高雄市政府交通局

107 年第二季廉政季刊

高雄市政府交通局政風室　　編

107 年 5 月

目　錄

廉政案例宣導

案例一：詐取出差交通費案

郭○○係前臺南市政府文化局文化資源科科長，明知依國內出差旅費報支要點規定：…機關專備交通工具便車者，不得報支交通費。詎其仍意圖為自己不法之所有，利用於 102 年 1 月 28 日至 103 年 1 月 27 日期間均搭乘公務車至臺南市政府永華行政中心開會或佈展之機會，於出差旅費報告表上虛偽填列不實之交通費，使不知情之臺南市文化局人事單位、主計承辦人、主計單位主管、機關首長等僅具形式審查義務之人均陷於錯誤，而據以核准上開期日之出差旅費報告表所示之交通費，並依報請之數額於填報後如數核發，共計詐得新臺幣 5,826 元，足生損害於臺南市政府核發出差費之正確性。

案經臺南地檢署檢察官偵查終結，認郭○○所為係涉犯貪污治罪條例第5條第1項第2款之公務員利用職務機會詐取財物罪、刑法第214條使公務員登載不實等罪嫌並提起公訴。

案例二：過失洩密案

臺北市政府環境保護局北投垃圾焚化廠副組長吳ＯＯ，於 101 年 2 月間，擔任「北投垃圾焚化廠減速機及附件（PT101131）招標案」開標主持人時，明知因職務而得知上開採購案之「底價」，依政府採購法第 34 條第 3 項之規定，於開標後至決標前應予保密，竟於上開採購案因最低價投標廠商之投標價低於核定底價 70%，致須依「政府採購法第 58 條處理總標價低於 80% 案件之執行程序」宣布保留決標之際，竟疏未注意，當場宣布底價，而洩漏底價予當時在場參與投標廠商代表等人知悉。全

案經法務部廉政署調查後，移送臺灣士林地方法院檢察署偵辦。

案經臺灣士林地方法院檢察署檢察官偵查終結，以吳ＯＯ所為，係犯刑法第 132 條第 2 項過失洩漏國防以外之秘密罪。惟查吳ＯＯ並無前科，係因一時疏失所致，而犯後接受偵查時隨即坦認犯行，深表悔悟，態度良好，所犯情節又尚屬輕微，爰依刑法第 57 條所列各款事項，予以職權不起訴，以啟自新。

（一）當門禁系統成為駭客的挖礦機

◎臺北市立中正高中資訊組長　李詩婷

物聯網的時代來臨，新興科技帶來便利的同時，背後也隱藏了重大的資安風險，機關在採購相關設備時也要小心謹慎，減少資安事件發生的機會。

門禁系統潛藏安全漏洞

好萊塢特務電影的駭客，只要手邊有一台電腦就能控制任何資訊系統，從屏蔽大樓監視器的畫面，或是遠端控制門禁鎖，讓人輕易地進出機關重地等都只是小菜一碟。以上場景觀眾已經司空見慣，但若以為這些只會出現在電影裡那就是大錯特錯了，隨著駭客手法日新月異，電影中的許多情節都已成真。

《台灣電腦網路危機處理暨協調中心（TWCERT ／CC）》於去（2017）年 9 月時就發出警告，數個特定考勤門禁系統中已被發現存在資安漏洞，可能被駭客利用而植入木馬或後門等惡意程式，不僅具有機敏資訊（例如內部人員出勤紀錄、員工編號或帳號密碼等）外洩的風險，而且可能被駭客進一步取得系統完整的控制權。

「運算資源」成為駭客覬覦目標

不要以為駭客只會針對資料有興趣，就心存僥倖。許多資安事件案例顯示，駭客想竊取的已不只是有價值的「資料」，而是轉為鎖定裝置的「運算資源」。典型的攻擊手法是植入殭屍（bot）病毒，成為受駭客控制的殭屍電腦，潛伏並隨時等候駭客下一步

命令，一旦殭屍網路大軍成形，就能用來發動分散式阻斷服務攻擊（Distributed Denial-of-Service attack, DDoS），讓雲端服務或網站連線負載量過大而造成服務停擺。

除此之外，新型態的攻擊手法則是植入比特幣挖礦的惡意程式，讓裝置搖身一變成為駭客專屬的虛擬貨幣挖礦機，不僅難以追查，還能立即替駭客帶來金錢上的利益，比過去還要設法販賣機敏資料或向被害企業組織勒索贖金更方便省事。

物聯網裝置成為駭客眼中的肥羊

門禁卡感應、指紋辨識、車牌辨識等門禁系統皆屬於物聯網（Internet of Things, IoT）技術的應用，物聯網是近年來最火紅的技術之一，其應用例如智慧家電、居家安全偵測及監控系統或穿戴式裝置等，並可與監控系統、網路、中央控制等系統整合，以進行數據收集與遠端控制。

然而， 在一窩蜂擁抱物聯網技術的熱潮中，不得不重視的是其背後所隱藏的隱私問題和資安風險。據資安業者卡巴斯基實驗室（Kaspersky Lab）調查，光是去年就出現逾四千種新 IoT 惡意程式，遠高於前年的 3,219 種。

分析 IoT 惡意程式如此蓬勃發展的原因，是因為物聯網裝置具有以下特性，故容易成為駭客攻擊的目標：

一、資通安全易被忽略

人們通常會專注於保護個人電腦和智慧型手機的隱私，但卻容易忽略物聯網裝置的資安風險。在僥倖心理下，即使知道所使用的裝置系統已有安全漏洞，也可能因為成本預算及人力等考量而無法進行產品升級或汰換。

二、與一般電腦存在同樣的安全問題

隨著物聯網裝置功能需求提高，裝置內部所使用的作業系統也向一般使用者電腦貼近，以應付高階的運作需求。以物聯

網裝置可能搭載的Linux嵌入式作業系統為例，其內部的核心（Kernel）與上層應用軟體和函式庫也可能存在與一般電腦相同的安全漏洞。例如2014年9月曾爆發的Shell Shock重大漏洞（CVE-2014-6271），可能造成目標主機的機敏資料洩露或甚至被駭客所控制，影響的範圍主要為使用bash shell的作業系統，包含CentOS、Ubuntu 及MacOS X等，而亦有不少Linux 嵌入式作業系統內建了bash shell，故同樣存在資安風險。

