糾　正　案　文

壹、被糾正機關：臺北市政府。

貳、案　　由：臺北市政府於100年間，將薪資發放管理系統主機由內網移至DMZ區，卻未依業界標準，設置相關資安防護措施，致使任何人在Yahoo可搜尋薪資清冊上之員工個人資料；並遲至106年1月9日接獲通報始知悉資安漏洞而以防火牆設定阻擋並加入認證機制，讓4萬餘名員工遭受個資外洩風險長達6年，使2,313名員工之薪資報表疑遭外部IP連結或下載。復未依個資法施行細則第22條第2項規定，對疑遭個資外洩員工個別通知相關事實及已採取的因應措施；遲至本院約詢後，始於106年6月6日起，針對2,313名員工再次發送通知函，違失情節明確。另該府「智慧支付平台 pay.taipei」及「單一陳情系統 Hello Taipei」未督促得標廠商採用Https加密技術而致個資外洩爭議，以及「臺北市政府志工管理整合平台」發生世界大學運動會志工個資外洩事件，亦核有疏失。臺北市政府近3年來(104年至106年)，共編列約2億1,258萬元之資安防護預算，卻發生資安事件至少19起，其中17起有系統漏洞且有明確事證可證實已發生資料遭洩漏、系統或資料遭竄改、業務運作遭影響或系統停頓等情事之1，依法須通報行政院；高達12起係肇因於「應用程式漏洞」或「軟硬體漏洞」；並有2起個資外洩、6起遭外部有

心人士實際入侵之嚴重情事，違失情節明確，爰依監察法第24條提案糾正。

參、事實與理由：

「臺北市政府於民國(下同)105年斥資不斐自行開發設計『薪資發放管理系統』(下稱薪資系統)，處理轄下機關、學校、臺北市議會等人員之薪資發放、考績等業務，詎未妥善保護個人資料(下稱個資)，致部分公務員之姓名、薪資、考績等資料曝光於網路」及「臺北市政府『智慧支付平台 pay.taipei』及『單一陳情系統 Hello Taipei Android 版 APP』涉及使用者帳號、密碼等資料外洩，其網站為何未使用加密通訊協定等情事」二案，經本院於106年1月25日親赴臺北市政府資訊局(下稱北市府資訊局）履勘，並洽請台灣微軟股份有限公司(下稱台灣微軟公司)、香港商雅虎資訊股份有限公司台灣分公司協助提供相關資料；嗣於106年5月23日約請行政院資通安全處副處長徐嘉臨、法務部調部辦事主任檢察官聶眾、刑事警察局科技犯罪防制中心主任林豐裕、臺北市政府副秘書長林萬發、台灣微軟公司副總經理廖○○等，率相關業務主管人員到院說明；復於106年7月12日~13日及106年8月10日~11日派員持調查證赴六都之資訊局/資訊中心及台灣微軟公司實地訪查。業調查竣事，臺北市政府核有下列明顯重大之違失，應予糾正促其注意改善。茲臚列事實與理由如下：

一、臺北市政府於100年間，將薪資系統主機由內網移至DMZ區[1]，卻未採取「依業界標準作法標記不予攀爬或

[1] DMZ(DeMilitarized Zone，直譯為非戰區，但資訊用語翻為邊界網路)係屬網路架構布置方案之一種，常被使用的架設方案是在不信任的外部網路和可信任的企業網路外，建立一個面向外部網路的邏輯子網路，在受保護網路與外部網路之間新增的網路，用於對外部網路的伺服器主機，可提供額外保護內部網路的安全層，有時亦稱為週邊網路。

索引」、「設置防火牆及存取控制白名單」及「建立登入驗證機制」等資安防護措施，致使任何人在Yahoo可搜尋該清冊之員工職稱、姓名、帳戶號碼、薪資明細等資料，遲至106年1月9日接獲通報始知悉資料外洩而以防火牆設定阻擋並加入認證機制。該府實際清查結果，有190筆薪資報表檔案連結外露，其中18張報表連結疑遭23個外部IP連結或下載，受影響員工2,313名。台灣微軟公司發現至少有一個網頁連結到一個目前已不存在的第三人網站，該網站涉嫌惡意個資蒐整或其他不法運用等犯罪。該府未依個人資料保護法第18條妥善維護所屬員工個資之安全，讓4萬餘名員工遭受個資外洩風險長達6年，使2,313名員工之薪資報表疑遭外部IP連結或下載，核有嚴重違失。

