# 資通安全情資分享辦法草案總說明

「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。依本法第八條規定，主管機關應建立資通安全情資分享機制；其資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。為增進公務機關及特定非公務機關面對資通安全威脅及風險之應變能力，妥為規範資通安全情資之分析、整合與分享之內容、程序、方法等相關事宜，爰擬具「資通安全情資分享辦法」(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、資通安全情資之定義。(草案第二條）

三、各機關進行資通安全情資分享之對象。(草案第三條）

四、資通安全情資分享之限制。(草案第四條）

五、分享及接收資通安全情資之注意事項及安全維護之規定。(草案第五條及第六條）

六、資通安全情資分享之方式。(草案第七條）

七、未適用本法之個人、法人或團體，得經主管機關或中央目的事業主管機關同意後，進行資通安全情資分享。(草案第八條）

八、本辦法之施行日期。(草案第九條）

# 資通安全情資分享辦法草案

| 條文 | 說明 |
| --- | --- |
| 第一條　本辦法依資通安全管理法（以下簡稱本法）第八條第二項規定訂定之。 | 明定本辦法訂定之依據。 |
| 第二條　本辦法所稱資通安全情資（以下簡稱情資），指包括下列任一款內容之資訊：<br>一、資通系統之惡意偵察或情蒐活動。<br>二、資通系統之安全漏洞。<br>三、使資通系統安全控制措施無效或利用安全漏洞之方法。<br>四、與惡意程式相關之資訊。<br>五、資通安全事件造成之實際損害或可能產生之負面影響。<br>六、用以偵測、預防或因應前五款情形，或降低其損害之相關措施。<br>七、其他與資通安全事件相關之技術性資訊。 | 為使公務機關或特定公務機關（以下簡稱各機關）得以知悉何種資通安全資訊具有進行分享之效益，以利進行資通安全情資分享，爰參考美國 Cybersecurity Information Sharing Act of 2015, SEC102(6)之規定，明定本辦法所稱資通安全情資之定義。其中第一款所定資通系統之惡意偵察 (malicious reconnaissance)或情蒐活動，包括進行資通系統之弱點、安全漏洞是否存在等資訊蒐集之異常活動；第四款所定與惡意程式相關之資訊，例如惡意指令、控制受害者、中繼站位址或連線資訊之方式等。 |
| 第三條　主管機關應就情資分享事宜進行國際合作。<br>主管機關應適時與公務機關進行情資分享。<br>公務機關應適時與主管機關進行情資分享。但情資已依前項規定分享或已經公開者，不在此限。<br>中央目的事業主管機關應適時與其所管之特定非公務機關分享情資。<br>特定非公務機關得與中央目的事業主管機關進行情資分享。 | 一、考量目前資通安全之攻擊可能來自全球各地，為強化資通安全管理體系下之預警功能，於第一項明定主管機關應就資通安全情資分享進行國際合作。<br>二、第二項至第五項明定主管機關與其他公務機關及中央目的事業主管機關與特定非公務機關，進行情資分享之規定，俾利各機關掌握情資，提升其資通安全維護能量，以適時調整資通安全應變機制，預防相關資通安全威脅之發生。<br>三、另各機關於知悉自身之資通安全事件時，應依本法及資通安全事件通報及應變辦法之規定進行通報及應變，已達情資分享之效，爰本辦法就該等情形不再另行規範，併予敘明。 |
| 第四條　情資有下列情形之一者，不得分享：<br>一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害公務機關、個 | 為避免各機關進行情資分享時，可能影響其他個人、法人或團體之權益，或有其他依法令規定應秘密或應限制、禁止公開之情形，爰參考美國 Cybersecurity Information Sharing Act of 2015, |

| | |
|---|---|
| 人、法人或團體之權利或正當利益。但法令另有規定，或為避免人民生命、身體之重大損害而有必要，或經當事人同意者，不在此限。<br>二、 其他依法令規定應秘密或應限制、禁止公開之情形。<br>情資含有前項不得分享之內容者，得僅就其他部分分享之。 | SEC104(d)與政府資訊公開法第十八條第一項第七款及第二項規定，明定不得分享情資之範疇，並明定情資含有不得分享之內容者，得僅就其他部分分享之。 |
| 第五條　公務機關或特定非公務機關（以下簡稱各機關）進行情資分享，應就情資進行分析及整合，並規劃適當之安全維護措施，避免情資內容、個人資料或依法令規定不得分享之資訊外洩，或遭未經授權之存取或竄改。 | 為督促各機關妥適管理及運用情資，及避免發生情資外洩、遭未經授權之存取或竄改，或其他侵害個人、法人或團體權益之情事，爰明定進行情資分享應就情資為分析及整合，並應規劃適當之資通安全維護措施，例如於分享前應遮蔽無關之個人資料或其他依法令應予保密或不得分享之資訊等。 |
| 第六條　各機關應就所接收之情資，採取適當之安全維護措施，避免情資內容、個人資料或依法令規定不得分享之資訊外洩，或遭未經授權之存取或竄改。 | 考量各機關於接收其他機關分享之情資後，應以適當方式確保情資之安全性，爰參考 Cybersecurity Information Sharing Act of 2015, SEC104(d)之規範意旨為本條規定。 |
| 第七條　各機關進行情資分享，應分別依主管機關或中央目的事業主管機關指定之方式為之。<br>各機關因故無法依前項規定方式進行情資分享者，得分別經主管機關或中央目的事業主管機關同意後，以下列方式為之：<br>一、 書面。<br>二、 傳真。<br>三、 電子郵件。<br>四、 資訊系統。<br>五、 其他適當方式。 | 一、為確保情資分享之效率及正確性，進行資通安全情資分享之方式宜臻明確，爰於第一項規定各機關應遵循之資通安全情資分享方式。<br>二、考量實務上可能發生各機關依規定應進行情資分享，惟因故無法依第一項規定方式辦理之情形，為使各機關適時掌握情資，仍應循其他方式進行情資分享，爰參考其他法規所定提供資料之方式，於第二項明定各機關於此情形得採取之情資分享方式。 |
| 第八條　未適用本法之個人、法人或團體，得經主管機關或中央目的事業主管機關同意後，與其進行情資分享。<br>主管機關或中央目的事業主管機關同意前項個人、法人或團體進行情資分享，應以書面與其約定應遵守第四條至前條之規定。 | 一、考量未適用本法之個人、法人或團體亦可能持有資通安全情資，或有資通安全情資分享之需求，爰於第一項明定該等個人、法人或團體得經主管機關或中央目的事業主管機關同意後，與其進行資通安全情資分享。<br>二、為確保第一項與主管機關或中央目的事業主管機關進行情資分享之個人、法人或團體處理情資符合本辦 |

| | |
|---|---|
| | 法相關規定，爰為第二項規定。 |
| 第九條　本辦法施行日期，由主管機關定之。 | 明定本辦法施行日期，由主管機關定之。 |