行政資料傳輸正式報告書

壹、前言

隨著政府數位化政策持續深化，跨部門協作與資料整合的需求日益增加，建立一套安全、標準化且高效的行政資料傳輸基礎設施，已成為當前推動智慧治理與強化公共服務的關鍵任務。現階段多數機關在資料交換上仍面臨流程不一致、效率低落、資安風險高等挑戰，亟需導入具備韌性、合規性與可擴充性的整合解方。

為因應上述需求，數位發展部積極推動多項核心數位基礎建設，包括：**T-Road 政府資料傳輸平臺**，提供具備加密、驗證與可稽核性之資料交換機制；**CNS11643 全字庫**，建立統一文字標準以促進資料正確與一致性；**ODF 開放文件格式**，強化跨機關文件的應用互通性；以及導入**零信任架構（Zero Trust Architecture, ZTA）**，提升政府系統整體的存取控管與資安防護能力。

這些基礎建設不僅回應當前行政資料流通的實務需求，更為未來智慧政府的資料治理、資訊安全及業務效率奠定穩固基礎。接下來，本文將分別就各項基礎設施的建置背景、法規適法性分析與未來發展展望進行說明與探討。

貳、政府資料傳輸基礎設施介紹

一、 T-Road 政府資料傳輸平臺

T-Road作為跨機關資料安全傳輸的核心架構(如下圖示意)，具備高度的資料安全性與可追蹤性，依據ISO/IEC 29134（資料保護影響評估標準）、ISO/IEC 27001（資訊安全管理系統標準）與NIST SP 800-122（個資保護指南）等國際標準進行規劃與建置。該平臺不直接儲存實際傳輸資料內容，而是透過機關憑證加密傳輸、數位簽章、時戳驗證及區塊鏈技術，保障傳輸過程的安全性與透明性。此外，政府透過第三方獨立機構進行系統的安全檢測與滲透測試，維護平臺的安全性與合規性。

(一) 應用場景

在 COVID-19 疫情期間，政府為減輕民眾經濟負擔，迅速推動振興三倍券、五倍券、急難紓困金、全民普發現金等多項政策。然而，這些政策牽涉之發放對象、資格標準與所需資料來源多樣，涉及內政、健保、移民署、社福、農保、勞保、財政等眾多機關。由於各部會各自建置發放系統、名單比對作業標準不一，導致資料勾稽流程耗時，甚至出現重複發放、資格爭議及民怨事件，暴露出我國在跨機關資料整合與即時傳輸方面的系統性挑戰。

面對上述困境，T-Road 政府資料傳輸平臺提供了一套安全、可追蹤且合規的跨機關資料交換解決方案。T-Road 採用 GSN VPN[1] 建構資料傳輸加密通道，搭配憑證驗證、數位簽章、時間戳記及完整的日誌保存機制，確保每筆資料流動均符合資通安全管理法、個人資料保護法及相關管理規範的規定。透過此一架構，資料提供機關與使用機關間得以實現點對點、高韌性且具備審計功能的資料傳輸環境。

例如在辦理全民普發現金政策時，須整合戶政基本資料、身分別註記、未成年人監護資料、社福補助資格、農保/勞保/國保狀態等，然多數資料主管機關尚未建置支援 API 傳輸的服務。為此，數位發展部即協助各資料主管機關建置或改寫API，並依 OAS 規範介接 T-Road，使資料可在合乎資安與隱私要求的條件下快速傳送、核對與查調，大幅縮短名單比對時程與減輕行政負荷。

此外，此案例亦帶動了 T-Road 機制的進一步制度化與普及。計畫中即要求資通安全責任等級為 A 級之機關優先導入 T-Road，同時進行內網調整、資源配置與資料項目盤點，並納入資訊安全監控系統（SOC），藉以強化政府整體資料傳輸韌性，提升日後災害、突發事件下之數位應變能力。

T-Road 在本案例中發揮了統合跨機關資料、簡化作業流程、加強資料保護與提升行政效率的關鍵作用，具體展現其作為「資料治理基礎建設」之核心價值。未來，透過持續推廣及法制配套，T-Road 將可支撐更多政策場景下的即時資料應用需求，邁向更全面的數位治理環境。

