調　查　報　告（公布版）

壹、案　　由：據悉，新北市政府消防局所屬蔡姓小隊長等人，疑將緊急救護派遣或死亡案件等國防以外秘密洩漏予殯葬業者並收取賄賂，前經檢察官以違反貪污治罪條例等罪起訴在案。另部分不肖殯葬業者委託駭客侵入高雄市政府消防局所建置、維運之內政部消防署版「行動派遣APP」及「119報案APP」系統，或購買已燒錄警政及消防機關專用頻道之無線電，藉以竊取民眾個資及機關派遣即時資訊，或盜接截聽民眾報案等通信內容，嚴重侵害國家執行職務之廉潔性及秘密性。究警政、消防及殯葬業等主管機關，是否切實落實督導及查核工作？相關法規與執行面有無不足？均有深入瞭解之必要案。

貳、調查意見：

新北市政府消防局（下稱新北市消防局）所屬蔡姓小隊長等人，疑將緊急救護派遣或死亡案件等國防以外秘密洩漏予殯葬業者並收取賄賂，前經檢察官以違反貪污治罪條例等罪起訴在案。另部分不肖殯葬業者委託駭客侵入高雄市政府消防局(下稱高雄市消防局)所建置、維運之內政部消防署（下稱消防署）版「行動派遣APP」及「119報案APP」系統，或購買已燒錄警政及消防機關專用頻道之無線電，藉以竊取民眾個資及機關派遣即時資訊，或盜接截聽民眾報案等通信內容，嚴重侵害國家執行職務之廉潔性及秘密性。究警政、消防及殯葬業等主管機關，是否切實落實督導及查核工作？相關法規與執行面有無不足？均有深入瞭解之必要案，已調查完畢，茲臚列調查意見如下：

一、新北市消防局蔡姓小隊長及10名隊員於民國(下同)110年9月7日至113年7月30日間，將值班時經由智慧雲端動態救護系統[1]（下或稱救護系統、EPCR系統）獲知民眾緊急救護、死亡、應派遣救護地點，或該系統之帳號、密碼等應秘密事項，洩漏予3家殯葬業者知悉，蔡姓小隊長及其中9名隊員向殯葬業者收受賄賂合計新臺幣（下同）154.1萬元，經臺灣新北地方檢察署（下稱新北地檢署）檢察官提起公訴，目前由臺灣新北地方法院（下稱新北地院）審理中；涉案人員業分別經核定記大過1次、記過2次或1次等。另新北市政府警察局（下稱新北市警察局）3名警員於108年4月至112年9月間，將所受理110報案之民眾死亡方式、地點等應保密資訊，洩漏予1家殯葬業者，其中1名警員向殯葬業者收受賄賂234萬元，經新北地院判決處有期徒刑2年，褫奪公權3年，緩刑5年確定，業經核定免職，另1名警員經申誡2次。該十餘名人員均為基層警消，服務機關或上級機關已為相當之行政懲處，新北市消防局及警察局允應引以為戒，加強人員之管理，以端正風紀。

(一)按公務員服務法第5條第1項規定：「公務員有絕對保守政府機關（構）機密之義務，對於機密事件，無論是否主管事務，均不得洩漏；離職後，亦同。」新北市消防局及新北市警察局人員分別於110年至113年間、108年至112年間，洩漏國防以外應秘密之消息，且部分人員收受殯葬業者賄賂，茲分述如下：

1、新北市消防局部分

[1] 即電子化救護紀錄表系統（Electronic Patient Care Record, EPCR），系統內存有涉及個人之機敏資料，詳後述。

（1）消防人員服務守則第9點規定：「消防人員應遵守保密規定，因執行職務知悉或持有之公務機密或個人隱私資料，不得洩漏，離職後亦同。」

（2）新北市消防局救災救護指揮中心蔡姓小隊長及第二救災救護大隊(下稱第二大隊)10名隊員，洩漏職務上資訊予萬叡禮儀有限公司（下稱萬叡公司）、仁祥生命終章有限公司（下稱仁祥公司）及鉅陽國際人文有限公司（下稱鉅陽公司），且蔡姓小隊長及其中9名隊員收受賄賂。法務部廉政署（下稱廉政署）於114年11月18日將上開11名消防人員及5名殯葬業者移送新北地檢署偵辦，該署檢察官於同年12月3日將蔡姓小隊長、其中9名隊員及4名殯葬業者提起公訴（113年度偵字第4889號等起訴書，另1名隊員及1名殯葬業者獲檢察官緩起訴處分），該案目前由新北地院審理中。起訴書所載犯罪事實略以：

