考試院第 11 屆第 225 次會議考選部重要業務報告

民國 102 年 2 月 7 日

壹、考選行政

本部因應個人資料保護法施行相關作為執行情形報告

一、前言

個人資料保護法（以下稱個資法）於民國 99 年 5 月 26 日經總統公布，嗣經行政院於 101 年 9 月 21 日以行政院院臺法字第 1010056845 號令發布除第 6 條、54 條條文外，其餘條文定自 101 年 10 月 1 日施行;並於同年月 26 日公布個人資料保護法施行細則。

本部辦理國家考試，依法蒐集應考人報名資料，另為典試及題庫作業需要，蒐集學者專家個人資料建立國家考試典試人力資料庫；各項考試期間聘用協助試務作業之臨時人員，及考試期間遴聘之監場人員，爰保有個人資料項目及總量甚為龐多，自 84 年 8 月 11 日公布施行「電腦處理個人資料保護法」，本部悉依前揭法規辦理各項個資之處理及利用。

鑑於修正公布之個資法擴大個人資料定義以及適用範圍主體，對於個資蒐集、處理及利用要件增加相關規範，就發生個資外洩採無過失損害賠償責任，且保護之客體擴及非經電腦處理之個人資料，對機關個資管理責任衝擊甚鉅，爰自個資法於 99 年公布後，本部即配合主管機關法務部指導原則規劃相關因應作為，俾期加強本部涉及個人資料管理制度及措施之完備性。

二、因應作為執行情形

本部參照法務部所擬個資法施行後各公務機關注意參考事項，並依據個資法施行細則第 12 條所定防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，逐步採行因應作為（詳如附表）。茲從法制面、資訊面及管理執行面等三方面說明本部目前已執行之具體作為如下：

（一）法制面：

1、**公告保有個資項目：**本部依據個資法規定，先於 100 年 12 月完成本部保有及管理個人資料項目清點，並公告於本部全球

資訊網政府資訊公開項，供公眾查閱。另配合法務部於 101 年 10 月 1 日修正公布個人資料保護法之特定目的及個人資料之類別，及依個資法施行細則第 23 條規定，隨時公告更新本部保有個人資料，分別於 101 年 11 月 8 日及 102 年 1 月 11 日二次修正公布本部保有個人資料項目，其中包括國家考試典試人力資訊系統、國家考試網路報名系統、候用監場人員及臨時人員等 98 種資料項目。

2、制定個資管理規範及組織：

（1）訂定「考選部個人資料保護管理要點」，於 101 年 10 月 8 日公布施行，並即成立「考選部個人資料保護管理執行小組」，由本部政務次長擔任召集人，委員 15 人由各單位指派擔任，負責本部個人資料保護管理之規劃、執行及適法性之檢視、審議等事項。

（2）執行小組初期以每一個月召開一次會議為原則，並適時邀集外部個資專家與會。迄至本（102）年 1 月，已分別召開 3 次執行小組會議及 1 次專家座談會議，其中專家座談會邀請資訊工業策進會法律科技研究所專家到部簡報公務機關因應個人資料保護法之策略與作為，並就本部因應個資法之執行現況及適用疑義進行相關議題討論。

（3）另執行小組推舉稽核委員 7 人，每季至少進行本部各單位個人資料保護執行情形定期稽核一次，以確保本部同仁落實執行各項個人資料保護管理規範，第一次定期稽核已於本年 1 月中旬進行完竣；並預定於 4 月辦理專案稽核，擴大稽核範圍至臨時人員。

（二）資訊面：

本部自 91 年起，即依據考試院暨所屬機關資訊安全管理要點及本部危機處理小組作業要點，建立本部資訊安全相關管理制度，並視資訊系統之風險管理層級，導入國際資訊安全（ISO27001）稽核與驗證，現有管理制度如下：

1、考選部資訊安全作業管理規範：配合鈞院推動資訊安全管理系統（Information Security Management System, ISMS）政策，依據鈞院 89 年 5 月 9 日核定之「考試院暨所屬機關資訊安全

管理要點」，於 91 年 8 月訂定「考選部資訊安全作業管理規範」，建立本部資訊系統、網路及各項資訊軟硬設備安全管理制度。101 年 8 月並配合個資法規定，增加個資法為規範依據，並修正調整本部資訊安全推動小組，由政務次長擔任召集人。