(一)個人資料保護法(下稱個資法) 第18條規定：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」。

(二)查臺北市政府薪資系統係於91年以ASP架構,報表以Delphi程式語言開發。99年時，有鑑於系統老舊，將不支援新的作業系統架構，再加上當時實際需要(如：民國百年年序議題、健保局調整健保費、納入市議會薪資發放機制等)，故由該局同仁協同廠商以ASP.NET進行改寫，惟並未更動91年之程式邏輯設計方式。100年時，復為因應當時學校及同仁在外辦公需要，乃配合機關之申請，將主機移至DMZ區。

(三)北市府資訊局106年1月25日於本院履勘時之書面說明、該局106年2月22日北市資系字第10630054300號函、106年4月7日北市資系字第10605377600號函等資料顯示：106年1月9日傍晚時分，臺北市政府

警察局內湖分局（下稱內湖分局）警備隊小隊長吳○○因上網搜尋分局長調動之電子報相關訊息，發現網路上可連結取得該分局之薪資資料，遂向該分局秘書室反映。秘書室獲報後，於當日19時許由該室主任蔡○○通報臺北市政府警察局資訊室技佐尹○○，尹技佐於19時35分通報北市府資訊局。北市府資訊局設計師邱○○、股長楊○○接獲通報後，經該局同仁測試在Yahoo搜尋頁面中輸入「內湖分局薪資清冊」等關鍵字，可搜尋出相關之薪資清冊連結，且點選連結，可直接開啟該清冊之檔案，內容包含：職稱、姓名、帳戶號碼、薪資明細等。該局高級分析師廖○○即於19時46分以防火牆為該府薪資系統設定阻擋以避免影響擴大，並於21時50分將薪資清冊程式加入認證機制，爾後必需有授權之帳號才可開啟報表。惟本件涉及公務人員個資外洩事件仍於翌日(106年1月10日)為媒體披露，引發各界關注與質疑[2]。

(四)依北市府資訊局106年1月25日於本院履勘時之書面說明，及臺北市政府106年5月23日應本院詢問時之書面說明內容，本案薪資系統個資外洩事件發生後，北市府資訊局於106年1月9日當天經使用網路搜尋，共找到190筆薪資報表檔案連結在雅虎搜尋網站露出；嗣於106年1月23日調閱系統Log檔及分析存取IP，查知共18筆報表疑遭23個外部IP查看或下載，涉及2,313名員工資料。又因本案外洩的薪資檔案連結僅在雅虎搜尋網站及微軟Bing搜尋引

[2] 「北市府出大包 7萬公務員薪資看光光」，自由時報106年1月10日。
「北市府出包外洩員工資料 柯文哲：不計算重複大概2千名」，Ettoday 106年1月11日。
「北市府外洩員工個資 官員辯：這不算重大機密」，中時電子報106年1月11日。
「15年薪資老系統為何出包？北市薪資報表外洩關鍵大剖析」，iThome online106年1月11日。

擎中露出，且兩者均使用Bing搜尋引擎，該局爰判定係Bing搜尋引擎預設將網址列的資訊自動傳送至Bing，以加快瀏覽速度及搜尋結果之機制，導致使用者於薪資系統上之瀏覽行為等資訊被傳送，引發後續Bing去爬取網址內容的爬蟲行為。

(五)依北市府資訊局106年8月7日北市資系字第10607735200號函，臺北市政府業於106年6月9日檢送IIS Log檔(105年1月1日至106年1月11日)及全府IP清冊，函請臺北市政府警察局刑事警察大隊(下稱北市府刑警大隊)協助確認是否有遭受攻擊或入侵情事後，於106年7月6日正式向北市府刑警大隊提出妨害電腦使用之刑事告訴。