〈1〉萬叡公司部分

《1》林○紘為萬叡公司之負責人，負責處理死亡案件之亡者殯葬業務及公司營運管理事務。因殯葬業者就處理亡者殯葬案件，有以優先到達死亡現場與亡者家屬接洽者，獲取承接後續該亡者殯葬處理業務之習，是殯葬業者若能第一時間較其他同業取得死亡案件發生之地點，將能獲取優先承接殯葬案件之利益。

《2》林○紘於110年8月間，透過友人結識新北市消防局第二大隊泰山分隊之陳○暉。林○紘向陳○暉表示，希望陳○暉可以洩漏

其在值班時知悉之相關亡者資訊，以利其承接亡者殯葬案件。陳○暉於110年9月7日至111年4月4日間，將值班時經由救護系統獲知民眾緊急救護、死亡、應派遣救護地點等應秘密事項，以LINE通訊軟體傳送至林○紘所使用之LINE通訊軟體內，藉此洩漏應秘密事項予林○紘知悉。

《3》陳○暉於111年4月22日將任職在新北市消防局新莊分隊張○哲之個人聯繫資料傳遞予林○紘，並向林○紘表示因為新莊案件比較多，之後可以與張○哲聯繫取得亡者資訊，經張○哲同意後，由林○紘與張○哲聯繫，雙方約定由張○哲通報透過救護系統得知無意識、無呼吸心跳等緊急救護或死亡案件訊息至林○紘所使用之LINE通訊軟體或萬叡公司所使用TELEGRAM之群組內，若萬叡公司成功獲接案件，則每件以1萬5,000元、1萬元、5,000元論件計酬。張○哲於111年4月22日至111年8月間、112年4月26日至113年1月間，將值班時經由救護系統獲知民眾緊急救護、死亡、應派遣救護地點等應秘密事項，以LINE通訊軟體傳送至林○紘所使用之LINE通訊軟體或萬叡公司所使用TELEGRAM之群組內，藉此洩漏予林○紘知悉。

《4》張○哲於112年6月2日前詢問任職在新北市消防局第二大隊之陳○文有無意願透過洩漏亡者資訊予林○紘之方式賺取外快，經陳○文應允後，張○哲即將陳○文之LINE聯絡資訊傳遞予林○紘。嗣林○紘

與陳○文聯繫，雙方約定由陳○文通報透過救護系統得知無意識、無呼吸心跳等緊急救護或死亡案件訊息告知張○哲，再由張○哲轉傳至林○紘所使用之LINE通訊軟體、由陳○文直接將亡者資訊傳遞至萬叡公司所使用TELEGRAM之群組內或由陳○文提供帳號、密碼供林○紘登入救護系統查看消防救護訊息之方式洩漏亡者訊息，若萬叡公司成功獲接案件，則每件以1萬元、5,000元論件計酬。陳○文於112年6月至113年1月25日間，將值班時經由救護系統獲知民眾緊急救護、死亡等應派遣救護地點及救護系統之帳號、密碼等應秘密事項，透過張○哲以LINE通訊軟體傳送至林○紘所使用之LINE通訊軟體，直接傳遞至萬叡公司所使用TELEGRAM之群組內或由林○紘直接使用其帳號、密碼登入救護系統查看消防救護資訊，而藉上揭方式洩漏予林○紘知悉。林○紘每月結算張○哲、陳○文通報成案之件數後，與張○哲相約交付張○哲、陳○文之賄款予張○哲，由張○哲收受及轉交或轉匯賄款予陳○文，張○哲收受林○紘所交付賄款約6萬2,000元；陳○文收受林○紘所交付賄款共10萬7,000元。

〈2〉仁祥公司部分

《1》林○億為仁祥公司之員工，亦為仁祥公司負責人劉○潔之配偶，其等共同負責處理死亡案件之亡者殯葬業務及公司營運管理事務。

《2》林○億、劉○潔透過在新北市消防局擔任義消之仁祥公司前員工史○鴻，結識陳○暉。劉○潔於111年8月間，與陳○暉約定由林○億、劉○潔以陳○暉通報透過救護系統得知無意識、無呼吸心跳等緊急救護或死亡案件訊息至仁祥公司所設立之LINE群組內，若仁祥公司成功獲接案件，則每件以7,000元、3,000元（清寒家庭）論件計酬。陳○暉於111年8月至113年1月間，將值班時經由救護系統獲知民眾緊急救護、死亡、應派遣救護地點等應秘密事項，以LINE通訊軟體傳送至仁祥公司創設之群組內，藉此洩漏予林○億、劉○潔知悉。

