普(抽)查資料管制室建置構想

行政院主計處為保障普（抽）查受訪者權利，避免個別資料外洩，並擴大統計資料運用層面，爰規劃管理機制，並設置資料管制室，提供各界應用。

◉ **潘寧馨、陳巧鐘、陳明志**（行政院主計處第四局科長、專員、研究員）

壹、前言

統計法及同法施行細則明文規定，各機關對統計調查取得之個別資料應予保密，除供整體統計分析外，不作其他用途，各調查主辦機關多能恪遵是項規定，善盡保密之責。惟邇來資訊技術快速發展，外界對統計資料之需求日殷，使用目的亦趨多元，個別資料外洩風險急遽增加；復以詐騙事件層出不窮，個人隱私意識抬頭，調查環境日益艱困，主辦機關必須以更嚴謹之態度，執行各項資訊安全作業，俾免個別資料外洩，損害受訪者權益，進而爭取其信賴與合作，提升統計調查品質及確度。行政院主計處爰積極規劃資料管制機制，設置獨立空間提供需求者使用所需資料，期於資訊安全無虞之情形下，滿足各界對於普（抽）查資料應用及分析需求。

貳、現況簡介

除於行政院主計處全球資訊網公開登載並彙總陳示之統計資訊及資料庫查詢系統，外界如須索取其他各類型式資料，原則須於行政院主計處全球資訊網中「本處出版品目錄」下之「統計資訊提供」或「中華民國統計資訊網」中「出版品及統計資訊提供」項下搜尋所需資料，經既定申請程序，於行政院主計處審查核可後提供，並依「行政院主計處提供統計資料及使用資料管制室收費標準」規定，酌收資料處理機時費。惟鑒於資料應用方式益趨多元，前揭網站所列資訊或無法全面滿足外界需求，爰另補充說明如次：

一、基本國勢調查光碟資訊：

基本國勢調查原始資料因涵蓋面廣、資訊豐富，統計利用價值甚高而需求者眾，爰應各界要求及作業

便利性，逕行提供移除個體識別碼之光碟資料，惟部分資料可能仍具個別資料辨識之風險。

二、**代為處理方式**：鑒於邇來資訊發展蓬勃，電腦應用普及，部分已移除個體識別碼之普（抽）查原始資料，仍有可能藉由交叉比對及檔案連結，辨識特定個別資料。行政院主計處爰依不同需求，先行產生彙總統計資訊，或移除相關資料欄位後再行提供，俾降低隱私外洩風險。

前揭作法業已行之有年，亦未曾有不法及不當使用資料之情事發生，惟因逕行提供光碟資訊，個別資料辨識之風險仍存；而代為處理則須針對不同需求，研判資料內容並予量身訂作，非僅耗時，內部作業負擔亦較重。為兼顧資訊安全，提升普（抽）查資訊之應用價值，參酌國內、外作法，建置資料管制室之構想，爰應運而生。

參、國內、外作法簡介

鑒於近年電腦及網路應用日益普及，資訊安全概念之重要性亦顯著提升，部分學術研究機構及機密性資料主管之政府機關，為避免業務產生或蒐集之個別資料遭人為意圖不當及不法使用，爰制訂資訊使用管制措施，其中設置「資料管制室（Data Lab）」為首要作法，茲舉國內、外數例並略述如次：

一、**中央研究院**：為達統計資訊應用普及化目的，中央研究院調查研究專題中心於民國93年即著手規劃機密資料使用管理機制，將該院及相關政府機關辦理之統計調查原始電子資料，以設立機密資料使用室（On-site data laboratory）並移除個體識別欄位之方式，提供各界人士分析應用。該中心規定使用者必須符合特定資格，經過申請審核通過後，始能預約親赴資料使用室臨場使用資料，並針對提供使用者分析之原始與衍生電子資料、書面資料之攜出、使用場地、電腦安全防護、使用者行為監控、物品管控方式，訂定相關管制規定，俾維護資訊安全。

二、**財政部財稅資料中心**：財政部因主管各類財產及財稅資料，機密性甚高，爰責由財稅資料中心成立資料監控室，分別以「財稅資料中心UNIX主機臨場作業要點」及「外單位使用監控室臨場作業管制要點」，對內及對外嚴格規範財稅資料之使用，包括使用對象、地點及攜出資料欄位等事項；另如採資料檔逕行提供方式，除移除個體識別欄位外，亦整體考量各該提供對象歷次索取之檔案，經連結後有無隱私外洩之疑慮；至內部人員如須瀏覽或使用個