(六)台灣微軟公司以106年4月10日微軟法字第1060410-3號函及106年6月9日微軟法字第1060609-65號函查復本院稱：

1、微軟Bing搜尋引擎可以透過Microsoft Internet Explorer提供的「Suggested Sites」(建議的網站)功能找到某些新的URL[3](網址)，系統會嘗試造訪瀏覽過的URL來建議新網站。惟Bing並不會自動索引(Index)從Internet Explorer瀏覽器發現的所有網址，這只是Bing用來決定某一個公開網址中，是否包含對搜尋服務使用者有用資訊的眾多因素之一。

2、上開功能係於西元(下同)2008年上市。使用者可隨時參考微軟知識庫文章「Search and get browsing suggestions in Explorer 11」所提供的步驟，關閉「Suggested Sites」功能。惟即使使用者已選擇且同意分享上開瀏覽器資訊

[3] URL（Uniform Resource Locator)，直譯為統一資源定位器，俗稱為網頁位址（**網址**)。如同在網路上的門牌，是網際網路上標準的資源的位址（Address)。

予微軟，Bing僅能攀爬(Crawl)及/或索引(Index)：(1)可公開取得之內容，即未放置在防火牆後、登入入口網站或透過其他妥適安全機制加以保護之內容。(2)並未依業界標準做法標記(mark)不予攀爬或索引的內容。若某一網頁可公開取得，該網站即可透過多種方式被搜尋找到。由於目前可取得的資訊十分有限，微軟於本案確實無法說明本案網址的所有來源，微軟僅能說明，我們發現至少有一個網頁連結到一個目前已不存在的第三人網站(http://3x9y.com/detail/ISW%20Login.html)，建請網站管理者(Webmaster)檢閱該網站之安全措施。

3、臺北市政府薪資系統網頁(http:// orgsalary.taipei.gov.tw)，最早被Bing接觸的時間為2012年11月間。惟如前所述，Bing並不會索引每個可從公眾網際網路接觸到的網域，而是透過當時適用的演算法(Algorithms)，來決定哪些網域可能是對搜尋服務使用者最有關連性內容。於本案，直到2016年6月16日，Bing並未索引本案上述網域，且於2017年1月11日依臺北市政府之要求立刻移除相關搜尋結果。又該等資訊並未留存備份於微軟Bing內。

(七)經查，依台灣微軟公司上開說明，及北市府資訊局於106年1月9日接獲通報後之採取相關處置(以防火牆設定阻擋、薪資清冊程式加入認證機制等)即能在第一時間有效阻絕個資外洩情事擴大，以及臺北市政府網路組市政顧問於106年1月17日就本案之討論會議提出「DMZ區提供對外服務之主機系統不應存有Real Data」、「為提升應用服務系統之安全性，建議增設存取控制(Access Control)白名單

及密碼驗證機制，檔案下載連結建議設定期限作為管控」等建議，足證Bing搜尋引擎雖有「Suggested Sites」(建議的網站)的特殊網址攀爬機制，惟只要臺北市政府能確實依業界標準作法標記不予攀爬或索引之內容，即能防免本案薪資系統報表檔案之連結遭攀爬或索引之情事。退一步而言，縱使其連結網址為Bing所攀爬並索引，臺北市政府若有建立防火牆及存取控制白名單，或設置登錄驗證機制等資安防護設定，亦能保護本案連結網址中之個資不致直接外洩。臺北市政府就上開資安防護作為，應作為能作為而不作為，致生本件薪資系統個資外洩情事，顯未善盡個資法第18條之資安防護職責。

(八)綜上，臺北市政府於100年間，為因應當時學校及同仁在外辦公需要，將薪資系統主機由內網移至DMZ區，卻未採取「依業界標準作法標記不予攀爬或索引」、「設置防火牆及存取控制白名單」及「建立登入驗證機制」等資安防護措施，致使任何人在Yahoo可搜尋使用該薪資清冊員工之職稱、姓名、帳戶號碼、薪資明細等資料，讓數萬名員工(依臺北市政府106年5月23日應本院詢問時之書面說明，106年1月使用薪資系統發薪人數共44,520人)遭受個資外洩之風險。該府資訊局遲至106年1月9日接獲該府警察局資訊室通報後，始知悉以防火牆為設定阻擋，並將程式加入認證機制。該府實際清查結果，有190筆薪資報表檔案連結外露，其中18張報表連結疑遭23個外部IP連結或下載，受影響員工2,313名。台灣微軟公司發現至少有一個網頁連結到一個目前已不存在的第三人網站，該網站涉嫌惡意個資蒐整或其他不法運用等犯罪。該府未依個資法第18條妥善維護所屬員工個資之安全，讓4萬餘名員工