《3》林○億、劉○潔於111年8月後，向陳○暉表示希望可以邀其他新北市消防局同事加入通報緊急救護、死亡案件訊息予仁祥公司之行列，陳○暉即邀第二大隊泰山分隊郭○宥、陳○呈、五工分隊李○菲加入，並介紹劉○潔讓其等認識，另向其等表示可於值班時將獲悉之緊急救護、死亡等應派遣救護地點之地址傳送至仁祥公司之群組或傳送予陳○暉，再由陳○暉轉傳予仁祥公司，若仁祥公司成功接案則可賺取仁祥公司所支付5,000元、3,000元，陳○暉則可由其等通報地址供仁祥公司成功接案後，於每案中抽取2,000元，郭○宥另可由陳○呈通報地址供仁祥公司成功接案後，於每案中抽取2,000元。郭○宥、陳○呈、李○菲於111年12月至113年1月間，將值班時經由救護系統獲知民眾緊急

救護、死亡、應派遣救護地點等應秘密事項洩漏予林○億、劉○潔知悉。林○億、劉○潔成功接案後，由劉○潔每月結算陳○暉、郭○宥、陳○呈、李○菲通報成案之件數，與陳○暉相約交付陳○暉、郭○宥、李○菲、陳○呈之賄款予陳○暉，再由陳○暉轉交賄款。陳○暉於111年8月至113年1月期間，收受賄款共26萬2,000元；郭○宥、李○菲、陳○呈分別收受賄款12萬元、1萬元、0.8萬元。

《4》林○億、劉○潔於111年8月間，另透過陳○暉聯繫任職第二大隊新莊分隊之張○哲。張○哲於111年8月18日主動聯繫劉○潔，雙方約定由林○億、劉○潔以張○哲通報透過救護系統得知無意識、無呼吸心跳等緊急救護或死亡案件訊息至劉○潔所使用之LINE通訊軟體或仁祥公司所設立之LINE群組內，若仁祥公司成功獲接案件，則每件以7,000元、3,000元（清寒家庭）論件計酬。張○哲另邀第二大隊陳○文、頭前分隊黃○澤、蘇○鼎、更寮分隊周○霖加入。張○哲、陳○文、黃○澤、蘇○鼎、周○霖於111年8月至113年1月間，將值班時經由救護系統獲知民眾緊急救護、死亡、應派遣救護地點等應秘密事項，以LINE通訊軟體洩漏予林○億、劉○潔知悉。而林○億、劉○潔成功接案後，由劉○潔每月結算張○哲等5人通報成案之件數，與張○哲相約交付張○哲等5人之賄款予張○哲，再由張○哲收受及轉交或轉匯賄

款予陳○文等4人。張○哲、陳○文、黃○澤、蘇○鼎、周○霖各收受林○億、劉○潔交付之賄款15.6萬元、4萬元、3.75萬元、2.35萬元、2萬元。

〈3〉鉅陽公司部分

《1》沈○哲為鉅陽公司負責人，負責處理死亡案件之亡者殯葬業務及公司營運管理事務。

《2》沈○哲於111年7、8月起透過里長父親介紹認識於110年年初轉調至新北市消防局救災救護指揮中心之蔡○華，經聯繫蔡○華洽談後，雙方約定以蔡○華通報透過救護系統、救護平板得知無意識、無呼吸心跳等緊急救護或死亡案件訊息至沈○哲所使用TELEGRAM通訊軟體內，或以GOOGLE表單填寫地點傳送至沈○哲所使用GMAIL帳號及提供帳號、密碼供沈○哲登入救護系統查詢亡者死亡地點之方式，洩漏死亡案件訊息予沈○哲，若鉅陽公司成功獲接案件，則每件以5,000元至10,000元論件計酬。蔡○華於111年7、8月至113年7月30日間，將值班時經由救護系統獲知民眾緊急救護、死亡、應派遣救護地點等應秘密事項，以前揭方式，將值班時所知悉之死者所在地點或住址等應秘密之事項洩漏予沈○哲知悉。沈○哲每月結算蔡○華通報成案之件數，並於每月交付現金賄款予蔡○華收受，於111年7、8月至113年7月30日共交付約69萬5,000元作為蔡○華洩漏其職務上知悉應秘密事項之對價。

（3）蔡○華小隊長之官等官階為警正4階（相當薦任第6職等），經新北市政府核定記大過1次；該10名隊員之官等官階為警佐3階至警正4階（相當委任第3職等至薦任第6職等）不等，經新北市消防局或新北市政府分別核定記過1或2次、記大過1次等。

2、新北市警察局部分

（1）警察機關勤務指揮中心作業規定第9點第3款規定：「各級勤指中心資料管理如下：……（三）執勤、業務及處理110案件人員對110報案資料，負有保密之義務，非經機關首長或其指定授權人員許可，不得提供……。」