(二) T-Road DPIA[2] 風險評估參考標準

1. 本案 T-Road DPIA 風險評估方法採用之國際標準說明

T-Road 的風險評估方法建構於多項國際隱私與資訊安全標準之上，分別如下：
(1) APEC 隱私保護原則（共九項原則): 如避免損害原則、告知原則、資料品質原則等，作為隱私保護基本框架。
(2) ISO/IEC 29134：提供隱私衝擊評鑑指南，是本案 DPIA 的核心標準，涵蓋執行時機、範圍、執行者、利害關係人溝通、風險處理與報告等程序。
(3) ISO/IEC 27001：資訊安全管理系統標準，導入資安管理制度建置規範。
(4) ISO/IEC 27701：為 27001 擴充之隱私資訊管理系統，強化隱私風險的控制與管理能力。
(5) NIST SP 800-122：針對個人可識別資訊(PII)的保護原則，補充技術與流程層面的實作依據。

2. 應執行 DPIA 之單位及依法應辦事項

DPIA 並非單一機關責任，應由所有涉入 T-Road 作業流程之單位執行，包含：
(1) T-Road 維運機關：負責管理平台運作與系統開發維運。
(2) 資料中心建置機關與介接機關：需依資通安全責任等級辦理風險分級與控制。
(3) 涉及 個人資料蒐集、處理、利用 的機關應依個資法第 2 條進行適法性評估，涵蓋蒐集、處理與利用三階段。

3. T-Road DPIA 評估時機時機

(1) 系統功能開發階段：上線前先行確認法遵與技術風險。
(2) 系統功能大幅度異動時：如架構變更、新增功能或外包開發。
(3) 介接機關傳輸資料前：須評估資料傳輸適法性、使用目的與風險，避免影響當事人權益。
(4) 定期或不定期進行評估: 每年定期針對介接 T-Road 部分相關安全防護措施,進行資料 保護安全評估或收到外界通報最新資安或個資風險情資後進行評估。

4. 風險發生機率與嚴重性評估方式

(1) T-Road 採用風險評估矩陣進行量化評估，表格如下:
 圖二

(2) 風險發生嚴重性評估方式如下:

- 非常嚴重（Catastrophic）:當資料遭未授權揭露、遭竄改或系統無法運作，並影響到法律遵循性（例如使機關人員需負刑事責任）時，若其後果對機關營運、資料、聲譽或資產造成災難性、不可回復的損害，即屬此級。此等風險通常需高層級決策者即刻介入與全面處理，為最需優先控管的情境。
- 嚴重影響（Major）: 指在相同風險來源發生下，對機關造成顯著且可能擴大的損害，例如業務流程中斷、系統異常或民眾信任受損，雖不致災難，但已對正常運作構成實質干擾。此風險等級需制定具體改善計畫並持續監控進度。
- 有限影響（Limited）: 屬影響程度較低的風險，即便發生非授權揭露或短暫服務異常，其對機關營運或聲譽的影響可控且可恢復。處理上可透過一般性維運機制與例行風險管理予以因應，不必立即大規模資源投入。

(3) 風險發生機率評估方式如下:

- 高機率（幾乎確定會發生）: 指評估者根據過往業務經驗與機關內、外部稽核發現，並結合對現行控管措施之評估，認為該風險事件時常發生或在未來發生的可能性極高。此類風險通常已出現多次徵兆或具備明顯脆弱點，應列為高優先處理項目。
- 中機率（偶爾發生）: 代表該風險事件在過去有發生紀錄，但非經常性或周期性出現，其發生機率屬中等。控管措施可能有部分缺口，需建立定期監控機制並進行改善，以降低風險未來再次發生的可能性。
- 低機率（甚少發生）: 依據過往經驗與稽核紀錄，評估者認為該風險事件從未發生過或僅在極例外情況下可能出現，且現行控管措施嚴謹，發生機率極低。此等風險可納入常規風險監測範圍，不需立即主動處理。