別資料，須經申請許可後，於監控室爲之，相關程式均寫入記錄檔供日後查驗。

三、**美國商務部普查局**：先進國家中實施資訊安全措施最具規模及成效者，當屬美國。美國商務部普查局因管轄各類普（抽）查資訊，爲降低隱私外洩之可能性，爰責由經濟研究中心（The Center for Economics Studies； CES），於全美設置9處資料研究中心（Research Data Centers；RDC），供爲臨場使用及管制業務之用，茲依程序條列簡介如次：

（一）計畫研提及審核：資料申請者必須提出完整研究計畫，包括使用動機、計畫、期間、方法、所需資料之機密性（confidentiality）等事項，經濟研究中心爰據以邀集相關專家審查其內容，通過者方得使用資料研究中心。

（二）「特別立誓」（Special Sworn Status；SSS）：通過審核之申請者先行於既定表格填妥各項資料，由普查局相關人員爲公證人，負責查驗身分並確認申請者同意該表格所列各項規定。經簽名後，申請者即取得「特別立誓」認證。如資料使用期間較長，該認證須每年更新，方得繼續使用。

（三）帳號啓動及訓練：經前揭程序，資料研究中心人員接續執行帳號啓動，至申請者除須研讀資料研究中心寄發之使用手冊外，尚須按年採線上學習方式，接受機密資料法令規範與資訊安全訓練，通過者方得使用資料研究中心。

（四）使用時間及地點安排：申請者於申請表格須註明臨場使用地點、使用期間及頻度等事項，資料研究中心爰據以安排作業進程，並對於配合度高且遵守規定者，於翌次申請時給予較高使用順位。

（五）申請者成果回饋：申請者於資料使用期間須按時提交資料使用成果及進度資訊予資料研究中心，並於使用完畢後提交研究或計畫成果，並收錄於經濟研究中心論壇（CES Discussion Paper series），同時作爲未來再度申請使用資料研究中心之重要參據。

肆、管制室建置規劃

爲落實資料保密工作，並使管制作業有所依循，行政院主計處爰仿效前揭國內、外作法，積極研擬「提供普（抽）查資料管制作業要點」，其內容係針對資料分類、使用者申請及內部審核程序、管制室軟、硬體規劃及使用方式等事項妥適規範，俾供爲作業準則。茲將前揭事項概述如次：

一、資料分類：為完整呈現普（抽）查資料全貌，俾利資料使用及管制，行政院主計處各普（抽）查主辦科爰將業管資料依個別資訊揭露之程度分為二類，置於行政院主計處全球資訊網，供使用者選取應用。茲略述如次：

（一）第一類資料：經去除識別欄位（如身分證字號、營利事業統一編號、公司中文名稱、姓名等）及足以辨識個別資料特徵值後之原始資料，或原始資料經同類合併加總、彙整等處理後之次級資料，且其內容無涉隱私。

（二）第二類資料：指去除個體識別欄位或將其亂碼處理後，資料內容仍具敏感性或有涉及隱私之虞。

二、資料提供對象、申請程序及使用限制：依前揭資料類別規範如次：

（一）第一類資料：無特殊對象限制，得由資料需求者或受委託者填寫申請單後，向本處資料主管單位申請，各單位受理後，依規定程序審查核可後逕行提供（詳附圖）。

（二）第二類資料：鑒於資料具有隱私外洩之虞，資料需求者須行文提出申請，經審查核可後，親赴本處建置之資料管制室，簽署保密切結書後，進行臨場作業（詳附圖），且提供對象僅限政府、民意機關、學校及學術機構，其使用限制依提供對象分類列述如次：

1.政府或民意機關：須以統計為目的，若為辦理統計調查所需，該調查須依法列管在案。除應調查名冊所需，攜出調查受訪者基本資料外，餘僅限無涉個別隱私之原始資料或彙總之統計結果；若為提升統計調查運用效能，精簡相關統計調查，得經亂碼處理後，連結相關檔案。