（2）新北市警察局警員許○寶於108年4月至111年8月間，洩漏110報案資料予萬昌禮儀有限公司（下稱萬昌公司）並收受賄賂。新北地檢署偵辦期間，另發現邱○印警員及陳○敏警員洩密予萬昌公司。許○寶經新北地院114年度訴字第832號刑事判決，處有期徒刑2年，褫奪公權3年，緩刑5年確定。新北地檢署檢察官考量陳○敏、邱○印乃基於人情、同事情誼而失慮致罹刑章，所生危害非鉅，犯罪情節尚非嚴重等一切情狀，予以緩起訴處分（113年度偵字第4887號等）。該判決及緩起訴處分書之（犯罪）事實略以：

〈1〉許○寶警員部分

《1》許○寶自86年12月1日起至112年12月2日止，在新北市警察局板橋分局擔任警員，並借調新北市警察局勤務指揮中心，負責受理民眾110報案業務；陳○東為萬昌公司負責人，綜理該公司處理死亡案件之亡

者殯葬業務及公司營運管理事務。

《2》陳○東透過友人結識許○寶，陳○東於108年4月間與許○寶見面約定，由陳○東每個月給付6萬元予許○寶，作為許○寶洩漏於執行勤務中得知死亡案件亡者訊息予陳○東之對價。而許○寶明知死者死亡過程、死因及死者家屬之住家地址等資料，均為勤務指揮中心警察職務上之秘密，應保密不得洩漏，然竟於108年4月至111年8月間，違背其職務，接續將所受理獲知110報案民眾死亡之電話內容等應保密之事項，以通訊軟體Messenger、LINE，傳送透過110報案系統所獲知死亡案件之亡者死亡方式、地點等應保密資訊，洩漏予陳○東知悉。陳○東並於每月中旬，交付6萬元之現金賄款予許○寶，作為許○寶洩漏因職務上知悉之110報案民眾死亡訊息內容之對價。許○寶於108年4月至111年8月以上揭方式收受陳○東所交付賄款共計234萬元。

〈2〉陳○敏、邱○印警員部分

《1》陳○敏於83年7月7日迄今，擔任新北市警察局樹林分局警員，並自110年10月起至112年9月間，負責於新北市警察局樹林分局勤務指揮中心受理民眾110報案業務。陳○敏之母親於106年間過世時，透過友人介紹陳○東協助處理其母親之殯葬事宜，陳○東進而得知陳○敏在該分局勤務指揮中心任職。陳○東請託陳○敏若於執行勤務時得知有民眾死亡案件時，可以協

助告知地點。陳○敏於110年10月至112年9月間，接續將其職務上所受理110報案民眾死亡之電話內容等應秘密事項，以LINE通訊軟體，傳送應秘密資訊，洩漏予陳○東知悉。

《2》邱○印自91年8月1日起迄今，擔任新北市警察局蘆洲分局警員，並自105年起至112年9月間，負責於該局勤務指揮中心受理民眾110報案業務，其在該局勤務指揮中心任職時，與許○寶為同組之同事，許○寶有意招攬邱○印共同為洩密之不法行為，後於108年4月間交付行動電話1支予邱○印，並告知邱○印可於值班時因職務上知悉之死亡案件地點，透過行動電話內已設定好的LINE傳遞予他人，邱○印於108年4月間，使用許○寶所交付之行動電話，以LINE通訊軟體，傳送職務上知悉之死亡案件地址應秘密資訊，洩漏予陳○東知悉。

（3）該3名警員之官等官階均為警正4階（相當薦任第6職等），許○寶經新北市警察局核定自115年1月20日起免職；邱○印之違失行為，因已逾懲處權之行使期間，該局建請免究，經內政部警政署核復「准予照辦」；陳○敏經新北市警察局樹林分局核定申誡2次。

(二)據上所述，新北市消防局救災救護指揮中心蔡姓小隊長及第二大隊10名隊員於110年9月7日至113年7月30日間，洩密予3家殯葬業者，蔡姓小隊長及7名隊員向1家殯葬業者收賄、另2名隊員向2家殯葬業者收賄，各人收賄金額為0.8萬元至69.5萬元不等，收賄金額合計154.1萬元，收賄之蔡姓小隊長及9名

隊員經檢察官提起公訴，該案目前由新北地院審理中，新北市消防局或新北市政府分別核定記大過1次、記過2次或1次等。新北市警察局3名警員於108年4月至112年9月間，洩密予1家殯葬業者，其中許○寶洩密並收賄234萬元，經新北地院114年度訴字第832號刑事判決，處有期徒刑2年，褫奪公權3年，緩刑5年確定，新北市警察局核定免職；邱○印及陳○敏洩密但未收賄，經檢察官為緩起訴處分，邱○印之行政責任因已逾懲處權之行使期間而免究，陳○敏經新北市警察局樹林分局核定申誡2次。