5. 風險處理方式

(1) 風險避免（Avoidance）：取消或調整特定活動以避免風險。
(2) 風險降低（Mitigation）：採取技術、組織、管理性措施來減低風險可能性或影響程度。

(3) 風險降低（Mitigation）：採取技術、組織、管理性措施來減低風險可能性或影響程度。
(4) 風險接受（Acceptance）：對於低風險項目，在評估後選擇接受其存在。

(三) T-Road 風險評估方法說明

1. 個資法適法性評估方法

此節針對 T-Road 平臺與介接機關在資料傳輸、處理過程中是否符合《個人資料保護法》進行檢視，主要依據為 APEC 九大隱私保護原則，對照我國個資法條文（如第6、8、11、19條等）分析其合規性。
重點評估項目包括：
(1) 是否明確定義蒐集與利用目的
(2) 資料利用是否和目的相符
(3) 當事人是否有充足的知情與選擇權
(4) 機關有無取得合法授權依據
(5) 是否提供當事人查詢、更正或異議機制

2. 保有個資重要性評估方法

目的在於辨識資料敏感程度與處理風險，藉以導引風險控制優先順序，有助於釐清高風險資料集，納入重點保護範圍。。評估指標包括:
(1) 資料筆數與成長性（如每日交換數量）
(2) 資料欄位敏感性（如身分證字號、醫療資訊等）
(3) 可識別性（是否能直接或間接識別個人）
(4) 使用情境（是否跨系統、跨單位流通）
(5)潛在損害程度（對機關、民眾、社會信賴的影響）

3. 委外開發安全評估方法

針對 T-Road 系統功能開發若採委外模式，需針對委外廠商及其開發過程進行安全評估，強調在專案管理與委外過程中即導入資安與隱私保障原則。項目包括：
(1) 是否將資訊安全要求納入委外契約中（如資安條款、保密協定）
(2) 人員背景查核與權限控管措施是否落實
(3) 開發期間的系統測試、安全驗收與交付前稽核是否完整
(4) 供應鏈風險管理制度是否到位
(5) 廠商是否具備 ISO 27001 等國際安全認證

4. T-Road 維運機關資通安全管理措施評估方法

此評估針對負責 T-Road 日常維運之主責單位（如政府資料管理中心）所應建立的管理制度與技術機制進行檢視，確保平台核心維運單位具備制度化、常態化的資安防護能力。包括：
(1) 組織架構與資安職責分工明確性
(2) 是否建立資訊安全政策與持續改善機制

(3) 員工資安教育與訓練是否常態化
(4) 系統弱點掃描、日誌紀錄、異常監控是否定期執行
(5) 是否完成 ISO 27001/27701 等資安與隱私管理認證

5. 資料中心設置機關資通安全管理措施評估方法

T-Road 所依託之物理資料中心（如政府雲）是否具備良好資訊安全與營運韌性，確保資料中心在面對災害、人為事故或系統異常時，能迅速恢復服務。包括：
(1) 實體門禁與機房安全控管
(2) 網路備援、供電備援、硬體容錯能力
(3) 備份與災難復原計畫（如定期演練、異地備援）
(4) 系統故障通報與事件回應流程是否完整

6. 介接機關資通安全管理措施評估方法

針對所有與 T-Road 平臺互通的政府機關，評估其在資料交換與處理過程中的安全管理能力，強化整體資料交換鏈中的每一環節，達成一致的資安標準與操作行為。
包括：
(1) 系統開發流程是否具變更管理機制
(2) 存取權限設計與審核流程是否嚴謹
(3) 存取權限設計與審核流程是否嚴謹
(4) 是否具備資安事件通報機制與應變預案
(5) 資料僅於授權範圍內存取與使用