三、安全性漏洞修補頻率低

在電腦或是手機上還有多種防毒軟體可以安裝使用，例如微軟、Apple 或Google等亦常會釋出安全性修補程式，但卻少有針對物聯網裝置開發專門的防護軟體，只能仰賴裝置製造商釋出的韌體（即燒錄於硬體內的軟體）更新。在成本的考量下可能無法於一年內更新一次，且即使製造商釋出了更新，使用者端也不具備自動修補的能力，故常見的狀況是裝置的韌體未更新，最後只能以汰換硬體收場。

四、常使用預設的帳號密碼

物聯網裝置為了方便進行大量生產，往往會使用預設的帳號密碼，這種現象可能出現於同一個型號的產品或甚至同一個產品線的所有裝置，且工廠出貨後部署至使用者端時，裝機人員也不會特定去修改裝置的預設帳號密碼，甚至可能無法修改，故大開駭客方便之門。駭客只要鎖定共同供應契約清單上所列的裝置，一旦成功破解，則採購同一型號的機關組織皆有被入侵的風險。

五、不易發覺異常

功能需求及成本考量下， 物聯網裝置本身往往不需具備大型的使用者螢幕，僅需顯示必要訊息（例如通行碼或異常燈號），故入侵行為也不易被直接發覺。

六、長期不關機

駭客入侵成功後，除了要避免被資安設備察覺，還需要確保惡意連線的暢通，否則好不容易攻下的據點若隨時會失效，那就不符合攻擊的時間成本。而物聯網裝置的需求就是要能隨時提供服務，例如門禁系統必須 24 小時開啟，且隨時連結網路，一旦被成功入侵就可讓駭客長時間使用，可能被當作駭客的跳板機或是殭屍網路成員，長期潛伏並靜待駭客下達攻擊命令。

結論

現今的物聯網資安防護仍相當脆弱，特別是在連網裝置端點上的安全防護更是被人所忽略，全球的物聯網裝置於 2020 年預估會成長到二百至五百億台，更顯出潛藏資安問題的急迫性。資安專家建議使用者在架設物聯網裝置時，應變更裝置的預設帳號密碼，且不要讓裝置暴露在公開網路上讓人隨意存取，並且關閉系統尚不必要的網路服務，以防有心人士惡意探測系統上的漏洞；若設備有疑似遭到入侵的跡象或異常行為，應立即聯繫相關設備廠商重新安裝系統或更新韌體版本。只要遵行這幾項建議，即可大幅降低資安風險，減少被惡意程式狙擊成功的機會。

（資料來源：清流雙月刊2018年第1月號）

（二）網路攝影不設防，直播主角換你當

◎國防部中校參謀　葉清源

國外網站《Insecam》全天候播放來自世界各地的網路直播畫面，前陣子也有臺灣女生的寢室曝光，致其個人隱私全被看光光，這猶如電影《楚門的世界》般的情節正在現實中上演，你是否已經成為最佳男（女）主角了？

「出門在外，想關心一下家中的長輩，於是登入居家安全系統來查看家中的情況」；「炎炎夏日，在外勤奮地跑了一天的業務，為了回家時能有一個舒服的環境，於是遠端啟動家中的冷氣機」；「出門旅遊，看見難得的美景，為了讓親朋好友也能立刻欣賞到相同的景色，所以拍照留念並立刻打卡上傳雲端」；這些在現代看似理所當然的服務，皆拜現今網路發達及科技進步所賜，讓我們平淡無奇的生活處處充滿了便利，但是，在這便利科技的黑暗面中，隱藏了什麼樣的危機呢？

許多人都知道，現在居家防護系統非常多樣化，除了租用保全公司所提供的服務外，熟悉電腦及網路架構的用戶也可以購買相關設備，自行架設一套自己的防護系統，但這些保護居家安全的雲端設備，該由誰來保護它的安全？近年來，網路攝影機遭駭事件層出不窮，國外號稱擁有最多線上攝影機的網站《Insecam》，光是監看臺灣的攝影機就有四百多部（其中二百多部是落於臺北市區），而這個網站甚至依據攝影機的廠牌、架設地區、城市，以及時區等項目進行分類，讓有特殊興趣的人士可以隨時選擇他們想觀看的鏡頭。那麼，當我們使用這些設備時，為避免隱私外露，該採取哪些保護措施？建議各位最基本一定要做到的，就是將登入系統的密碼更換為高強度密碼，另外亦需不定時地更新系統軟體，以及檢查連線紀錄，以避免遭人監看而不自知的情況發生。

其次聊聊雲端家電的便利與風險，可連接雲端的家電，除了最常見的冷氣之外，現在亦有廠商開發電動門、智慧電表、空氣清淨機、電鍋等智慧型連網裝置。這類家電的確可以為我們的生活帶來相當程度的便利，達到節電、省時並提供舒適的生活環境，但若此類系統設計有缺陷，難保駭客不會運用這些設備來進行惡意攻擊。例如，在寒冷的冬天啟動冷氣並將其溫度調降至19度，進行無意義的惡搞；或是竊賊趁家中無人時透過遠端搖控開啟電動門，趁機入侵住宅搜括財物，相信無人願意上述情況發生。

那麼，我們該如何善用這些設備，而又不用擔心它可能隱藏的危害呢？商品生產者當然需要背負最大的防護責任，定時檢測並更新相關系統軟體，而使用者務必保護控制裝置的安全。舉例來說，若透過手機使用雲端APP 來控制家中的冷氣，這部手機就不要安裝太多應用程式；再者，家中的智慧型裝置若是透過Wi-Fi 進行連線，則Wi-Fi 密碼也不應該設定的太過簡單，以上兩點防護作為無需高超的電腦功力，一般人應該都可以做到。

至於即時分享旅遊美景這類的行為，究竟隱藏了什麼樣的危機呢？首先我們該考慮到，有哪些人可以看到我們上傳的照片，如果隨意一個路人都可以存取我們的照片，那我們就不該上傳較隱私或者是背景為機敏地區的照片。此外，亦應留心提供服務的供應商背景，還有使用前應詳讀使用合約，因為某些公司在合約條款中提到，客戶上傳照片後，版權就屬於該公司所有，他們可以任意使用，這類型的合約非常不合理，但多數使用者均未查覺，致損害了自身的權益。另外，若決定使用這類型服務時，仍應注意登入服務的密碼設定是否安全，照片中是否夾帶GPS資訊等等，才能達到較佳的保護效果。

整體而言，智慧型裝置已為現代生活帶來了相當程度的便利，只是身為使用者的我們，除了懂得如何「用」以外，更該瞭解安全防護做法；好好保護自身隱私，就不會成為最佳男（女）主角而不自知！