(三)經核，新北市警消人員所涉上開案件之刑事責任，業分別經檢察官起訴、緩起訴或法院判決確定。該十餘名人員均為基層警消，所為違反前揭公務員服務法、消防人員服務守則或警察機關勤務指揮中心作業規定等，服務機關或上級機關已為相當之行政懲處，新北市消防局及警察局允應引以為戒，加強人員之管理，以端正風紀。

二、「資通安全責任等級分級辦法」(下稱資安分級辦法)對於機關之資通安全責任等級(下稱資安責任等級)、資通系統防護需求分級及其防護基準均定有明文及構成要件，俾使風險評估與控制符合衡平性原則。經查全國除臺北市政府消防局及新北市消防局為資安責任等級B級機關以外，其餘地方消防主管機關均為C級機關，且119勤務指揮派遣系統(下稱119派遣系統)之各部署機關亦有部分防護需求等級未臻妥適情形；另新北市消防局智慧雲端動態救護系統(EPCR系統)之存取控制措施並未落實其防護基準等，有未盡周妥情形，消防署允宜秉持資安聯防精神，適時督飭相關機關通盤檢討，以符資安相關法遵及合規性。

(一)資通安全管理法施行細則（下稱資安法施行細則）及資安分級辦法係依資通安全管理法授權訂定，本案各機關資通安全風險評估控制相關措施應符合110年8月23日（行為時）修正版本，茲將涉及本案之規定重點摘要如下：

1、資安法施行細則

（1）第7條第1項：前條第1項第1款所定核心業務，其範圍如下：

〈1〉第1款：公務機關依其組織法規，足認該業務為機關核心權責所在。

〈2〉第4款：各機關依資通安全責任等級分級辦法第4條第1款至第5款或第5條第1款至第5款涉及之業務。

（2）第7條第2項：前條第1項第6款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表9資通系統防護需求分級原則之規定，判定其防護需求等級為高者。

2、資安分級辦法

（1）第2條：公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為A級、B級、C級、D級及E級。

（2）第3條第3項：直轄市、縣（市）政府應每二年提交自身、所屬或監督之公務機關，與所轄鄉（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之資通安全責任等級，報主管機關核定。

（3）第5條：各機關有下列情形之一者，其資通安全責任等級為B級：

〈1〉第2款：業務涉及區域性、地區性民眾服務

或跨公務機關共用性資通系統之維運。

〈2〉第5款：屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。

（4）第6條第1項：各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為C級。

（5）第9條：各機關依第4條至前條規定，符合2個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。

（6）第10條：各機關之資通安全責任等級依前6條規定認定之。但第3條第1項至第5項之公務機關提交或核定資通安全責任等級時，得考量下列事項對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級：

〈1〉第1款：業務涉及外交、國防、國土安全、全國性、區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院業務者，其中斷或受妨礙。

〈2〉第2款：業務涉及個人資料、公務機密或其他依法規或契約應秘密之資訊者，其資料、公務機密或其他資訊之數量與性質，及遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害。

〈3〉第3款：各機關依層級之不同，其功能受影響、失效或中斷。

〈4〉第4款：其他與資通系統之提供、維運、規模或性質相關之具體事項。

（7）第11條第2項前段：各機關自行或委外開發之資通系統應依附表9（如附表一）所定資通系統防護需求分級原則完成資通系統分級，並依

附表10（如附表二）所定資通系統防護基準執行控制措施。

(二)經查中央及地方消防主管機關於資安分級辦法之法遵及合規性，可發現有三種合規性問題之樣態，包括「部分地方消防主管機關未確實評定資安責任等級」、「119派遣系統未確實認定核心資通系統及評定防護需求等級」，以及「未落實自訂之防護需求等級控制措施」等三類，茲臚述如下：

1、有關「部分地方消防主管機關未確實評定資安責任等級」部分，依照資安分級辦法，若機關符合「業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運」（第5條第2款）及「屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項」（第5條第5款），則應依該辦法評估為B級機關。僅符合「維運自行或委外設置、開發之資通系統者」（第6條第1款）方可列為C級機關。考量全國各消防局為緊急救護運作（含119派遣系統）所開發或維運之資通系統，均符合資安分級辦法第5條「區域性、地區性民眾服務或跨公務機關共用性」及「業務涉及區域性或地區性之關鍵基礎設施事項」等B級機關構成要件，爰其資安責任等級似均應不僅為C級。惟依消防署查復說明，全國各直轄市、縣（市）政府消防局之資安責任等級，除臺北市及新北市為B級機關外，其餘四都（桃園市、臺中市、臺南市及高雄市）及各縣（市）政府均為C級機關，消防署似應秉持資安聯防精神適時督飭地方主管機關檢討評估。