(四) T-Road 風險評估結果整理

1. 整體適法性表現：T-Road 維運機關在功能增修與維運過程中，依據個人資料保護法、資通安全管理法等規範辦理，於評估期間並無違規情形，適法性表現良好。
2. 個人資料保留與最小化原則：
   (1) 為處理介接聯繫所需，T-Road 單一登入模組（SSO）保留機關承辦人員之姓名、公務聯絡資料及憑證卡號。
   (2) 資料已進行亂碼化處理與去連結化，並依最小必要原則保存，具合法性與正當性。
3. 不保留民眾個資與傳輸內容：T-Road 維運機關僅提供傳輸平台服務，不蒐集或處理民眾個資，也不保留傳輸資料內容。
4. 傳輸紀錄保存機制：所有資料透過 GSN VPN 加密通道傳輸，系統保留完整傳輸紀錄以便未來稽核與事後追查。
5. 第三方安全驗證與未來規劃：已取得國際資訊安全標準（如 ISO 27001）驗證，並計畫於 113 年進行隱私保護之外部驗證。
6. 建議措施：建議維運機關建立辨識個資之自動機制，由資料提供機關事先標註是否含個資欄位，以利風險控管。

(五) T-Road 維運機關安全性評估結果

1. 安全管理制度建置完備：依據《個資法》、《資安法》與 ISO 27001/27701 等規範執行開發與維運管理，無違規紀錄。
2. 安控作業與復原機制：定期由廠商彙整安控月報，並執行災害復原演練，確保異常狀況下可於容忍中斷時間內復原。
3. 傳輸規範與稽核作業：訂定「政府資料傳輸平臺管理規範」，並針對介接機關進行定期或不定期稽核，確認其符合規範。

(六) T-Road 委外開發安全評估結果

1. 制度與稽核機制：維運機關通過第三方驗證，開發廠商須符合委外開發相關資安與隱私規範。
2. 法規遵循與要求明確：包含《資安法》第9條、《個資法》施行細則第8與第12條，以及資訊安全制度要求（如供應鏈管理、測試、驗收）。
3. 無即時高風險項目：無即時高風險項目：經檢視無重大違規或需立即處理之風險事項。

(七) T-Road 運作功能安全管理措施評估結果

1. 介接機關申請與稽核程序：須提出介接申請，依《資安法》進行資訊安全管理，並配合 T-Road 維運機關定期稽核。
2. 個資保護與機關責任：包括公示義務、告知義務、個資事件通報、個資當事人權利保障等措施。
3. 資料傳輸前法遵確認：傳輸前須確認資料是否含有個資，若含個資，應於目的結束後刪除，或依法保留。
4. 法源依據：依據《個資法》第17條及施行細則第23條，公務機關對於個人資料檔案的公開與異動應於法定期限內完成。
5. 管理規範落實：T-Road 維運機關依據「政府資料傳輸平臺管理規範」審查與核可介接機關作業，並對違規單位保有准駁與追責權限。

(八) T-Road 介接機關適法性評估結果

1. 管理功能完備：具備中央控管、設定管理、運作監控、環境監控、時間戳記等核心功能，並記錄各項操作與環境狀態。
2. 傳輸與加密技術：資料透過 GSN VPN 加密通道傳輸，並以 RSA2048 和 AES256 加密，保證資料完整性與機密性。
3. API 與版本控管：導入 Open API 架構與監控機制，可即時掌握介接狀態與異常情形。
4. 文件化與開發流程安全：安全設計、測試、維運及版本控管全程留存紀錄並有完整防護流程。
5. 持續稽核與教育訓練：委外廠商須定期接受資安教育，並持續強化變更與防護措施管理。合規驗證證據齊全：
   (1) 已完成第三方資訊安全驗證，預計執行隱私保護標準驗證。
   (2) 若系統異常，已建立依法令要求之通報與處理機制。

