資通安全情資分享說明

一、依據：資通安全管理法第八條第二項及資通安全情資分享辦法。

二、作業方式：

若機關需依資通安全情資分享辦法第三條第三項進行情資分享，請依說明四各項目撰寫電子郵件或填寫「資通安全情資分享通報單」後以電子郵件併同截圖或其他佐證資料逕送本院國家資通安全會報技術服務中心之服務信箱(service@nccst.nat.gov.tw)。

三、一般填寫：

(一)每項皆須填寫，「入侵指標(IoC)」可填寫「無」。

(二)為避免無法匯入請勿合併欄位。

(三)欄位多值填寫，請以全形逗號「，」區隔各項。

(四)若有惡意程式樣本，請加密後併同情資分享通報單逕送服務信箱，並將密碼填入「附件資訊」1 欄。

四、各項撰寫說明

項目	撰寫說明	撰寫範例
機關名稱	機關名稱，如：行政院。	機關 A
填報機關識別碼(OID)	機關識別碼 OID 可至物件識別碼中心網站(https://oid.nat.gov.tw/OIDWeb/)查詢。	
填報日期	YYYYMMDD，使用西元年(4 位數字)、月(2 位數字，1-9 月首位補 0)、日(2 位數字，1-9 日首位補 0)。	20200101
情資種類	依據「資通安全情資分享辦法」第 2 條定義之資通安全情資，自下列 7 項擇一填寫： 一、資通系統之惡意偵察或情蒐活動。 二、資通系統之安全漏洞。 三、使資通系統安全控制措施無效或利用安全漏洞之方法。 四、與惡意程式相關之資訊。 五、資通安全事件造成之實際損害或可能產生之負面影響。 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。	四、與惡意程式相關之資訊。

項目	撰寫說明	撰寫範例
	七、其他與資通安全事件相關之技術性資訊。	
情資說明	200 字以內之簡短描述，說明本資通安全情資之發現歷程及可能造成之損害。	接獲社交工程郵件，經檢視郵件所附檔案，確認為包含惡意程式，可越權存取使用者資訊。
入侵指標(IoC)	自下列 5 項擇一填寫： 一、惡意程式樣本。 二、惡意程式特徵值。 三、可疑或惡意 IP 位址。 四、疑似 C&C server 使用之網址或 DNS。 五、其他。	一、惡意程式樣本
短期應變措施	依據資通安全情資執行之強化資安防護作為，若無因應作為擇填「無」。	以電子郵件提醒機關人員近期社交工程郵件威脅，將惡意程式之特徵值加入防毒軟體。
附件資訊	提供之附件說明，如：惡意程式樣本之密碼。	惡意程式樣本 1 份，密碼：XXXXXXXX。