（1）為使資安風險與其控制措施符合衡平性原則，資安分級辦法對於不同資安責任等級之機關

尚賦予不同強度之應辦事項。茲將B級機關及C級機關應辦事項比較（兩等級均應辦理事項不列）如表6。由表6顯示，B級機關及C級機關之法遵事項、防護頻率及密度、第三方驗證及資安專職人力等資源配置均有顯著差異，俾使B級機關防護強度明顯高於C級機關。

表1　資安責任等級B級機關及C級機關應辦事項比較表

控制措施（110年8月23版本）		B級機關應辦事項（依據資安分級辦法附表3）	C級機關應辦事項（依據資安分級辦法附表5）
管理面	資通系統分級及防護基準	1年內……完成附表10之控制措施	2年內……完成附表10之控制措施
	資訊安全管理系統之導入	……3年內完成公正第三方驗證，並持續維持其驗證有效性	-
	資通安全專責人員	配置2人	配置1人
	內部資通安全稽核	每年辦理1次	每2年辦理1次
	資安治理成熟度評估	每年辦理1次	-
技術面	安全性檢測-弱點掃描	每年辦理1次	每2年辦理1次
	政府組態基準	1年內完成導入並持續維運	-
	端點偵測及應變機制	2年內完成導入並持續維運	-
	資通安全防護-入侵偵測及防禦機制	1年內啟用，並持續使用及適時進行軟、硬體之必要更新或升級	-
	資通安全防護-具有對外服務之核心資通系統者，應備應用程式防火牆	1年內啟用，並持續使用及適時進行軟、硬體之必要更新或升級	-
認知與訓練	專業證照及職能訓練證書	2名專職人員各自持有證照及證書各	1名專職人員持有證照及證書各1張

控制措施 （110年8月23版本）		B級機關應辦事項 （依據資安分級辦法附表3）	C級機關應辦事項 （依據資安分級辦法附表5）
		1張以上，並持續維持證照及證書之有效性	以上，並持續維持證照及證書之有效性

資料來源：依本調查案卷證整理。

（2）有關本案所涉高雄市消防局119派遣系統遭駭客入侵一節，查高雄市政府組織自治條例第6條第1項第15款以及該局組織規程第3條各款規定，該局掌理相關事項包括緊急救護業務。而該局119派遣系統之建置目的不僅為辦理前開緊急救護等核心業務，亦屬地區性關鍵基礎設施業務，爰其業務性質、服務範疇及其重要性，已明顯超出資安分級辦法對C級機關之標準，惟該局卻寬泛解釋法令並自評為C級機關，造成整體資安防護資源、密度及強度不足，肇生資安事件之風險極高，亦有檢討空間。

（3）據高雄市消防局查復，該局係依據資安分級辦法第10條第4款「其他與資通系統之提供、維運、規模或性質相關之具體事項」而調整資安責任等級為C級；惟查該條序文已敘明「機關……得考量下列事項對**國家安全、社會公共利益**、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級」，同條第1款更明定調整等級時應考量：「業務涉及……**緊急救援**與醫院業務者，其中斷或受妨礙」，高雄市消防局未依前開規定提升資安責任等級，反寬泛解讀該條規定而調降資安責任等級，尚非可採。此外機關資安責任等級之評估，不宜優先援引例外規定，而宜優先適用該

辦法第5條及第9條規定，以符資安分級辦法之規範意旨。

2、有關「119派遣系統未確實認定核心資通系統及評定防護需求等級」部分，高雄市消防局已確實依資安風險將119派遣系統列為中級；惟查消防署卻未將所開發之署版119派遣系統納入「核心資通系統」，復未切實按資安分級辦法附表9所示之構面（機密性、完整性、可用性及法遵性）評估119派遣系統之資通系統分級，而僅將該系統列為普級，導致控制措施與風險顯不相當。惟本案囿於資源未能通盤調查全國各地方消防機關運用於勤務指揮派遣相關資訊系統之防護需求等級是否妥適，爰消防署亦應適時通盤評估。

（1）首先，內政部消防署組織法第1條明定該署設立目的，係為統籌全國消防行政及災害防救事務，指揮並監督各級消防機關執行任務，而署版119派遣系統涉及該署與各該直轄市、縣(市)消防機關核心業務職掌，並由該署統籌規劃、辦理與督導。是以，119派遣系統明顯符合資安法施行細則第7條第2項所定「支持核心業務持續運作必要之系統」之定義，而應納入「核心資通系統」，消防署卻漏未納入，已有違誤。