(九) 持續關注議題

1. 本部管理規範已建立
   (1) 數位發展部已訂定「政府資料傳輸平臺管理規範」，明定介接機關於使用 T-Road 傳輸資料時，應落實資訊安全與隱私保護措施。
   (2) 該規範作為目前 T-Road 資料傳輸機制的實施依據，確保維運端與介接端皆依循法規辦理。
2. 重大個資外洩事件引發社會關注
   (1) 109年間個資外洩事件：有境外網站於暗網拍賣我國民眾個資，聲稱資料來自內政部戶政資料庫，規模達 2 千萬筆，引發社會與媒體高度關注。
   (2) 內政部戶政司現況：其為 T-Road 介接機關，未來將透過 T-Road 傳輸戶政資料，故資訊安全風險與責任更形重大。
   (3) 結論建議：T-Road 維運機關除應強化平台安全外，介接機關亦須落實個資保護責任，共同保障民眾權益。
3. 憲法判決與制度改革趨勢
   (1) 憲判第13號（111年）：明確指出國家對個人資料保護的憲法責任，並強調對公務機關應有更高監督標準。
   (2) 行政院回應作為：於 112 年 12 月成立「個人資料保護委員會籌備處」，並研擬《個資法》修正草案。
   (3) 修法重點包括：

- 對公務機關的監督與責任落實。
- 建立個資侵害事件通報義務。
- 訂定個資安全維護之最低標準。
  (4) 法定時程：個資保護委員會將於 113年8月前正式成立，負責對政府部門進行監督、稽核與受理陳情。
  (5) 後續關注重點與趨勢重點發展：
- 個人資料當事人權利行使機制與程序設計。
- 個人資料辨識與標註機制的制度化與自動化。
- 公務機關責任化與查核制度的具體強化。

二、 中文交換碼全字庫（CNS11643）

(一) 全字庫簡介

「國家中文資訊標準交換碼」編訂起始於民國69年，經歷多次編碼，於民國75年獲中央標準局審定頒布為國家標準，編號「CNS11643」，並於民國81年更名為「中文標準交換碼 (Chinese Standard Interchange Code)」，即今日之「CNS11643 國家標準中文交換碼」。至民國114年，全字庫已更新至5.0版，並由數位數位發展部承續辦理。全字庫建置目的在於解決個人電腦中文字數不足、跨平臺與跨系統間中文資訊傳輸的亂碼、自造字無法交換及各機關內部同字不同碼、網頁上罕用字顯示等問題，並協助

機關、企業、團體整合及管理個人電腦上的中文字集。該字庫功能豐富，包括中文字碼的多種查詢方式（如注音、倉頡、BIG-5碼、Unicode碼）、字型即時下載、中文碼轉換、自造字管理與共享機制。截至5.0版全字庫，CNS11643已收錄逾108,000個字元，涵蓋漢字、自造字、符號等多種類型，漢字本體更超過96,000字。

CNS11643 採用多字面設計，每一個字面為 94×94 編碼空間，可容納最多8,836個字。各字面依照用途與字頻進行分類，目前第1至第11字面為標準區，第12至第15字面為使用者加字區，第16字面為私人造字區，第17、19、24字面作為戶政、教育部異體字、醫藥與化學符號等用途。其餘字面保留供未來使用。

 圖三

(二) CNS11643使用狀況

CNS11643 不僅是台灣官方制訂的中文資訊標準，也已廣泛應用於政府作業與民間系統，成為資訊交換的重要依據。其實際應用可分為下列幾個層面：

1. 政府資訊處理標準的依據
   CNS11643已被正式納入「政府機關資訊處理共通規範」，作為各類中文作業系統與資料交換的統一參考架構。此一標準亦被國內外多數資訊廠商視為系統設計與相容處理的重要準則。
2. 公文電子交換之標準內碼
   為確保政府機關間電子公文交換的標準化與互通性，凡經由「交換中心」（設於交通部資訊中心）傳遞之公文，皆需事先轉換為CNS11643編碼。
3. 大型系統內部碼應用案例
   目前全國戶役政系統即採CNS11643作為其內部資料結構基礎。該系統運行於UNIX架構下之MITUX平台，雖採用EUC編碼，其結構與字集均直接承襲CNS11643，實為 CNS11643應用於內碼轉換的典型案例。
4. BIG-5E字集之編碼基礎
   行政院研考會推動的BIG-5E（Big5 擴充字集）即以CNS11643為藍本進行設計。此字集涵蓋CNS第1字面中的3個部首字、第3字面之3,891字，以及第4字面中的59個常用字。
5. 跨系統轉碼支援與工具整合
   為促進資訊流通，目前多數資訊廠商已開發對應工具與轉碼演算法，可實現CNS11643與其他主流內碼（如 Big5、Unicode）間之相互轉換，並支援開發者進行資料交換與應用整合。
6. 與國際標準（ISO 10646 / Unicode）之對應性
   國際標準如ISO 10646及Unicode系統，目前已納入逾2.6萬個漢字，其中約2.3萬字來自CNS11643第1至第7字面與第15字面，顯示 CNS11643 在國際編碼發展中扮演基礎角色。此高度重疊性不僅有助我國標準與國際接軌，也提升國內資訊產業的國際競爭力，並為未來中文編碼轉換與整合提供良好基礎。