（資料來源：清流雙月刊2018年第1月號）

機關安全維護專區

（一）「國家關鍵基礎設施防護」的思維與工作面向

◎國立聯合大學土木與防災工程學系助理教授　李中生博士

開車返鄉或出遊前，有一件很重要的事必須提醒：須先保養車輛，檢查並確定各項狀況良好，包括引擎、煞車、水箱、電力等系統；也需要確定車裡各項資訊傳輸儀表顯示以及監控系統正常，能夠正確告訴我們檔位、引擎轉速、溫度、油量、電力等控制資訊。然而，就算車輛狀況正常，預備充足的油料與電力也是確保能順利抵達目的地的必要條件。此外，還有一項必要的項目，那就是駕駛。在無人車技術發展成熟之前，缺了駕駛員還是無法成行的。故若我們分析開車出遊這項任務時，執行它所需要具備的條件可以歸納為：車內各項機械系統（實體）、儀表顯示與監控（資通訊），以及駕駛（人員），而燃料與電力則是必要的資源，缺乏前述任何一項條件都將使得這項任務中斷。

而「國家關鍵基礎設施」(Critical Infrastructure，簡稱：CI)所指的即是支持著國家與社會運作所需要的重要功能設施與系統，包括能源、通訊、交通、機場、港口等，而要使這些設施系統能夠正常地運作，同樣必須要仰賴「實體」、「資通訊」控制系統以及「人員」等三類必要條件，而這三類必要條件有各自不同的風險與安全威脅。若是其中一類遭受災害影響，將進而導致CI功能失效，不僅會嚴重影響民眾生活，中斷都市社會運作機能，造成國家經濟重大損失，降低政府聲譽與信用，甚至有可能影響國家安全。

國內外最近幾年發生過多起CI防護失當案例，顯示出CI一旦失效將造成重大的影響層面與災害損失。因此有必要對這些「CI」進行特別的防護與管理。在我們探討那些設施是CI之前，我們必須先了解CI防護的思維。

CI防護思維

一、安全與韌性

美國推動CI防護工作已逾二十餘年,不論是在觀念上以及在作法上都值得借鏡。在2013 年美國國土安全部提出以「安全（Security）與韌性（Resilience）」為推動目標的國家基礎設施防護計畫（NIPP）。根據美國定義，「安全」是指「利用實體防護與網路防禦來降低因為入侵、攻擊或天然以及人為災害對關鍵基礎設施所造成的風險」。而「韌性」的定義則是指「對於蓄意攻擊、意外，或是天然災害等威脅與突發情況能夠有所準備、調適與因應，以及在中斷後能快速恢復的能力」。綜整上述描述，CI 的防護工作目標可以整理出以下幾點工作面向來進行說明：

（一）於平時分析威脅來源並進行防護

在2005年卡翠納颶風造成重大災害以及後續所發生之重大資安事件後，美國政府即要求以全災害（All-Hazards）的思維來進行分析CI 威脅並進行防護。

全災害可區分為天然災害與人為災害兩大類,而生活在臺灣對於天然災害的類型並不陌生,包括地質災害以及氣象災害兩類。人為災害，根據美國消防工程師學會NFPA1600的分類，則可區分為生物危害、人為意外事件、人為蓄意事件、技術事件以及其他危害等，如表一所示。在這個工作面向中，不僅需要依據CI的功能特性與位置，分析來自外部與內部災害威脅的可能性,更需要瞭解威脅一旦發生所可能造成的災害與衝擊影響,進而針對可能遭受破壞的項目進行防護工作。

（二）對於突發事故的處理能夠事前規劃

在此工作面向上，必須掌握設施間的相依性，以及必要的外部資源（如水、電、通訊等），做為分析連鎖性影響的

根據。另應該針對不同威脅類別與程度評估可能造成設施失效的狀況、影響範圍與層面，以及災害損失等，並依照災害情境規劃處置對策以及處理程序。

（三）在災害事故發生時能夠有效因應

在此工作面向上，須仰賴有效的災害事故應變組織、機制以及處置對策，更應熟稔應變程序，包括指揮調度在內對各項應變技能進行技術與教育訓練。此外，利用演練與演習驗證、檢討並改善各項處置對策與處理程序，於平時即提升對於各類災害事故的應變能力與技術，以確保在事故發生時能夠有效因應，並降低且限縮災害影響的範圍與層面。

（四）在功能中斷之後能夠快速恢復

CI擔負重要功能，因此如何確保在災害事故下能夠持續運作，或是在中斷之後能夠快速的恢復功能，是推動防護工作最重要的目的之一。因此，國際間在推動「CI防護」的工作上，均已導入「持續營運管理」的觀念，藉由設施功能的允許中斷時間以及目標復原時間，做為持續營運管理以及設計功能恢復手段（如備援）的目標與依據。

二、 設施盤點與分級

為了推動CI 防護工作並有效地進行管理，必須藉由設施盤點與分級建立資料庫。在設施盤點方面，依照系統功能屬性，行政院國土安全辦公室已經將我國CI分為八項主領域：能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學與工業園區；而在各主領域下亦再區分次領域，例如在能源領域之下再區分為電力、石油、天然氣、核能、化學材料等次領域。其目的乃希望以領域功能為目標，進行有系統的盤點工作，藉以掌握支持領域功能運作所必要的實體設施與網絡（如供水、供電網絡）、資通訊控制系統，以及關鍵的技

術（人員）等。

在設施分級上，不僅需要評估設施的重要性，更需要考慮設施的相互影響關係。在設施重要性上可藉由「功能重要性」、「失效影響」以及「民心士氣影響」三大項目進行評量。功能重要性則建議由政府機關運作、重要資通訊系統、維生與運輸機能、金融秩序、疫病系統、治安與防救、國家重要象徵與資產、重要產業與園區、防衛動員等面向進行評量；在失效影響方面，可由設施價值、影響人數、經濟損失等進行評量；而在民心士氣影響方面，則由影響國際形象、影響政府聲譽、影響民眾信心等方面評估。藉由上述這三大面向的綜合評估，將使各自領域內設施系統依重要性排序。