（2）其次，資安分級辦法附表9規定各機關應評估資安事件發生時，按照對於機密性、完整性、可用性及法遵性之影響程度，賦予資通系統適當的防護需求等級，俾使受影響程度與風險控制強度相符。以機密性為例（如圖13），若資通系統遭資安事件影響而對機關之營運、資產或信譽等方面僅產生有限之影響時，才能列為「普級」；若將產生嚴重之影響時，則防護等

級就必須列為「中級」。而檢視本案情形，緊急救護或派遣資訊若有洩漏，則相關勤務指揮調度情形將為外界所掌握，不僅嚴重影響社會公益，於天災或戰時更將陷緊急救護體系於災難性的風險之中，因此應屬「嚴重之影響」，而不能僅稱之為「有限之影響」，益證消防署將119派遣系統僅列為「普級」洵屬不當，至於該署稱「該系統並無第一線受理民眾報案」、「由地方消防機關負責維運、管理，相關案件資訊於結案後始傳送至消防署」云云，亦無足採。

（3）另據該署查復資料顯示，署版119派遣系統支援多元管道案件報送機制，凡部署該系統之縣（市）消防機關所屬救災救護指揮中心之119受理人員，均係透過該系統進行案件受理、派遣及追蹤，涉及人力指揮調度必須之案件資訊如報案人、報案電話、案件地址、案情摘要、座標定位等均係透過系統傳遞至勤務單位，至通報案件後續之追蹤控管與重大災害之緊急應變，亦與地方消防機關執行核心業務密不可分，是以該署明顯低估119派遣系統之防護需求等級。

防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。

圖1　資通系統防護需求分級原則之機密性構面

資料來源：數位發展部資通安全署。

（4）再者，該署於106年爭取119派遣系統建置案中程計畫時，計畫內容敘明:「需要穩定軟硬體措施，以確保指派系統不會癱瘓」、「實是中央及地方政府刻不容緩之重要事項」等語。既已一再強調119派遣系統之重要性，益證該系統之防護需求等級絕不應僅列為「普級」。換言之，消防署於爭取系統建置經費時強調其重要性，而納列核心資通系統及防護需求等級時又輕忽其重要性，並辯稱「並無第一線受理民眾報案」、「地方消防機關負責維運、管理，相關案件資訊於結案後始傳送至消防署」云云，實無足採。

3、至於「未落實自訂之防護需求等級控制措施」部分，經查新北市消防局建置之「智慧雲端動態救護系統」已納列該局核心資通系統，並核定防護需求分級為「高」級，尚符相關資安法令規定。惟調查發現，EPCR系統自108年建置至113年全面清查帳號權限前，有部分項目並未切實符合資安分級辦法附表10之控制措施（如帳號管理、最小權限、紀錄事件及日誌紀錄內容等）。換言之，該局EPCR系統長期未確實控制帳號共用之風險，違反資安管理「說、寫、做一致」之基本原則，容易導致攻擊面管理之罅隙，亦有未洽。

（1）新北市政府於108年建置之智慧雲端動態救護系統，以電子化救護紀錄表取代傳統紙本，進而提升緊急醫療救護品質及效率。該系統透過配置於外勤單位之救護平板，可將生理監視器於現場測量之患者生理資訊（生命徵象、12導

程心電圖、緊急救護技術員評估處置等）即時同步傳輸至協力醫院，並結合電子化救護紀錄表資訊，使病患到院前資訊更加完整。

（2）新北市消防局政風室於110年辦理EPCR（含救護耗材管理）系統資訊稽核時，已發現有使用者之帳號密碼共用或交由他人使用情形，並於該局110年度資訊使用管理稽核報告指出，稽核時點該局緊急救護科、各大隊及分隊同仁皆為帳號共用，無法透過單一使用者帳號識別真正使用者，更無法透過使用者的帳號識別碼來記錄或追蹤其相關的使用行為。惟該局係於所屬人員洩密收賄案經廉政署113年1月25日搜索後，始陸續於同年1月28日限縮救護平板僅能查詢所屬分隊救護案件資訊、2月2日強化救護平板之使用與保管措施、2月5日設置各分隊人員個人帳號用以查詢所屬單位案件、2月7日限制各分隊之選定公務電腦可登入該系統網頁版查詢、2月20日限制僅結案超過3個小時以上案件方可由各分隊及大隊端進行查詢、5月16日由系統自動記錄帳號登出入及查詢案件時間紀錄資料用以比對異常等存取控制措施。