(三) CNS11643新增字申請

各申請單位提出新增字申請，並提供相關屬性及事證資料。所提之文字屬性包括字形、注音、倉頡、部首、總筆畫數、筆順、部件、來源出處及字義，以供參考登錄，其中以字形、注音、部首、總筆畫數及來源出處為必要具備之屬性。

1. 主管機關進行初核，比對該用字是否新增。若認為該新增，則函送數位發展部複核。
2. 若數位發展部複核新增，則進行新增字作業及編訂暫編交換碼。此後再視需要召開電腦中文環境建置工作小組會議，決議是否送交納編標準交換碼。
3. 若決議納編標準交換碼，則由經濟部標準檢驗局審核納編中文標準交換碼，再由數位發展部依審核結果調整全字庫並公布。

(四) CNS11643與其他中文編碼標準之比較

 圖四

三、開放文件格式（Open Document Format, ODF）

(一) ODF簡介

為保障民眾在文書處理軟體上的自主選擇權，促進政府機關間、公私部門間以及政府與民眾之間的文件流通，並確保電子檔案的長期可用性與資訊自主性，實現數位治理中的「軟體平權」原則，行政院自104 年起，推動相容性高、適用於各種作業系統及有利於資料長久保存之開放文件格式CNS15251（對應ISO/IEC26300國際標準）為政府文件標準格式。

歷經三期推動（104–112年），ODF 格式逐步取得政府部門的廣泛應用成果。為強化品質管理與推廣實效，數位發展部於 113 年啟動第四期「政府文件標準格式(ODFCNS15251)實施計畫（113-116年)」，更進一步將ODF格式擴展至企業及政府軟體應用，建立ODF文件檢測工具，以達永續流通之目標。

(二) ODF格式特性與技術優勢

1. 跨平台相容性高：ODF 文件可於多種作業系統（如 Windows、macOS、Linux 等）開啟與編輯，無須依賴單一軟體供應商，提升使用彈性與文件交換效率。
2. 格式開放透明：ODF 採用 XML 為基礎，具自我描述能力，有助於格式的解析與開發應用，避免格式封閉所造成的資訊孤島。
3. 長期儲存穩定性強：由於其標準化與開放性，ODF 適合用於需要長期保存與跨年代交換的文件資料，例如政府公文、教育資源與學術報告等。
4. 軟體自主選擇保障：推廣 ODF 可避免政府機關與民眾在處理文件時受限於特定私有格式，確保數位主權與資訊自主權。