三、 組織與合作

CI防護是一項需要持續推動的管理工作，必須藉由管理體系與專責單位，分層負責推動與落實相關工作。我國目前由行政院國土安全辦公室負責督考各領域的CI防護管理工作，推動國家層級威脅情境辨識，擬定國家CI管理與執行策略與目標。各領域主管機關應建立推動小組，進行領域內的設施與系統的盤點與分級、災害威脅辨識，擬定領域層級的CI安全防護計畫，督考所轄的CI防護工作，並建立資訊通報與分享機制。而CI與系統的營運單位同樣需要導入持續運作的管理方法，擬定CI防護管理計畫，執行相關防護工作。唯有如此，才能夠使關鍵基礎設安全防護工作能夠在橫向與縱向上，在跨部門之間整合起來。

結語

若是以人的身體來比喻，CI就如人體內的骨骼、血管與經脈，支持一個人所要執行的動作。正因為如此，必須要有系統地建立設

施資料庫，以系統性的方式進行風險分析後並加以防護。CI安全防護所推動的是一套風險管理程序，從設定目標、設施盤點與分級、風險評估（威脅、暴露量、脆弱度、後果）、規劃防護優先次序，進而實施防護計畫並且評量實施成效。而在推動過程當中，以「持續營運管理」的方法，在實體、資通訊、人員三個項目上進行風險管理與防護。CI支持著國家各項重要功能的運作，因此必須要在各層面上提升其耐災韌性，並且對於變動的風險威脅能夠及時調適與因應。

（資料來源：清流雙月刊2018年第3月號）

（二）從「珍珠港事件」談關鍵基礎設施的重要性

◎南華大學國際事務暨企業學系兼任教師　楊宗鑫

珍珠港事件中，日軍雖重創美國太平洋艦隊，但忽略了油庫、造船廠等關鍵基礎設施，美軍得以迅速重建、加以反擊。

行動前的情報活動

20世紀初，製糖業是夏威夷的主要產業。因當地土著稀少，大量日本人被引進蔗園工作，加以當時美國仍有「排華法案」，使得日裔移工成為夏威夷人口比例最高的外來族群，在二戰爆發前，已超過人口總數的百分之十，成為日本對美蒐情的一大助力。

為了刺蒐美軍動態，日本將曾任海軍飛行員的吉川猛夫，以化名「森村正」派往駐夏威夷領事館擔任書記員。吉川抵達後，發現美軍太平洋艦隊主力均停泊於歐胡島的珍珠港，乃找上一家毗鄰港灣、且由日本人開設的「春潮樓」飯店，作為觀測據點。日本艦隊集結6艘航空母艦，運送大量戰鬥機進行珍珠港偷襲行動。

他經常進入其中一間面海的客房，窺視窗外美軍艦艇的動向，並將停泊艦艇總數、不同類型艦艇的數量及艦名、戰列艦及航空母艦停泊位置等情資，製作成每日要況。此外，吉川還利用當地日裔移工人數眾多的優勢，吸收了多位眼線，用以蒐集美軍的例行性活動、休假輪值等狀況。

因事前準備充分，多位曾參與此次行動的日本官兵在事後回憶時均稱：「襲擊珍珠港，就像是在進行一次演習般，一切都在計畫中。」

行動中的保密措施

除了充足地情報蒐集外，在偷襲過程中，為了不讓美軍預作準備，日方也研擬了最嚴密的保密措施，包括航線選擇、艦艇通訊，都經過精心策劃。

日本到夏威夷的直線距離， 大約是6,300多公里。當時的日本艦隊，共集結了6艘航空母艦（赤城號、加賀號、蒼龍號、飛龍號、翔鶴號、瑞鶴號）及數十艘護衛艦，規模之大，堪稱當時人類史上之最。如此龐大的艦隊，要穿越太平洋而不被發現，並不容易。因此路線的選擇，是擬定偷襲行動的第一要務。

帝國時期的日本海軍，係以位於本州神奈川縣的橫須賀軍港為基地，包括海軍兵工學校、造船廠都設置於此。參與珍珠港事件的艦艇，在行動前亦停泊該處。由橫須賀軍港啟程，應是最便利的方式，然而為了掩人耳目，日軍刻意將艦艇逐一駛往北海道擇捉島，集結完畢後才由此揮軍東進。

由日本到夏威夷的海上交通路徑，有北、中、南三種航線。中間及南邊的兩條航線，無論在氣象或水文上均較佳，有利於艦隊航行及油料補給，然而這兩條航線因往來商船眾多，且附近多有美國占領的島嶼，容易暴露行蹤，因此遭否決。相較下，北方的航線，儘管距離較遠、容易起霧、視距不良、風高浪急，但這些航海上的

不利因素，反倒有利於艦隊的隱匿性，經過再三權衡，日軍認為保密重於一切，乃決定以此作為航行路徑。

選定了航線後，為了預防在行駛中艦艇彼此溝通往來的電磁訊號遭偵蒐，聯合艦隊指揮官山本五十六下令，全程必須隨時保持無線電靜默，電臺只收不發，僅接受東京方面傳送有關珍珠港最新狀況的報文，每艘艦艇相互不得進行電報往來，要傳遞消息只能使用傳統的信號旗。

百密一疏：獨漏「關鍵基礎設施」

抵達歐胡島外230浬海域後，日軍開始進行攻擊部署，6艘航空母艦上共354架俯衝轟炸機、魚雷轟炸機逐一起飛，對美軍艦隊發動攻勢。90分鐘後，停泊在港內的8艘戰列艦中，有5艘被擊沉、3艘遭重創，另有11艘巡洋艦、驅逐艦受創、超過300架飛機被毀損，美軍喪生人數達2,400多人。

值得稱幸的是，原本被視為攻擊重點的3艘航空母艦，恰巧都不在港內。其中企業號、列星頓號正在他處執行任務，薩拉托加號則在美國本土進行維修，這也成為日後美軍反擊的基礎。

負責執行攻擊行動的，是擔任第一航空艦隊指揮官的南雲忠一中將。他前後下令日軍發動了兩波攻擊，在將8艘美軍戰列艦擊沉或重創後，認為任務已達成，要求艦隊折返。擔任副手的山口多聞少將、三川軍一中將等，則以為美軍油庫、港口、潛艇基地、造船廠等設施尚未受損，力諫發動第三波攻勢。然而南雲主張，偷襲戰的原則是「速戰速決」，若繼續攻勢，則美軍將從混亂中反應過來，待整裝完畢、防空炮火架設完成後，日軍損失的戰機將倍增，因此堅持返航。

聯合艦隊指揮官山本五十六在獲悉戰果時，對於未能將美軍關鍵基礎設施摧毀一事，深感遺憾，並如此評價南雲：「他在指揮作戰時，就像小偷入室行竊般，進門時膽大包天，稍一得手，就急於