（3）該局113年辦理資訊使用管理稽核時，指出該系統仍有不符ISMS（資通安全管理系統）規定情形（摘要如下），有影響附表10控制措施縝密性之虞。

〈1〉程序面：權限審核流程未書面化。

〈2〉帳號管理：部分留職停薪人員帳號未停權、部分離退人員帳號未刪除、廠商部分測試帳號未註銷。

〈3〉紀錄保存：未建置使用者查詢紀錄檔功能、

未審查及覆核紀錄檔。

〈4〉權限管理：未適當限縮瀏覽權限，以及網頁版EPCR可於私人網路及電腦登入。

（4）承前，新北市消防局之EPCR系統經該局列為防護基準「高級」之資通系統，惟該系統之帳號管理機制有欠妥適，長期存在所屬同仁共用帳號情事。相關案件查詢權限亦未做最小化開放，使任意使用者可查詢非所屬分隊案件，且系統未完整記錄帳號登出入及查詢案件時間紀錄（Log）資料，均於案發後方有檢討改善作為。前述情形均有未落實附表10各項控制措施之情形，且涉及新北市消防局案之殯葬業者即曾以取得之EPCR系統帳號、密碼登入查詢案件資料，對於救護患者之個人資料蒐集、處理及利用構成風險，亦有未洽。

(三)綜上，資安控制措施必須與資安風險相當，以符合衡平性原則，實為資安相關法規之制定精神，本案經調查中央及地方消防主管機關於資安分級辦法之合規性，發現部分機關之資安責任等級評估、119派遣系統防護基準等級以及EPCR系統控制措施合規性等，均有未盡周妥情形。相關機關未確實依據前開辦法評定資通安全等級、認定系統防護機等並執行相應控制措施，不利緊急救護體系之資安風險管理，消防署允宜秉持資安聯防精神，適時督飭相關機關通盤檢討。

參、處理辦法：

一、修正後通過。

二、調查意見一，函請新北市政府督飭所屬消防局及警察局確實檢討改進見復。

三、調查意見二，函送內政部消防署督飭相關機關通盤檢討見復。

四、調查意見，函送法務部參考。

五、調查意見(含案由、處理辦法、調查委員姓名及附表)，經委員會討論通過後，遮隱個資上網公布。

調查委員：施錦芳

張菊芳

趙永清

附表一、「資通安全責任等級分級辦法」第11條附表9「資通系統防護需求分級原則」(110年8月23日修正)

附表九 資通系統防護需求分級原則

防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

附表二、「資通安全責任等級分級辦法」第11條附表10 「資通系統防護基準」(110年8月23日修正)

附表十　資通系統防護基準

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
存取控制	帳號管理	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、應依機關規定之情況及條件，使用資通系統。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。 五、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、遠端存取之來源應為機關已預先定義及管理之存取控制點。 二、等級「普」之所有控制措施。		一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取機關內部網段或資通系統後

				臺之連線。 四、應採用加密機制。
事件日誌與可歸責性	記錄事件	一、應定期審查機關所保留資通系統產生之日誌。 二、等級「普」之所有控制措施。		一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。
	日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。		
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。		
	日誌處理失效之回應	一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	資通系統於日誌處理失效時，應採取適當之行動。	
	時戳及校時	一、系統內部時鐘應定期與基準時間源進行同步。 二、等級「普」之所有控制措施。		資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
	日誌資訊之保護	一、定期備份日誌至原系統外之其他實體系統。	一、應運用雜湊或其他適當方式之完整性確保機	對日誌之存取管理，僅限於有權限之使用者。

		二、等級「中」之所有控制措施。	制。 二、等級「普」之所有控制措施。	
營運持續計畫	系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
	系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。		無要求。
識別與鑑別	內部使用者之識別與鑑別	一、對資通系統之存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	
	身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。		一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失

			敗驗證機制。 四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性）進行確認。	
	系統發展生命週期設計階段	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	無要求。
	系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、系統應具備發生嚴重錯誤時之通知機制。 三、等級「中」及「普」之所有控制措施。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。
	系統發展生命	一、執行「滲透測試」安全檢測。	執行「弱點掃描」安全檢測。

	週期測試階段	二、等級「中」及「普」之所有控制措施。		
	系統發展生命週期部署與維運階段	一、於系統發展生命週期之維運階段，應執行版本控制與變更管理。 二、等級「普」之所有控制措施。		一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統不使用預設密碼。
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
	獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
	系統文件	應儲存與管理系統發展生命週期之相關文件。		
系統與通訊保護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證應定期更換。 五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	無要求。	無要求。
	資料儲	資通系統重要組態設	無要求。	無要求。

	存之安全	定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。		
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二、等級「中」之所有控制措施。	一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無要求。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之系統防護基準。