(三) 政府推動與應用現況

1. 第一、二期計畫（104-109年）：工具開發
   (1) ODF 文件應用工具（106年）：以開源軟體為核心開發本工具，結合中文標點、罕用字等在地化需求，協助民眾於個人電腦製作、編修ODF檔案。
   (2) ODF API 工具（107年）：供機關之系統開發人員自動化產製ODF格式文件或報表，以降低轉檔成本。
   (3) ODF 雲端編輯工具（108年）：支援行動裝置與共筆功能，使用者可透過行動裝置進行線上編輯ODF文件。
2. 第三期計畫（110-112年）：強化應用
   (1) 資安強化與工具整併（110年）：整合ODF API與雲端編輯工具，升級核心版本並導入資安防護技術，提升文件格式相容性與作業安全性。
   (2) 異地辦公雲端加值服務（111年）：因應疫情期間異地辦公需求，建置ODF雲端編輯工具整合問卷模組，支援機關線上調查與遠距作業需求。
   (3) 平台優化與學習資源充實（112年）：優化問答集與機關統計指標網站介面，取得AA無障礙標章，並新增教學影片與線上學習資源，提升使用體驗。
3. 使用成效（截至112年12月）
   (1) 中央機關電子公文ODF附件使用率逾90%。
   (2) 直轄市與縣市政府中已有10個逾70%。
   (3) 政府網站提供ODF格式下載比率與資訊系統支援ODF格式比率皆逾 90% 。
   (4) 於112年9月及10月參與 LibreOffice 國際社群，分享我國推動成果與應用經驗（LibreOffice Conference 2023 及 LOUCA23）。
4. 第四期計畫（113–116年）
   (1) 計畫架構與推動策略
   第四期計畫推動策略著重於提升軟體平權流通環境、維護數位主權關鍵基礎韌性，並聚焦下列五大主軸：

- 人才培育：擴增ODF教學資源，培育政府ODF應用人才。
- 關鍵基礎：維護政府關鍵基礎文書核心軟體能量，強化推廣人員軟體平權意識。
- 標準建立：發展政府ODF文件格式驗證機制，持續ODF技術國際標準交流。
- 產業推廣：提升ODF公私領域服務運作，持續推動運用公務ODF文件。
- 軟體精進：提升ODF應用工具友善使用介面，建立推動ODF經驗與示範。

(2) 推動機制與分工
本計畫由數位發展部統籌規劃，定期邀集相關機關召開跨機關推動會議，負責整體規劃推動、協調各機關推動事宜及追蹤本計畫之執行成效。同時制訂三項分工原則，由數位發展部主責總體發展推動、行政院所屬機關（如各部會、國營事業、各縣市政府、各直轄市政府）配合實施各機關共同事項，並由權責有關機關（如行政院人事行政總處、公共工程委員會、教育部）辦理特定推動工作。

(3) 經費來源
本計畫所需經費，由各機關於行政院核定其各年度中程歲出概算額度內，優先編列相關預算支應。

(4) 預期效益與相關目標

- 每年培訓一定比例政府人員參與ODF教育訓練課程，以健全政府機關ODF人才培育生態系，增加政府ODF應用人才能量。113年目標為75%人員，至116年達90%。
- 各機關提升招標文件ODF格式使用率，113年目標為72%，116年目標為80%。
- 強化我國數位基礎建設自主能力，增加政府機關資源配置彈性。
- 研提ODF格式檢測能量評估與測試，確保未來檢測能量暨檢測程序之合宜性，及完備推動ODF流通環境之發展。
- 驅動ODF相關應用及服務供需常態化，落實軟體平權。

四、短網址服務（Short Urls）

(一) 短網址服務簡介

政府短網址服務，能讓政府機關將冗長、不易記憶的長網址轉換為精簡的短網址，有利於政府機關傳播公共資訊。該服務生成的短網址皆以 `https://gov.tw/XXX` 為開頭，讓民眾更容易識別政府網站，減少誤連詐騙或釣魚網站的風險，公眾亦可於該平台反查短網址對應之原始連結，增加透明度。該服務更明確限制僅限gov.tw域名與gov.tw電子郵件使用，防堵民間短網址被不法利用偽造政府內容。

(二) 短網址服務使用概況

該服務自111年10月推出起，便獲政府機關廣泛採用，於推出一週內（10/14–10/20）即註冊約 100 條短網址，累計轉址約 17萬次 。於疫情期間，該服務更成為政府推播疫情資訊、政策宣導的常態工具，中央流行疫情指揮中心也一致使用此服務，替代民間短網址工具 。目前該服務平台已逐步推廣至所有政府機關 ，包括新北市警察局、婦幼隊等地方單位均開始使用。至2025年6月為止，該服務平台已累積產生逾3.6萬條短網址，累積轉址約9350萬次。