開溜。」美軍方面，儘管太平洋艦隊嚴重受創，但因油庫、造船廠、港口等設施倖免於難，得以修復受損船艦，因此在短時間內，迅速恢復戰鬥力，繼續與日本進行海上激戰。

結論

近年越來越多評論者以為，儘管日軍在戰術上取得勝利，卻因未能同步摧毀關鍵基礎設施，可謂犯下了極大的戰略失誤。在傳統軍事理論中，戰爭的攻擊對象係以殲敵為首要考量，其餘均是等而下之的選項，這樣的觀點，在冷兵器時期尚能適用，待進入熱兵器時期後，關鍵基礎設施的存續實不容忽視，直接攸關國家的後勤動員能力，已成為構成國家總體實力的重要環節。

（資料來源：清流雙月刊2018年第1月號）

創意或抄襲—以政策行銷為例

◎新北市政府經濟發展局政風室主任　吳仲明

媒體報導臺北市長柯文哲，於106年3月出席竹子湖海芋節開幕儀式，為了推廣政策，配合主題「漫慢」，cosplay 成知名動漫《火影忍者》的主角漩渦鳴人，是否已經算是著作權法的重製？另外，隨著「精靈寶可夢」系列遊戲的風靡，在開學季，有學校以「寶可夢」意象迎新，甚至師長直接cosplay，校方能主張尚屬《著作權法》的合理使用範疇嗎？

外國人著作之保護

依我國《著作權法》第4條規定，對於外國人著作的保護，採取「首次發行原則」及「互惠原則」。前者要求外國人的著作必須於我國管轄區域內首次發行，或於我國管轄區域外首次發行後30日內在我國管轄區域內發行者。但以該外國人之本國，對我國人之著作，在相同之情形下，亦予保護且經查證屬實者為限；後者指依條約、協定或其本國法令、慣例，我國人之著作得在該國享有著作權者。然而，自91年1月1日，我國以「臺澎金馬個別關稅領域」正式加入世界貿易組織（WTO）後，必須遵守「與貿易有關之智慧財產權協定（TRIPS）」，因為TRIPS 同時具備「最惠國待遇」條款，所以依據前開的「互惠原則」，包括日本在內的164個會員體，即使沒有在我國「首次發行」，一樣還是受到我國《著作權法》的保護。而且，由於TRIPS要求會員體必須遵守《伯恩公約》之規定，而《伯恩公約》規定有回溯保護之適用，故我國加入WTO時，承諾回溯保護原來不受保護的外國人著作。

思想與表達

其次，《著作權法》第10條之1規定：「依本法取得之著作權，其保護僅及於該著作之表達，而不及於其所表達之思想、程序、製程、系統、操作方法、概念、原理、發現。」是以著作權之保護標的僅及於表達，而不及於思想。然而，在具體個案中，究竟如何區別，一般以「抽象測試法」為主要判斷方法，即將事件逐一抽離，當超過一定的界限後，其普遍性或抽象性可適用於任何其他作品的模式，就屬於公共財產，非《著作權法》所保護的範圍，而本質上無法加以解構的著作，如美術著作、圖形著作等，則通常用「整體觀念及感覺測試法」加以判斷，以下試以「人鬼戀」故事為例說明之。

愛情故事的類型百百種，其中跨越陰陽的人鬼戀可謂獨樹一幟，不論是源自《聊齋誌異》中的《聶小倩》改編而成的電影《倩女幽魂》，或者是1990年的美國電影《Ghost》（中譯：第六感生死戀），均膾炙人口，風靡一時。其中，「人鬼相戀」此一題材即是抽象的「概念」，而不同的情節鋪陳、角色刻畫，則是著作人的「表達」方式，受到《著作權法》的保護。從而，前開所舉cosplay之例，恐非單純「概念」之範疇，而應探討該重製行為能否主張合理使用。

合理使用

《著作權法》一方面為保護創作者的利益以鼓勵創作，另一方面為避免創作者壟斷，使大眾能共享人類智慧成果，除了賦予創作者著作權之外，也以合理使用及強制授權，限制著作人之權利，俾兼顧私權與公益。

故《著作權法》於第三章第四節第四款明定「著作財產權之限制」，其中第44條至第63條即列舉了各種合理使用態樣，包括基於政府公務、司法、文教、新聞傳播、公益、資訊或商品流通等目的

或個人、學術、視聽障礙者使用或公開場所展示等用途，以及在第65條第2項的概括合理使用規定。另外在《著作權法》第64條要求利用人在合理使用他人著作時，應明示「出處」，並以合理之方式表明「著作人姓名或名稱」。惟並非只要註明出處、作者，即屬於「合理使用」，利用行為是否合於「合理使用」，仍須依《著作權法》第44條至第63條及第65條第2項的規定加以判斷。此外，合理使用的範圍僅限於「著作財產權」，不及於「著作人格權」，此觀諸《著作權法》第66條規定：「第44條至第63條及第65條規定，對著作人之著作人格權不生影響。」自明。