2.學校或學術研究機構：須以從事相關研究為目的，且非經許可不得連結其他檔案，攜出資料僅限彙總之統計結果。

三、作業分工：

（一）普（抽）查主辦科：即資料主管科，負責以下作業：

1.事先審查：就使用者所提之申請內容，審查使用者身分、使用目的及用途、所需資料內容及攜出內容等事項是否符合規定。

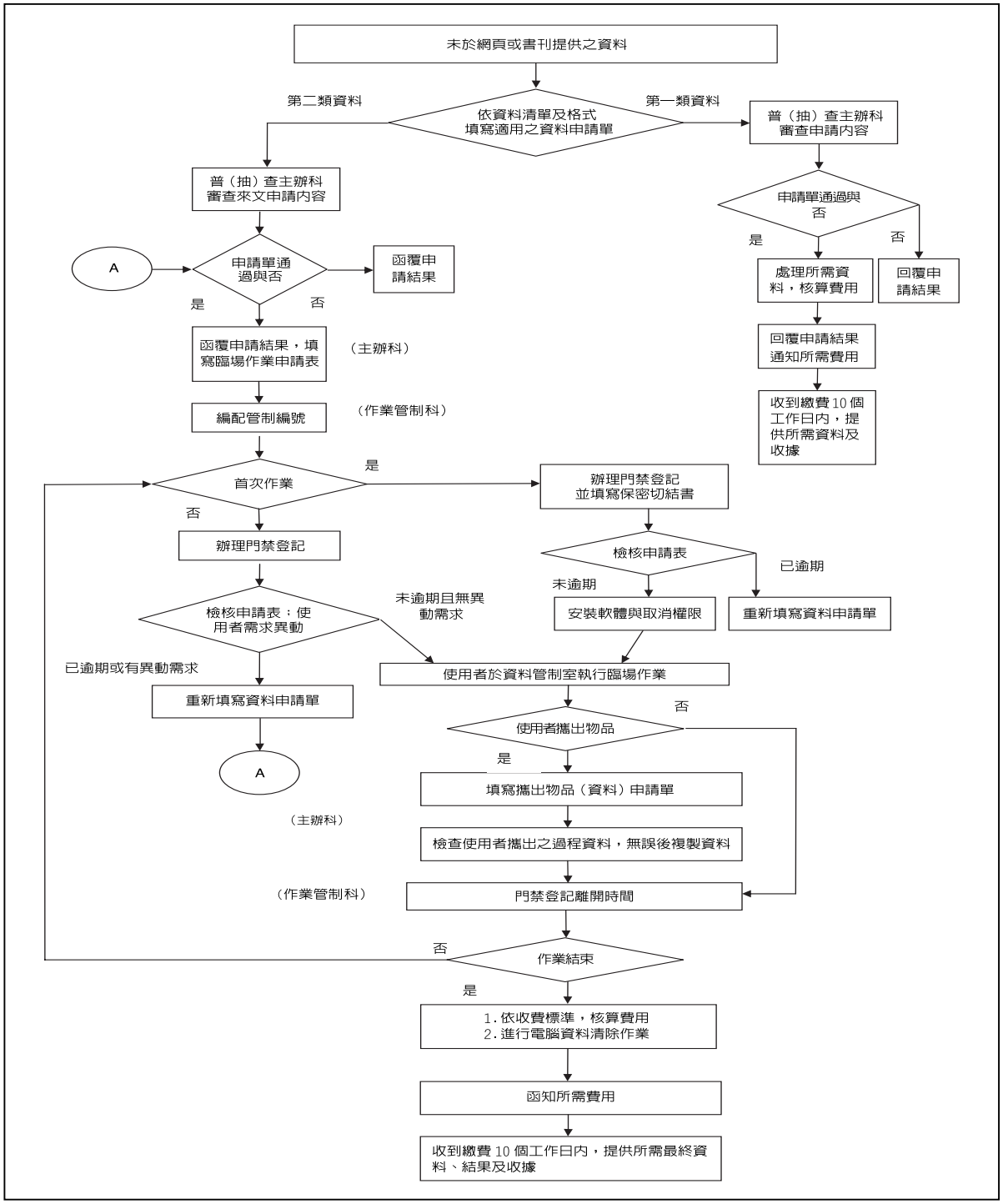
2.臨場作業執行：

（1）執行前：整理資料使用者所需資料並放入抽取式硬碟，以及臨場作業執行之申請。

（2）執行中：抽取式硬碟之保管與安裝設定作業、檢查使用者需用軟體授權文件及相關資料、使用者疑難問題之排解及需求異動之申請。

（3）執行後：保管保密切

行政院主計處普（抽）查資料申請程序流程圖



結書、檢查使用者所欲攜出之資料內容、執行電腦資料清除作業。

（二）作業管制科：分別由行政院主計處第三局及第四局指派，並負責以下工作：

1.編配管制編號、電腦帳號與密碼授權。

2.門禁登記、進出門禁卡片保管與分發。

3.控管資料管制室大門。

4.資料使用者之錄影監控。

四、資料管制室作業：鑒於第二類資料受訪者隱私揭露之風險較高，爲防止使用者不當或不法使用資料，爰針對資料管制室之使用空間、設備、電腦安全防護、對使用者行爲監控及作業查核，規範嚴密事項如次：