2、考選部資通安全事件緊急應變計畫：參照前揭資訊安全作業管理規範，除於 94 年 2 月依據「考選部危機處理小組作業要點」訂定，成立本部資通安全緊急應變小組，建置本部資訊系統與網路安全事前安全防護機制、事中緊急應變程序及通報流程，並適時配合行政院國家資通安全會報訂頒之「國家資通安全通報應變綱要」（101 年 8 月 1 日修正公布），修正相關資安事故預防、通報與應變作業。101 年 11 月 27 日並主辦「考試院暨所屬資通安全緊急應變小組」101 年第 2 次會議，院及所屬各機關於該次會中就因應個資法之執行情形進行經驗交流。

3、**國際資訊安全（ISO27001）驗證：**本部國家考試網路報名系統及試務整合性管理系統，分別於 95 年 5 月及 99 年 5 月取得認證，其中國家考試網路報名系統於 101 年 11 月業完成第 3 次重新認證作業，試務整合性管理系統將於本年 3 月辦理第 1 次重新認證作業。配合前揭國際資訊安全認證，本部除定期接受驗證機構進行外部稽核外，並設有資訊安全處理小組，定期進行本二系統之內部稽核作業，所稽核範圍均含蓋涉及此二系統之本部正式職員、臨時人員及相關委外廠商；另資訊管理處與系統承商每季定期召開一次維運專案會議，審查及檢討防毒、主機系統及網路等資安重要事件。

（三）管理執行面：

1、**告知義務之履行：**個資法施行前，本部即於 101 年 8 月，依個資法第 8 條規定，於國家考試典試人力調查表末頁，增列蒐集個人資料時應明確告知當事人之事項，並送個資當事人簽名確認。另針對個資法施行前本部已蒐集或非由當事人提供之個人資料，亦要求同仁依個資法第 9 條第 3 項規定，於首次利用時告知個資當事人。

2、**進行資訊系統個資流程盤點，確實掌握涉及個人資料之內容、流程及風險程度**：本部於 101 年 8 月先由資訊管理處進行資訊系統盤點，並配合盤點及風險評估結果，逐步進行各項資訊系統個資瘦身，提本部個人資料保護管理執行小組討論。主要有：設定「國家考試網路報名系統」會員資料保存期限（3 年）及刪除機制，降低個資保存風險；刪除「統計系統」可直接辨識之個資欄位，以減少保有個資系統等。本部刻正依資訊工業策進會資安專家建議，將於 2 個月內儘速完成本部法規盤點作業。

3、**加強個資及資安認知宣導及教育訓練**：本部已於 101 年 9 月 13 日及 9 月 25 日辦理 2 梯次個人資料保護法 3 小時講習及測驗，未來將適時賡續辦理。另為加強機關人員資安意識，每年均定期辦理 2 梯次社交工程教育訓練及演練，本（102）年已定於 3 月辦理。本年 2 月 6 日並已針對本部臨時人員辦理個人資料保護法及典試試務資訊安全意識講習。

4、**導入資料庫稽核系統，加強本部相關系統使用紀錄、軌跡資料及證據保存能力**：因應個資法對於交易紀錄保存與稽核舉證要求，本部已於 101 年 12 月優先針對保有完整個資之「典試人力管理資訊系統」及「試務整合性管理資訊系統」二系統完成導入資料庫稽核系統（Imperva SecureSphere）。另於本年規劃針對國家考試網路報名系統導入資料庫稽核系統建置案，並進行效能測試，將視考選基金執行情形適時導入。

三、 結語

個人資料保護管理制度是一個規劃（Plan）、執行（Do）、檢查（Check）及行動（Act）的 PDCA 循環作業流程，必須組織內所有單位及人員持續改善工作流程，與隨時因應組織內外部發展趨勢、法律、規範及環境的變化，進行調整與持續提升改善。本部將持續檢視內部業務流程及相關法規，加強人員個資保護意識與資訊安全防範能力，以建立出一套完善的個資保護框架和實務，俾完善管理本部保有之個資，並保護同仁避免誤蹈法網。