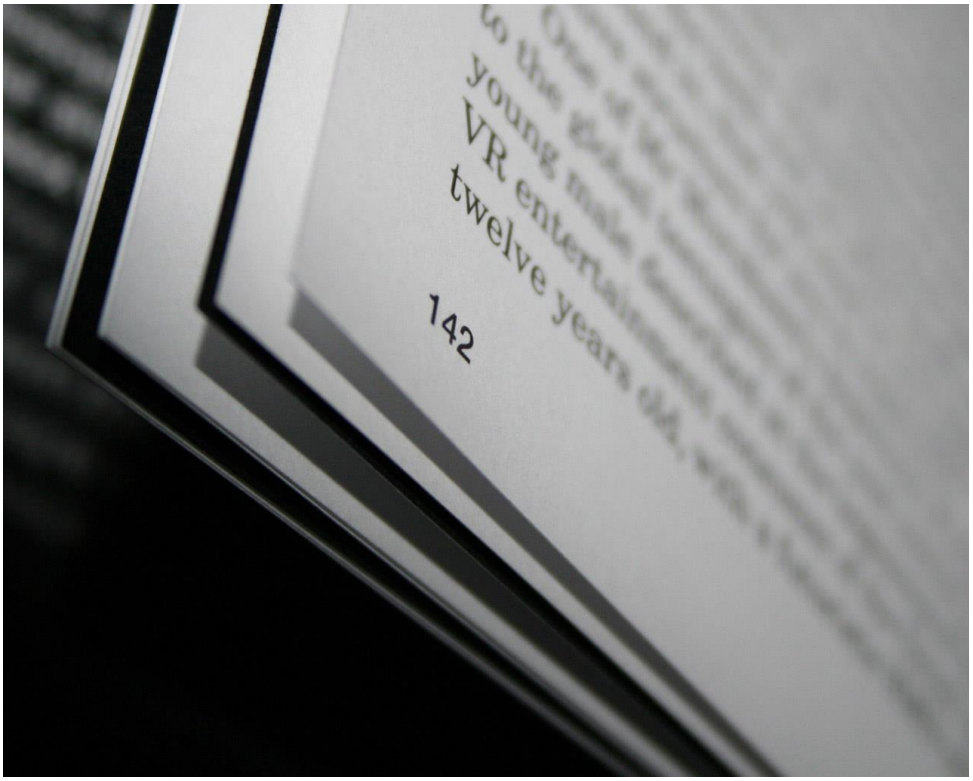
舉例而言，依《著作權法》第55條規定：「非以營利為目的，未對觀眾或聽眾直接或間接收取任何費用，且未對表演人支付報酬者，得於活動中公開口述、公開播送、公開上映或公開演出他人已公開發表之著作。」，欲對於「已公開發表」之著作依本條主張合理使用，其要件除了經濟部智慧財產局90年8月22日（90）智著字第0900007844 號函所示：（一）非以營利為目的、（二）未對觀眾或聽眾直接或間接收取任何費用、(三)未對表演人支付報酬外，依該局90 年11 月15 日（90）智著字第0906000833 號函釋，補充「著作之利用是否合於本法第55條之適用情形，除應考量本局上揭函示所釋明之三認定要件外，仍應以上開本法第65條第2項所列事項作為判斷之標準。」亦即應審酌一切情狀，尤應注意下列事項，以為判斷之基準：（一）利用之目的及性質，包括係為商業目的或非營利教育目的、（二）著作之性質、（三）所利用之質量及其在整個著作所占之比例及（四）利用結果對著作潛在市場與現在價值之影響，故本條之合理使用尚須符合「特定活動」之要件。因此，一般機關或公司舉辦尾牙、春酒活動時，由自己人粉墨登場，提供助興節目，均非屬經常性之特定活動，且未向觀眾或聽眾收取入場費，亦未向表演人支付報酬，即得依《著作權法》第55條主張合理使用著作。惟如基於政策行銷，表演他人已公開發表之著作（例如

配合背景音樂大跳最近流行之甩肩舞），並將過程錄製為影片，上傳至機關網頁或YouTube 等媒體，因得重複點閱，恐不符「特定活動」之要件。

結語

隨著科技進步及當今社會活潑氛圍，各式著作的利用普遍而多元，《著作權法》為平衡著作權人的私益與社會大眾公益，乃設有利用人得主張合理使用之制度，而政府機關在進行政策行銷時，為達到吸睛的效果與迴響，難免注入時下流行元素，若有涉及他人之著作權，應注意符合《著作權法》相關規定，以免因侵權而負民、刑事法律責任，並模糊原本的政策行銷焦點。

（資料來源：清流雙月刊2018年第3月號）



消費者保護宣導

(一)APP 費用併入電信帳單付款，小心使用免爆表！

行動裝置為現代生活中不可或缺的必需品，新興的電信帳單付款服務隨之成為經常使用應用程式（APP）購買的消費者的另一個付款選項，但相關爭議亦與日俱增。行政院消費者保護處（下稱行政院消保處）已協調國家通訊傳播委員會（下稱通傳會），要求電信業者將電信帳單付款功能預設為關閉、配合消費者要求提供明細，及落實帳單分列與分繳等措施，讓消費者權益得以確保。

行政院消保處表示，統計各直轄市、縣（市）政府 106 年受理之電信帳單付款相關申訴案計 38 件，較 105 年全年之 7 件明顯增加，且 107 年 1 月 1 日至 2 月底亦已累計 14 件，足見類似爭議案件有快速成長之趨勢。經分析主要之申訴態樣，並據以協調通傳會督促業者改善如下：。

態樣一、未成年人誤觸消費，致帳單包括電信費用及 Google Play 消費帳款

【案例】

某甲老太太手機僅用於撥接電話及 line 和 facebook 等，未申請手機門號付款功能，卻接獲繳款通知單，出現數筆總計約新臺幣（下同）16,000 元的 Google Play 款項，質疑電信業者擅自開啟其電信帳單付款功能，致家中孩童誤用。

【改善】

行政院消保處已協調通傳會督促業者將電信帳單付款功能預設為關閉；其後如相關功能之設定發生變更時，通知門號申辦人（如：未成年人之監護人或法定代理人等）。另，消費者如無 APP 內購買之需求，可將行動設備帳戶設定為此裝置在 Google Play

上購買任何內容時均需要通過驗證，或開啟 iPhone 與 iPad 的取用限制。

態樣二、消費者無法從電信帳單中得知未成年子女於 Google Play 或 App Store/iTunes 的消費明細

【案例】

某乙申辦門號時告知業者係供未成年子女通話使用，請業者勿開放任何上網或購物功能。卻收到電信業者通知異常消費 15,600 元，經致電客服說明係 Google Play 費用，如欲瞭解相關明細，須撥打 Google 客服電話；惟經撥打該電話，Google 客服以各種理由不提供明細。

【改善】

各電信業者均可依消費者要求提供電信帳單付款之消費明細，消費者可視自身需求撥打業者客服電話索取。

態樣三、業者未告知消費者名下門號之信用額度調整情形

【案例】

某丙手機門號之信用額度上限為 5 千元，卻收到 App Store/iTunes 費用近 2 萬元之帳單。經洽詢電信業者客服表示，因其按時繳費、信用良好，所以增加額度。消費者抱怨業者未通知信用額度已調高，致其過度消費。

【改善】

電信業者均提供消費者透過客服電話查詢名下手機門號之信用額度，另有部分業者之官網與 APP 已提供信用額度查詢，消費者可善加利用。

態樣四、電信業者將電信費用與 APP 等費用之帳單分列，但未落實分繳

【案例】

某丁因為 APP 消費款項爭議，僅同意繳交門號月租費，電信業者以其電信帳單付款尚有欠費為由，暫停其行動通訊。

【改善】

通傳會嚴格要求各業者落實電信費用及 APP 等其他費用帳單的分列與分繳，並已納入電信管理法（草案）規定。

最後，行政院消保處提醒消費者，數位時代下，行動購物與線上購買的支付工具日益多元，不論使用 Apple Pay、Samsung Pay、Line Pay 等綁定信用卡，或併入行動電話帳單付款，手機都是行動錢包，消費者應妥善保護帳戶、密碼等資料，並隨時注意手機簡訊與電子郵件收到的通知訊息，以免費用帳單爆表，造成荷包大失血。