疑遭受個資外洩風險長達6年，使2,313名員工之薪資報表遭外部IP連結或下載，核有嚴重違失。

二、臺北市政府於106年1月23日確認2,313名員工個資疑遭外洩後，僅先對全府員工發送通知，後函請報表遭外洩之機關單位轉知所屬，告知及建議同仁加強網路銀行密碼強度，未依個資法施行細則第22條第2項規定，對疑遭個資外洩員工個別通知其個資疑遭外洩之事實及已採取的因應措施，不僅未能保護疑遭個資外洩員工之權益，且易生賠償請求權時效何時起算之爭議。遲至本院約詢後，始於106年6月6日起，針對2,313名員工再次發送通知函，核有違失。

(一)個資法第28條第1項本文規定：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」同法第30條規定：「損害賠償請求權，自請求權人知有損害及賠償義務人時起，因2年間不行使而消滅；自損害發生時起，逾5年者，亦同。」同法第12條規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」第12條之立法理由為：「當事人之個人資料遭受違法侵害，往往無法得知，致不能提起救濟或請求損害賠償，爰規定公務機關或非公務機關所蒐集之個人資料被竊取、洩漏、竄改或遭其他方式之侵害時，應立即查明事實，以適當方式（例如：人數不多者，得以電話、信函方式通知；人數眾多者，得以公告請當事人上網或電話查詢等），迅速通知當事人，讓其知曉。」

(二)依北市府資訊局106年4月7日北市資系字第10605377600號函及臺北市政府106年5月23日應本

院詢問時之書面說明，臺北市政府於106年1月9日知悉其薪資系統有個資外洩情事後，於106年1月11日即透過email對全府員工發送通知，告知本案影響層面及請同仁加強網路銀行密碼強度。其於106年1月23日經調閱系統Log檔及分析存取IP，確認本案2,313名疑似遭外部IP查看或下載個人資料之員工名單後，於106年3月2日以北市資系字第10630060800號函請報表遭外洩之機關/單位轉知所屬：「薪資清冊有外洩疑慮，建議有使用網路銀行之同仁，檢視密碼強度是否足夠，及於登入銀行頁面時留意顯示之登入次數有無異常。」

(三)按個資法施行細則第22條[4]第1項但書雖規定，個資法第12條之通知需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。惟同條第2項規定：「依本法第12條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。」參以個資法第12條立法理由明載：「當事人之個人資料遭受違法侵害，往往無法得知，致不能提起救濟或請求損害賠償」，因此，依個資法第12條所為通知，必須讓個資被外洩之人均知悉其遭個資外洩之事實，以及政府已採取的因應措施，使其得知可依法提起救濟或請求損害賠償。

(四)台北市政府僅先對全府員工發送通知，後函請報表

[4] 個資法施行細則第22條：
(第1項)本法第12條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。
(第2項)依本法第12條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

遭外洩之機關/單位轉知所屬，告知及建議同仁加強網路銀行密碼強度，不僅未對2,313名疑遭個資外洩員工為個別通知，而且通知內容並未包括其個資疑遭外洩之事實，以及政府已採取的因應措施，其所為通知於法不合，不僅未能保護疑遭個資外洩員工之權益，且易生賠償請求權時效何時起算之爭議，核有違失。

(五)臺北市政府在本院約詢後，始於106年6月6日起，針對2,313名員工再次發送通知函，進行方式如下：就薪資系統留有email的2,000餘人，逐一發送郵件再通知一次；其餘人員逐一列印相關通知內容，封裝後交換到發放薪津單位，委請轉交當事人；相關發送紀錄並留存備查（臺北市政府於本院106年5月23日詢問後之補充說明參照）。

