於第三項明定主管機關依第二項取得特定非公務機關之書面同意時，依電子簽章法之規定，得以電子文件為之。</p>
<p>第二十條 公務機關於本辦法發布前，已針對其自身、所屬或監督之公務機關或所管之特定非公務機關，自行或與其他機關共同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬或監督之公務機關或所管之特定非公務機關繼續依該機制辦理資通安全事件之通報及應變，不適用本辦法之規定。</p> <p>前項通報及應變機制如有變更，應送主管機關重為核定。</p>	<p>一、考量目前部分公務機關之業務領域已具備完善之資通安全事件通報及應變機制，為有效利用行政資源，爰為第一項規定。</p> <p>二、公務機關為因應業務或實務趨勢等內在或外在條件之改變，對於資通安全事件之通報及應變機制可能有配合調整之需求，其通報及應變機制經變更後，內容是否妥適而得免除適用本辦法規定，仍須由主管機關審視決定，爰為第二項規定。</p>
<p>第二十一條 本辦法之施行日期，由主管機關定之。</p>	<p>明定本辦法之施行日期，由主管機關定之。</p>