（二）自行車租賃 要把握 5 分鐘檢查時間！

國人以自行車代步通勤，不僅具有環保及健身效果外，加上目前全台各地規劃鋪設的自行車車道，亦已逐步完成，因此以自行車為主之旅遊風潮，也已成為風潮。為此，行政院消費者保護處(簡稱行政院消保處)特別提醒消費者，為避免因租用有障礙之自行車輛，造成身體傷害，倘若您(自行車租賃的承租人或其使用人)，於取車後的 5 分鐘內，請務必自行檢查，如發現有異狀，可依自行車租賃定型化契約應記載事項第 6 點規定，將自行車歸還原租賃場站，自行車出租人不得向您收取租用費用。

然而行政院消保處最近(107 年 1 月 2 日)檢視現行部分有樁式與無樁式自行車租賃業者於網站揭露之租借資訊後發現，雖然各業者於其租借資訊中均有載明取車 5 分鐘內發現車輛有異者可歸還業者。但是，對於「是否需通知客服人員，始

得不予計費」，卻有不同的規定；例如：U-bike 及 O-bike 記載歸還後，該次租借不予計費；然而在 C-bike、T-bike 及 V-bike，卻呈現「應通知客服人員者，該次租借不計費用」、「即刻通知客服人員專線返還收費」之記載內容，如此，似有需先通知後，方可退還已繳租金之疑慮，凡此請消費者應特別注意。

此外，市面上各自行車租賃業者對於前開障礙車輛之處理，除請承租人(使用人)將車輛歸還於原租賃場站外，行政院消保處也觀察發現業者約有下列三種不同的處理方式，敘述如下，由於事涉行車安全，也請各承租人在租賃自行車時，應謹慎注意：

(一)請承租人(使用人)將障礙車輛座椅反轉：

此作法有利於新承租人於租賃現場即時知悉車況，不會將之再作為租借對象；同時，也有助於業者維護人員在巡邏場站時，可以清楚掌握現場車況，進行相關修護事宜。

(二)請承租人(使用人)將障礙車輛訊息通知客服人員：

業者得藉由此種方式，掌握其車輛狀況，但障礙之訊息，有可能無法於現場或租借 APP 網頁中呈現。因此，對新承租人而言，將有可能造成消費者因無法即時獲知車輛的狀況，從而發生所租用之車輛可能為障礙車輛、無車可再租或因騎乘障礙車輛致生身體傷害的情形。

(三)未請承租人(使用人)將障礙車輛資訊傳達給業者：

倘業者無法由自身的經營管理系統上即時獲知障礙車輛之訊息時，除無法期待業者能於現場或於租借 APP 網頁中呈現最新車況外，對新承租人而言，不僅有可能造成前(二)所述之情形外，也會影響承租人(使用人)對於業者掌控車況能力之信心。

最後，行政院消保處亦提醒自行車租賃業者，提供充分正

確的騎乘資訊與安全無虞的車輛，係業者應盡之首要義務，建議各業者對於障礙車輛的資訊可於網頁中即時揭露，亦可加強對於障礙車輛的現場標示、管理與維護，因為讓消費者騎得安全，才是避免消費糾紛的最高指導原則。

（資料來源：消費者保護處）

防詐騙宣導

（一）「衛生紙之亂」有前傳？網瘋傳宣導短片 教你秒懂 ATM 詐騙

買衛生紙也會被騙？1 名美容師在購物網站訂購 1 箱新臺幣 499 元的衛生紙，詎料事後接到冒充該網站客服人員來電，以系統出問題導致重複扣款為由，要求被害人操作自動提款，詐騙新臺幣 8455 元得逞。刑事警察局公布最新宣導短片來提醒民眾，解除 ATM 設定詐騙是最多人中招的手法，並再次強調，自動提款機沒有解除任何設定的功能。

「放著彎腰就能撿錢的生意，誰還會老老實實做買賣呀？」影片裡艷麗的女主角，冷冷地說出了詐騙集團的心態，讓人恨得牙癢癢的。刑事警察局運用電影公司提供的這段影片，破解案件數排名始終居高不下的解除設定詐騙，指出詐騙集團慣用的技倆：先假冒網購客服人員，致電消費者謊稱這筆交易因作業疏失或其他原因，導致會重複扣款或重複訂購，再利用消費者害怕利益遭到損失的心理，假冒金融機構客服人員，以「解除設定」為由，隔空指導消費者操作 ATM 自動提款機，藉此將消費者戶頭裡的存款轉帳一空。

在中部工作的林姓美容師（女，75 年次）去年底在瘋狂賣客購物網站上訂購 1 箱衛生紙，不久就接到自稱瘋狂賣客的客服電話，說網購系統出問題，導致這筆交易變成會重複扣款 12 期，還說會請銀行協助取消重複扣款設定，接著就由假銀行人員來電，以確認交易為由，要求林女操作自動提款機，順利騙走新臺幣 8455 元。林女報案時表示，因為來電顯示和業者的客服專線相同，又非常清楚交易細節，才會深信不疑，沒想到詐騙集團連來電顯示都可以作假。

刑事警察局表示，來電顯示前面有個「+」就是境外來電，後面的號碼可以竄改，民眾接到這種電話務必提高警覺。除此之外，也呼籲網購業者務必加強資安防護措施，避免讓消費者的資料外洩，導致消費者變成詐騙集團眼中的肥羊。有任何疑問歡迎撥打反詐騙諮詢專線 165 查詢。

（二）假鄉民滲透 FB 在地社團「詐」劫難逃

165 反詐騙諮詢專線受理「假網拍詐騙」，單週就有 79 件在 FB 購物遭詐騙被害案件，其中有 24 件民眾於 FB 各在地鄉鎮租屋或聯誼社團，遭詐騙集團張貼販賣二手高價電器或 3C 電子產品訊息，與對方加 LINE 確認電器品牌、匯款後，卻遭封鎖帳號，求償無門。現年 36 歲被騙的職業軍人氣稱：「因為同是故鄉人，人不親土親，才掉以輕心，沒想到居然是詐騙。」