(六)綜上，臺北市政府於106年1月23日確認2,313名員工個資疑遭外洩後，僅先對全府員工發送通知，後函請報表遭外洩之機關單位轉知所屬，告知及建議同仁加強網路銀行密碼強度，未依個資法施行細則第22條第2項規定，對疑遭個資外洩員工個別通知其個資疑遭外洩之事實及已採取的因應措施，不僅未能保護疑遭個資外洩員工之權益，且易生賠償請求權時效何時起算之爭議。遲至本院約詢後，始於106年6月6日起，針對2,313名員工再次發送通知函，核有違失。

三、臺北市政府「智慧支付平台 pay.taipei」及「單一陳情系統 Hello Taipei」資安事件，係因採用國家發展委員會GCA SSL憑證進行加密，惟該憑證當時與Google Play尚不相容，該府不察，未能及時督促得標廠商改採其他商業電子憑證，以致短期間連續爆發

2件因未採用Https加密技術而致個資外洩爭議，核有疏失；「臺北市政府志工管理整合平台」發生世界大學運動會志工個資外洩事件，行政作業違失情節明確。

(一)106年6月25日，號稱全國首創的市政繳費整合平台臺北市政府「智慧支付平台 pay.taipei[5]」，方由市長柯文哲親自宣布上線，同月27日即「因為個資都是明碼，會外洩」，遭網友發文建議民眾勿使用此平台。北市府資訊局於當日(27日)證實「第一版智慧支付平台的超文字傳輸協定是用沒加密的Http，而非經過加密的Https，所以帳號與密碼都採明碼傳輸，確有外洩風險」，並於該日緊急下架進行更新[6]。

(二)臺北市政府105年11月1日上線的「單一陳情系統Hello Taipei」，106年7月13日亦遭媒體報導，其安卓（Android）版APP於系統前端資料傳輸時未加密，恐讓陳情民眾個資外洩[7]，北市府資訊局106年7月13日坦承，進行相關修正。

(三)106年8月7日，「臺北市政府志工管理整合平臺」復發生世界大學運動會(下稱世大運)駐選手村志工的手機號碼和身分證字號外洩事件[8]。

(四)詢據臺北市政府查復本院稱：

1、「智慧支付平台 pay.taipei」係於106年6月25日辦理平台試營運，106年8月完成主要功能查

[5] 民眾可使用電腦或手機登入該平台查詢臺北市水費、停車費、聯合醫院看診等費用；並可由該平台介接與市府合作的8家支付業者(包括：Pi行動錢包、台新銀行、玉山銀行、ezPay台灣支付、歐付寶、愛貝錢包、街口支付、橘子支付等)之系統，即時繳納上開帳單費用。

[6]「pay.taipei遭爆恐洩個資　北市坦言有疏失」，蘋果即時106年6月27日。
「台北Pay一上線就出包 未加密個資恐外洩」，卡優新聞網106年6月29日。

[7]「陳情app恐外洩個資 北市：未有資安風險」，中央社106年7月13日。
「北市『單一陳情系統』沒加密 6萬個資有外洩疑慮」，台灣好新聞報106年7月14日。

[8]「世大運再爆個資外洩！駐選手村志工身分證號、手機號碼全都露」，風傳媒106年8月7日。

驗。其系統**原係申請國家發展委員會核發之GCA SSL憑證進行加密**，**惟該憑證當時尚未與Google Play相容**[9]**，導致APP無法使用**，承包商逕改以固定IP及HTTP連線(未加密)方式，以解決APP連線使用問題。惟平台上線後，經該局發現即於106年6月27日中午通知承包商下架處理，並於6月28日改用付費之商用憑證補足安全強度。案後經檢視系統紀錄，**並未發現篡改或竊取資料等異常情事**。且由於該系統本身不處理金流，僅作為支付業者及各機關的服務中介(提供連結到各該支付業者服務介面)，故無盜刷等情事。業於106年8月8日依契約第14條規定，罰廠商3萬元懲罰性違約金。

2、「單一陳情系統 Hello Taipei」係於105年11月1日上線，系統包括Android APP、iOS APP、網頁版等平台。其中，Android APP**原係採用國家發展委員會GCA SSL憑證進行加密，惟該憑證當時與Google Play尚不相容**[10]，故由承包商調整為其他安全控管方式以符合Google Play上架規範。上架以來，並未發生異常存取、資料外洩之情事，惟該安全控管機制之強度相較於憑證加密，確實仍有不足，故北市府資訊局於106年7月3日通知承包商改採其他商業電子憑證，並於7月11日完成Google Play審核上架，提供民眾下載