（一）管制室地點、使用空間及設備：資料管制室設置於行政院主計處廣博大樓4樓東側，使用面積約7坪，並配置個人電腦6台供臨場使用，另爲加強資訊安全及人員管控，尚須裝設以下設備：

1.監視設備：含監控主機及攝影機3部，裝設於管制室門口及對角，期全盤掌握人員使用情形。其影像至少須保存至各作業結束後2個月，並由作業管制人員負責錄影監控。

2.人員進出管制設備：人員皆以感應卡進出，並以自動門方式控管，資料使用者進出資料管制室作業，應至作業管制科填寫「資料管制室進出登記表」，並由該科管控資料管制室人員進出。

3.抽取式硬碟作業：爲方便資料使用者於不同時間使用同台個人電腦，以彈性運用處理資料之時間，個人電腦內硬碟係採抽取式方式作業，各電腦均可配置多個抽取式硬碟，期防止儲存資料被其他使用者窺視，並可提高電腦使用效能。

（二）電腦安全防護方式：

1.不連線單機作業：爲強化權限管控，防止資料藉連線方式外洩，爰提供不連線單機作業之個人電腦設備供資料使用者使用，各使用者配賦不同的電腦帳號及開機密碼。

2.抽取式硬碟安裝卸除：歷次作業普（抽）查主辦科均須執行抽取式硬碟安裝設定作業，並於資料使用者離開後卸除抽取式硬碟，置於資料管制室專用鐵櫃內上鎖保管。

3.設備使用限制：資料使用者只能操作鍵盤和滑鼠，無法自行操作其他配備或外接裝置。

4.資料清除：普（抽）查主辦科於作業結束後，檢視個人電腦內軟硬體檔案，於次日開始進行資料清除作業。

（三）對使用者行爲的監控方式：

1.攜入物品：

（1）資料管制室內禁止飲食、攜帶手機、攝影機、筆記型電腦、PDA等可攜式儲存設備，且不得擅自以照相或其他方式，將電腦執行之畫面及結果，攜出資料管制室。

（2）攜帶之物品須置於資料管制室專用鐵櫃內。

2.攜出資料：

（1）須事先填寫「資料管制室臨場作業攜出物品（資料）申請單」。

（2）普（抽）查主辦科依申請之輸出檔案格式，逐一檢視輸出內容，經確認無誤後，開放USB可攜式儲存媒體之使用者權限，並複製資料使用者所需資料。

（四）作業查核：

1.禁止未經授權人員進入資料管制室臨場作業，一經發現，立即由作業管制科先行處理，若有無法處理、突發或重大危急狀況等，始通報政風處處理。

2.普（抽）查主辦科應依據作業管制科簽送之相關統計表報、「資料管制室進出登記表」及錄影等資料，辦理查核。

伍、結語

於各界對統計調查資訊殷切之需求下，妥適提供調查資料供各界應用，俾提升其效能，實係調查主辦機關之基本職責，亦為資料使用者殷切期盼之目標；惟因個人隱私意識抬頭，「保障受訪者權益」亦為調查主辦機關應盡義務。欲於前揭職責及義務間取得平衡，「建立適切之資料管制機制」，確屬良方。而實施嚴謹之資料分類措施，並建置資料管制室，於軟、硬體嚴密管控之環境中，規範使用者臨場執行資料處理作業，非但可提升資訊安全等級，亦可精準滿足使用者需求，並提供一體適用之程序及規範，降低內部作業負擔，鑒於優點甚多，美國普查局爰於眾多先進國家中率先採行，實施多年，確具成效；而行政院主計處歷經長時期之醞釀構思，參酌多方寶貴意見及經驗，終完成普（抽）查資料管制室規劃工作，期於工作人員戮力合作下，辦理建置作業並確實發揮資料管制功能，進而達成擴大資訊應用層面，保障受訪者隱私之最終目標。

參考文獻

1.Guidelines for the Operation of the Census Bureau Research Data Centers, March 15, 2006, U.S. Census Bureau Center for Economic Studies.

2.U.S. Bureau of the Census Center for Economic Studies Research Data Centers Handbook for Researchers, January 2008, U.S. Census Bureau Center for Economic Studies.

3.Instructions for Obtaining Special Sworn Status Center for Economic Studies, U.S. Census Bureau Center for Economic Studies.

4.「外單位使用監控室臨場作業管制要點」、「財稅資料中心UNIX主機臨場作業要點」，財政部財稅資料中心。

5.機密性調查資料資訊安全管控說明——以「台灣教育長期追蹤資料庫」現場使用版為例，中央研究院調查研究專題中心。❖