遭利用的社團包含：「嘉義縣市房地產租售資訊」、「正格租屋快訊」、「我是口湖人」、「苗栗人(新品二手)拍賣批發交易網」、「中部(台中)3C 手機、電腦、相機、全新或二手各類買賣交流平台的臉書粉專」、「虎尾人(讚)出來」等，詐騙手法均為被害人在臉書社團看到陌生人刊登出售二手液晶電視訊息，由於電器標榜九成新且二手價格優惠，被害人遂於臉書貼文留言表示購買意願，雙方利用 LINE 相互聯繫、確認販售物品、交貨方式後，被害人即匯款至歹徒帳戶，轉帳完成後，卻無法與歹徒聯繫，已遭封所刪除，才驚覺被詐騙。

警方憂此為新形態「假網拍」詐騙手法，自過去歹徒在購物平臺刊登假網拍訊息，標榜「加 LINE 私下交易享優惠」吸引民眾選擇私下交易購買到更低價商品，後盜用民眾 FB 帳號向其親友販售高階手機，現在最新手法則利用民眾最常交流的

FB 平臺，透過 FB 在地鄉鎮租屋或聯誼社團先取信於被害人，讓民眾有「親不親故鄉人」的親切感，誘騙不特定多數民眾以 LINE 私下交易的方式購買高階 3C 商品，而民眾匯款後卻遭詐騙集團已讀不回或封鎖，讓民眾求償無門，請民眾慎防最新崛起的假網拍詐騙趨勢。

刑事警察局提醒民眾在 FB 社團中看到刊登二手商品出清，應思考賣方的身分及交易條件是否值得信賴，若有購物需求，建議找較具知名度的電子商城、實體店面或採用面交方式購物，避免透過 LINE 私下交易，以免匯款後歹徒人間蒸發而求償無門，也呼籲臉書社團的管理者，應謹慎管理社團內貼文，應避免進社團時日尚短的社員，刊登低價販售高階電器用品或電子商品訊息，讓 FB 故鄉社團淪為詐騙工具。

刑事警察局於 165 官網、165 反詐騙 APP、165 臉書粉絲專頁及 165LINE 反詐騙宣導官方帳號公布並每週更新「千萬別加好友」的詐騙 LINE ID，分析此類 LINE ID 特徵，多以「無意義的英文數字組合而成」，如上週新公布的詐騙 LINE ID ：w266a、vi8y 等，民眾網路購物被賣家要求加 LINE 私下交易，而發現該 LINE ID 符合上述特徵，慎防可能係詐騙帳號，亦呼籲民眾踴躍向 165 反詐騙諮詢專線反映詐騙 LINE ID，避免更多民眾上當受騙。

（資料來源：165 防詐騙網站）

公職人員財產申報義務人

「網路授權介接財產資料」

＋

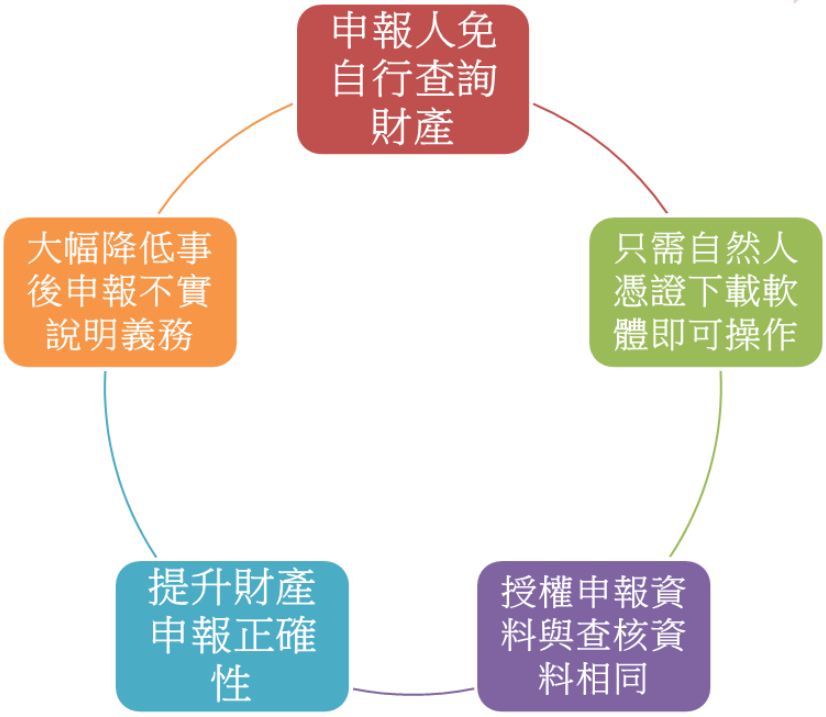
「網路申報財產」

財產申報將與網路報稅一樣便捷，提升財產申報正確性

104 年開始已透過監察院及法務部建置之「財產申報查核平臺」，技術上能利用網路介接作業方式，經由申報人授權後向相關政府機關及金融機構等取得大部分申報人應申報之財產資料，提供予申報人申報財產，減輕申報人負擔。

申報流程

便利性



目前共計介接500餘個政府機關及金融機構等之財產資料，提供申報人辦理定期財產網路申報參考，僅需再登載無法介接之財產資料（例如珠寶、古董、個人債權、債務等），所介接之資料與嗣後受理申報機關查核資料相同，可大幅降低過往由申報人自行查詢財產資料而有漏報、短報或溢報之情事

透過網路授權查調財產，不再需要自己四處奔波查詢填寫財產申報表

授權介接之財產資料與嗣後受理申報機關查核資料相同，不再煩惱漏報財產遭裁罰

廉政專線

一、法務部廉政署

我爆料---廉政檢舉專線電話：

(0800-你爆料-我爆料) 0800-286-586

傳真：02－2381-1234

郵政信箱：10099 國史館郵局第 153 號信箱

電子郵件信箱：gechief-p@mail.moj.gov.tw

二、高雄市政府政風處

廉政專線：0800-025-025

三、高雄市政府交通局政風室：

廉政專線：(07) 2299-814

廉政信箱：高雄郵政第 00670 號信箱

四、法務部調查局高雄市調查處：

檢舉專線：(07)281-8888

喊出廉政核心價值：「廉能是政府的核心價值，貪腐足以摧毀政府的形象，公務員應堅持廉潔，拒絕貪腐。」