[9] 依GCA政府憑證管理中心官方網站（http://gca.nat.gov.tw/web2/database01-103.html）**106年07月31日**公告：「本憑證管理中心經由GRCA重新簽發2張自發憑證(GRCA1_to_GRCA1_5.cer及GRCA1_5_to_GRCA2.cer)，**已可解決Firefox與Android 7.0以上遇到GCA SSL憑證不信任的問題**，請參考GCA網站公告之新版憑證安裝手冊。若已經安裝過GCA SSL憑證串鍊的網站伺服器，請參考『SSL憑證重新設定5層串鍊說明』手冊調整憑證串鍊設定。」

[10] 同註18。

更新。該APP上線迄今，該局不斷強化安全控管機制，並**未遭致市民陳情資料外洩及權益受損之情事**。

3、「臺北市政府志工管理整合平台」2017年世大運志工個資外洩事件，係因該府業務單位同仁於106年8月7日志工管理整合平臺上稿（公告）時，將個資未遮蔽完全之檔案放置於「未公開」區，**惟使用者經由訂閱功能所推播之資訊可收到包含公開及未公開之公告**，因而造成26位志工個資外洩事件。該則公告當日（8月7日）即緊急移除，並於翌日（8月8日）針對此功能進行調整，後續經查該個資並無在網路散布之情事，該府亦將依個資法相關規定通知當事人。

(五)綜上情節，本案「智慧支付平台 pay.taipei」及「單一陳情系統 Hello Taipei」資安事件，係因採用國家發展委員會GCA SSL憑證進行加密，惟該憑證當時與Google Play尚不相容，臺北市政府不察，未能及時督促得標廠商改採其他商業電子憑證，以致短期間連續爆發2件因未採用Https加密技術而致個資外洩爭議，雖未因此發生民眾個資外洩情事，惟仍難謂無失察之咎。至於「臺北市政府志工管理整合平台」發生26位世大運駐選手村志工的手機號碼及身分證字號外洩事件，則屬行政作業違失，情節明確。臺北市政府短期間連續發生多起資安事件，顯將傷害民眾對政府資安防護之信賴；允應儘速研謀改善，以避免類此情事再度發生。

四、臺北市政府近3年來(104年至106年)，共編列約2億1,258萬元之資安防護預算，卻發生資安事件至少19起，其中17起有系統漏洞且有明確事證可證實已發生資

料遭洩漏、系統或資料遭竄改、業務運作遭影響或系統停頓等情事之1，依法須通報行政院。高達12起係肇因於「應用程式漏洞」或「軟硬體漏洞」；並有2起個資外洩、6起遭外部有心人士實際入侵之嚴重情事，違失情節明確。臺北市政府允應儘速研謀改善，避免類此情事再度發生，以維護資訊安全。

(一)依北市府資訊局106年11月15日北市資設字第1067000395號查復，臺北市政府近3年來(104年至106年)，全府共編列約2億1,258萬元之資安防護預算，占該府總預算比例的0.043%。除用於各機關自行辦理之資安軟硬體採購、資安專業服務外，多屬全府共通性之資安防護措施(如防毒軟體、資安監控)，相關費用使用情形摘要如下：

1、臺北市立聯合醫院：醫療主機升級暨異地備援計畫案(105-106年)，約**4千萬元**。

2、臺北大眾捷運股份有限公司：防毒軟體採購(106-109年)，約**3千萬元**。

3、資訊局：防毒軟體大量授權(104-106年)、臺北市政府市政資訊網路暨機房設施管理維運整體委託服務案之資安服務(含骨幹網路防護阻擋、弱點掃描、防毒防護、資安事件處理、資安設備採購、辦理資安事件通報演練、網路釣魚演練、資安教育訓練等業務，104-106年)、防火牆及管理分析工具(104年)、遠端鑑識軟體及平台建置(105-108年)、資安健診及滲透測試(105年)、網站滲透測試(106年)，合計約**6,886萬元**。