五、資安A級機關導入零信任架構（Zero Trust Architecture，ZTA）

(一) ZTA簡介

零信任架構（ZTA）的核心理念在於「永不信任，持續驗證」，透過不間斷的使用者與設備驗證流程，建立高度資安防護。根據第六期「國家資通安全發展方案（110–113年）」推動策略，ZTA已被明確列為資安強化重點，並由數位發展部主責推動，優先針對資通安全責任等級為 A 級之政府機關進行導入與輔導。

(二) ZTA技術核心

ZTA的核心理念在於「永不信任，持續驗證」，透過不間斷的使用者與設備驗證流程，建立高度資安防護。ZTA架構依據NIST SP 800-207標準建構，導入以下五項核心功能：

1. 身分鑑別：採多因素驗證（如 FIDO2），以無密碼雙因子方式達成身分鑑別。
2. 設備鑑別：– 透過TPM（Trusted Platform Module，提供裝置可信驗證基礎）或Agent（負責回報裝置狀態與環境資訊）產生金鑰與憑證，完成設備註冊與鑑別；持續監控設備健康狀態，判斷設備是否可信。
3. 信任推斷：根據使用者角色、裝置安全狀況、IP、地點等動態條件，計算信任分數，決定存取或限制權限。
4. 存取閘道：負責網路導向與連線，不論存取來自內部或外部網路，皆必須且唯一經由存取閘道。其為唯一公開存取之組件，存取全程必須隱藏內部網路路徑(如利用反向代理技術)。
5. 決策引擎：決策引擎負責接收存取請求、決定允許與否及授予存取憑據，組件包含：

- 決策控制器：負責控制存取決策之流程，包含設定存取允許條件、接收存取請求、驅動3大核心機制及授予鑑別聲明。
- 3大核心機制：由身分鑑別、設備鑑別及信任推斷進行驗證與評估，並將結果回饋給決策控制器。
- 鑑別聲明伺服器：針對獲得允許之存取，發行鑑別聲明，做為存取RP（提供應用服務的系統，其發起登入需求，驗證結果會決定是否給予存取）之憑據。
   圖五

(三) 導入進程與成果

依據111年核定之資安A級機關清單，於113年底完成共47個資安A級機關的ZTA輔導，並全數成功導入「身分鑑別」機制，以協助機關加速逐步建立零信任網路資安防護環境。

1. 導入方式與流程
   (1) 政策指引制定：《政府機關導入零信任架構參考指引 V1》提供具體技術操作建議。
   (2) 驗證程序推動：採「檢核表驗證 → 功能展示驗證 → 測試部署驗證」三階段。
   (3) 協作模式：與資安廠商合作，要求產品須開放API並與現有AD（Active Directory，常用以管理身份驗證與授權）、資通系統相容。
2. 技術驗證成果
   已建置：
   (1) FIDO2 身分鑑別伺服器與前端系統
   (2) TPM 鑑別伺服器與代理程式
   (3) 設備健康管理伺服器與代理程式

(四) ZTA未來發展方向

1. 強化設備鑑別與行為監控模組。

2. 推動零信任認證產品納入政府採購契約。
3. 擴及 B 級與 C 級機關、企業、遠距辦公環境。
4. 鼓勵國內資安廠商開發零信任解決方案，強化在地資安產業鏈。

1. **GSN VPN（Government Service Network Virtual Private Network）**為政府建置之封閉式虛擬私人網路，專供各機關間進行敏感或具政策性資料之安全傳輸使用。透過加密通道與身份驗證機制，GSN VPN 能有效防止資料在傳輸過程中遭截取或竄改，並符合《資通安全管理法》相關規範，是政府跨機關系統如 T-Road 進行資料交換時所依賴的核心傳輸基礎設施。政府專屬的內網。 ↩
2. **DPIA(Data Protection Impact Assessments)**,資料保護衝擊評估: 為考量個人資料之生命周期執行其隱私相關的評估,包含辨識、 分析可能產生資料保護風險,著重於保護隱私資料的準確性、保密性、完整性、實際安全性。 ↩