附表　本部依個資法施行細則第 12 條採行之相關因應作為

個資法施行細則第 12 條規定之必要措施	本部相關因應作為
一、配置管理之人員及相當資源	1. 本部於 101 年 10 月 8 日公布「考選部個人資料保護管理要點」，並據以成立考選部個人資料保護管理執行小組，由政務次長擔任執行小組召集人，委員 15 人由各單位指派，由資訊管理處任小組幕僚單位，法制事項幕僚為考選規劃司。該執行小組負責本部個人資料保護、管理之規劃、執行及適法性之檢視、審議評估等事項，初期以每一個月召開一次會議為原則，並適時邀集外部個資專家與會，訖至本（102）年 1 月，已召開 3 次執行小組會議，及邀請資訊工業策進會法律科技研究所個資專家到部進行 1 次專題座談會議。 2. 建立本部個資聯絡窗口及各單位個人資料保護專人名單。
二、界定個人資料之範圍	1. 於 100 年 12 月依個資法第 17 條規定，將本部保有個人資料項目公開於全球資訊網站政府公開資訊項下，供公眾查閱。另依個資法施行細則第 23 條規定，隨時公告更新保有本部保有個人資料，於 101 年 11 月 8 日第一次修正公布本部保有個人資料項目一覽表。 2. 配合法務部於 101 年 10 月 1 日修正公布個人資料保護法之特定目的及個人資料之類別，於本年 1 月 11 日第二次修正本部保有個人資料項目一覽表。
三、個人資料之風險評估及管理機制	1. 本部於101年8月由資訊管理處先行就資訊系統進行個資盤點及風險評估，並配合評估結果，逐步進行各項資訊系統個資瘦身作業，提本部個人資料保護管理執行小組討論。目前已完成之系統主要有：（1）設定「國家考試網路報名系統」會員資料保存期限為 3 年及建立會員自主刪除機制，降低個資保存風險；（2）刪除「統計系統」可直接辨識之個資欄位，以減少保有個資系統等。（3）簡化本部「題務組人力資料」登載及查詢系統管道，使本部保有個資符合最小化原則。未來將賡續依據個資蒐集原則，檢視本部各項資料庫系統保有個資之適當性。 2. 依 101 年 12 月 11 日資訊工業策進會資安專家座談會建議，由本部法規會請各單位於本年 3 月前內完成本部法規

	盤點作業，俾使本部個資蒐集、處理及利用之法制依據更為完備。
四、事故之預防、通報及應變機制。	1.本部國家考試網路報名系統及試務整合性管理系統，分別於95年5月及99年5月取得國際資訊安全（ISO27001）認證，其中國家考試網路報名系統業於101年11月完成第3次重新認證作業，試務整合性管理系統將於本年3月辦理第1次重新認證作業。依據資訊安全管理制度驗證，本部定期辦理資安事件演練。101年計辦理2次資安演練，分別為： （1）101年6月14日：「國家考試網路報名系統」主站備份資料回存主站資料庫主機計畫演練，進行正式資料庫系統遭受攻擊導致資料毀損或破壞時，因同步備援資料亦不正常（因即時同步抄寫），必須採用備份資料進行資料回復作業之實際程序演練。 （2）101年7月6日：「國家考試試務整合性管理系統」異地回復演練，進行系統遭遇服務中斷達一定程度時，可以迅速採取行動使系統回復正常作業之實際程序演練。 2.配合鈞院推動資訊安全管理系統（Information Security Management System, ISMS）政策，依據鈞院89年5月9日核定之「考試院暨所屬機關資訊安全管理要點」，於91年8月訂定「考選部資訊安全作業管理規範」，建立本部資訊系統、網路及各項資訊軟硬設備安全管理制度。並參照前揭資訊安全作業管理規範，於94年2月訂定「考選部資通安全事件緊急應變計畫」，編立本部資通安全緊急應變小組，建置本部資訊系統與網路安全事前安全防護機制、事中緊急應變程序及通報流程。101年100年8月並配合個資法，修正調整本部資訊安全推動小組，由政務次長擔任召集人。11月27日並主辦「考試院暨所屬資通安全緊急應變小組」101年第2次會議，院及所屬各機關於該次會中就因應個資法之執行情形進行經驗交流。 3.依據行政院國家資通安全會報訂頒之「國家資通安全通報應變綱要」所定「資通安全業務資安事件通報與應變作業流程」，辦理相關資安事故預防、通報與應變作業。
五、個人資料蒐	於101年10月8日公布「考選部個人資料保護管理要