4、其他機關(共計約23個)：相關資安費用合計約**7,372萬元**。

(二)惟查，該府近3年來(103年12月26日~106年10月3日)，仍發生因系統漏洞而通報之資安事件共17起

(詳如附表)，有上開北市府資訊局106年11月15日北市資設字第1067000395號函檢附之資料在卷可稽。案經檢視附表所列之17筆資料發現：

1、17起事件中，高達12起係肇因於「應用程式漏洞」或「軟硬體漏洞」等違失，其餘5起則為遭受「惡意程式攻擊」事件(序號2、4、13、15、16)；其中，並有2起個資外洩(序號1、5)、6起遭外部有心人士實際入侵(序號3、4、7、14、15、17)之情事，其餘9起為自行發現或經技服通知，尚未查有實際損害。又17起中，臺北市停車管理工程處即占3件(序號9、13、15)，北市府資訊局及臺北市立聯合醫院分別占2件(序號1、5；序號8、17)。

2、發生個資外洩之2起事件，序號5即調查意見一所指摘之「臺北市政府薪資系統個資外洩案」；序號1則為調查意見三「2017年世大運志工個資外洩事件」。

3、17起事件中，並未包括調查意見三之「智慧支付平台pay.taipei」及「單一陳情系統Hello Taipei」傳輸未加密案。依該府之說明，係因依行政院規定，「應通報」之資安事件是指：系統有資料遭**洩漏**、系統或資料遭**竄改**、業務運作遭影響或**系統停頓**等3種情事之1者；旨揭2案尚無明確事證可證實前揭事項，故非屬應向行政院通報之資安事件。

(三)綜上情節，臺北市政府近3年來(104年至106年)，全府共編列約2億1,258萬元之資安防護預算，占該府總預算比例的0.043%，惟期間仍屢屢發生資安事件至少19起，包括因系統漏洞，且有明確事證可證實已發生資料遭洩漏、系統或資料遭竄改、業務運作遭影

響或系統停頓等3種情事之1，而依「國家資通安全通報應變作業綱要」須通報行政院之資安事件17起，以及本案調查意見三所指摘之「智慧支付平台pay.taipei」及「單一陳情系統 Hello Taipei」等2起資料傳輸未採用Https加密技術案。其中，高達12起係肇因於「應用程式漏洞」或「軟硬體漏洞」；並有2起個資外洩、6起遭外部有心人士實際入侵之嚴重情事，違失情節明確。臺北市相關經費運用效能，以及現行資安標準作業程序有無存在系統性問題等，均有澈底檢視之必要。臺北市政府允應儘速研謀改善，避免類此情事再度發生，以維護資訊安全，重建民眾對政府資安防護之信賴。

綜上所述，臺北市政府於100年間，將薪資發放管理系統主機由內網移至DMZ區，卻未依業界標準，設置相關資安防護措施，致使任何人在Yahoo可搜尋薪資清冊上之員工個人資料；並遲至106年1月9日接獲通報始知悉資安漏洞而以防火牆設定阻擋並加入認證機制，讓4萬餘名員工遭受個資外洩風險長達6年，使2,313名員工之薪資報表疑遭外部IP連結或下載。復未依個資法施行細則第22條第2項規定，對疑遭個資外洩員工個別通知相關事實及已採取的因應措施；遲至本院約詢後，始於106年6月6日起，針對2,313名員工再次發送通知函，違失情節明確。另該府「智慧支付平台 pay.taipei」及「單一陳情系統Hello Taipei」未督促得標廠商採用Https加密技術而致個資外洩爭議，以及「臺北市政府志工管理整合平台」世界大學運動會志工個資外洩事件，亦核有疏失。臺北市政府近3年來(104年至106年)，共編列約2億1,258萬元之資安防護預算，卻發生資安事件至少

19起，其中17起有系統漏洞且有明確事證可證實已發生資料遭洩漏、系統或資料遭竄改、業務運作遭影響或系統停頓等情事之1，依法須通報行政院。其中，高達12起係肇因於「應用程式漏洞」或「軟硬體漏洞」；並有2起個資外洩、6起遭外部有心人士實際入侵之嚴重情事，違失情節明確。爰依監察法第24條提案糾正，移送該府確實檢討改善見復。

提案委員：高鳳仙、江綺雯