集、處理及利用之內部管理程序	點」，明定本部各單位就個人資料之蒐集、處理或利用之程序。
六、資料安全管理及人員管理	1. 配合前揭國際資訊安全（ISO27001）認證作業規範，本部除定期接受驗證機構進行外部稽核外，並設有資訊安全處理小組，由外部資安顧問協同定期進行本二系統之內部稽核作業；另資訊管理處與系統承商每季定期召開一次維運專案會議，審查及檢討防毒、主機系統、及網路等資安重要事件。 2. 依法務部提供之「電腦資訊安全自主檢查表」，於每日同仁開啟電腦時自動呈現俾提醒同仁隨時保持資訊安全警覺。 3. 加強委外廠商管理，要求承商配帶識別證件；在委外契約中，明確定義第三方對個資管理上的職責要求和對第三方實施個資管理稽核的權利，以確認委外廠商是否落實相關個資管理作業，俾符合個資法對公務機關委外管理之要求。
七、認知宣導及教育訓練	1. 本部已於 101 年 9 月 13 日及 9 月 25 日就個人資料保護法辦理 2 梯次全員講習（3 小時）及測驗，未來將適時賡續辦理認知訓練。 2. 為加強機關人員資安意識，依本部資訊安全教育訓練作業綱要規定，所有員工每年應至少達成 3 小時以上之資訊安全認知教育訓練，資訊安全處理小組系統管理與內部稽核人員每年應至少完成 6 小時以上之專業性資訊安全教育訓練。爰每年均定期辦理 2 梯次社交工程教育訓練及演練作業，本年將於 3 月辦理，俾加強人員個資及資安認知。 3. 本年2月6日已針對本部臨時人員辦理個人資料保護法及典試試務資訊安全意識講習。
八、設備安全管理	1. 於 101 年 9 月 24 日修正公布「考選部資訊設備管理及使用規範」，加強維護本部資訊設備使用管理及安全維護。 2. 執行電腦設備管理，加強可攜式與行動設施的存取控制機制： （1）個人電腦：針對本部試務工作場所，回收電腦重新設定，除經申請之特定電腦外，禁用移動式儲存媒體（如 USB 隨身碟、外接硬碟）及電子郵件，以杜絕非授權之電子檔案傳輸行為。

	（2）筆記型電腦：限制使用者安裝軟體及修改網路設定權限，限定保管者以個人帳號、外借者以使用者（USER）帳號登入。
九、資料安全稽核機制	1.持續依據資訊安全管理制度 ISO27001，定期進行內部及外部安全稽核。個資法施行後，已進行 2 次安全稽核，分別為： （1）101 年 11 月 6 日完成試務整合性管理資訊系統內部稽核;該系統預定於 102 年 3 月辦理重新認證外部稽核。 （2）101 年 11 月 12 日、13 日完成網路報名系統 ISO27001 外部稽核，並取得第 3 次重新認證。 2.依據本部個人資料保護管理執行要點規定,由本部稽核委員 7 人,每季至少進行本部各單位個人資料保護執行情形定期稽核一次,以確保本部同仁落實執行本部各項個人資料保護管理制度,第一次定期稽核會議已於本年 1 月中旬辦理完竣。
十、使用紀錄、軌跡資料及證據保存	1.持續依據國際資訊安全（ISO27001）認證作業規範，於資訊系統建置稽核管理系統，蒐集應用程式存取資料、資料庫本機操作及作業系統軌跡資料，並定期提出稽核報告。 2.於 101 年 12 月優先針對保有個資之「典試人力管理資訊系統」及「試務整合性管理資訊系統」二系統完成安裝資料庫稽核系統（Imperva SecureSphere）軟體，並請承商配合本部需求修改系統功能，強化使用紀錄及軌跡資料，以因應個資法對於交易記錄保存與稽核舉證要求。 3.另預定於本年規劃針對國家考試網路報名系統導入資料庫稽核系統建置案，刻正進行效能測試，將視測試結果及本部考選基金執行情形適時導入，以逐步提升本部資料庫使用紀錄、軌跡資料及證據保存能力。