行政院 111 年 10 月 5 日院臺科字第 1110186745 號函核定

整體政府資通安全防禦技術暨系統韌性強化計畫

(核定本)

數位發展部

計畫期程：112 年至 115 年

中華民國 111 年 10 月

目次

圖目次

表目次

壹、計畫緣起

一、依據

近年來各類資通訊科技不斷地創新發展，舉凡智慧型手機、5G、雲端運算、區塊鏈、巨量資料、物聯網、人工智慧等，逐漸改變我們的生活型態，同時也大幅改變了公共服務的型態、以及政府與民眾的溝通模式。我國在推動「智慧政府」之政策下，也以新興資通科技和網際網路做為推力，極力改善公共服務的提供模式以回應整體社會的發展與民眾的期待。

隨著政府數位服務愈多元創新，其所帶來的資通訊威脅防禦與運作持續性更顯重要。各機關為因應業務創新發展而開發之系統服務，常因為無法與既有系統完美融合造成運作異常，或者缺乏良好資訊系統安全架構設計，遭資安攻擊導致寶貴資料遺失或使用者個資外洩，也常因為行銷或突發事件致大量使用者灌入，造成系統嚴重失靈，影響民眾權益也可能波及跨機關相關業務執行，更造成政府服務可信賴度及品質的嚴重威脅。

有鑑於此，如何確保提升政府資通安全防禦技術，並打造系統之安全性與韌性，成為現階段不容忽視且極需建構的機制，本計畫將扣合行政院自 2016 年起推動之「數位國家·創新經濟發展(DIGI^{+})方案」(2020 年轉型為「智慧國家方案」)，以促進政府數位系統安全與整備韌性環境為核心價值，辦理政府資訊系統防禦技術研發、數位韌性精進等業務，以協助政府機關打造高效、安全、穩定運作之政府數位服務，確保民眾數位生活福祉、驅動數位經濟創新及促進智慧國家相關服務穩定發展。

二、未來環境預測

根據世界經濟論壇(World Economic Forum, WEF)「2022 年全球風險報告」統計，新冠肺炎疫情對全球經濟、生活及技術應用等不同面向造成極大的影響，尤其高度數位化國家，面對疫情、極端氣候、能源危機等不確定災難，為政府數位服務持續運作增添不可控之威脅，技術治理

失效、數位權利集中、IT 基礎架構失效及資通安全等風險，將為國家、社會及經濟造成嚴重衝擊。

臺灣資通訊發展普及，個人上網率已達 86.6%，超過 68.2%的民眾幾乎天天長時間上網，也使得我國民眾比以往更依賴政府的數位服務。政府因應民需而發展出複雜多元的各種便民服務系統包括戶政系統、地政系統、財稅系統、遠距教育環境、醫療系統等各項政府便民服務，乃至為了政府內部運作便利所使用的電子公文交換、差勤系統、主計出納系統等，在高度的資訊化環境下，資通訊系統的安全與可用性，成為各界關注的議題。

2020 年初全球爆發新冠疫情、重創全球社會與經濟活動之際，臺灣因防疫得當，將影響降到最低，成為全球防疫典範。在歷經疫情後，世界各國也開始思考遭受疫情或其他災難之因應措施，居家辦公、線上學習、遠距醫療等資通訊應用成為生活日常選項，加上物聯網、人工智慧、5G 雲端化、區塊鏈等新興數位科技應用蓬勃發展，影響資訊系統運作範圍從傳統的 Client-Server 框架，擴大至民間設備、雲端運算、行動資訊載具，或是無所不在的 IoT 物聯網設備，造成相關資料登錄、傳輸、處理等環境更為複雜多變，也使得各級政府資通訊服務之設計架構與資通安全維護面對重大挑戰。同時，2020 年我國數位發展調查更發現有 64.9%的上網人口未採取任何資安防護作為或已經久未更新其防護系統，各種主客觀環境因素造成資通安全與個資洩漏的威脅日益升高，如何提供安全又可靠的政府服務，已成為必要且影響國安的議題，這也是總統多次要求強化整體資安，並將資安視為國安之主因。

數位系統安全穩定可用是智慧國家之基礎，面對數位科技應用之普及與多樣性，政府為擔負起社會責任，必須建立完備政府機關資訊系統韌性運作之能力，力求資訊系統架構安全穩定且可彈性運作，透過服務體驗滿足民眾需求並達資通安全可控可防等目標，在後疫情時代，透過數位再造，建構並強化新一代政府機關資訊系統安全與韌性，以維持整體社會正常運作及經濟穩定發展。

三、問題評析

完善的數位韌性環境並非一蹴可及，綜觀我國近年因資訊系統運作異常而引發民眾關切事件，如某全國性業務系統遭駭客攻擊造成業務停擺、某系統資料備份異常導致資料遺失、某預訂系統短時大量連線而中斷服務等，即可窺見政府資訊系統之運作安全強度與韌性尚待提升，而這些案例並非特殊事件，從這些機關的事前運作持續性準備以及系統架構穩固性來看，與很多機關並無二致，可見得大多數機關可能也有著同樣的系統失效風險，因此必須以通案性手段來解決，而非個案性的事後補強。

此外，近年重大社會事件，如八里遊樂園粉塵爆炸事件、COVID-19 防疫與紓困業務，均須緊急建構臨時性資訊系統，以整合各部會投注之資源、管理各項因應措施，然各機關多仍以業務職掌為界，缺乏整合各項既有資訊系統資料、流程、介面之能力，因而影響政府施政效率。而在目前各種業務都需要資訊系統，緊急事件發生時更需快速建構數位服務介面的社會氛圍下，更需統籌建構結構化且具資通訊安全強度的資訊系統機制，平時整備相關數位工具、共用模組、資通安全防禦技術，在緊急時刻可以協同主責機關建置臨時性系統或抵禦外界攻擊。計畫除建立系統架構外，系統模組細部設計將考量機密性、完整性、可用性的資安整備，將納入防駭與病毒防禦等機制，阻擋外來入侵的同時，也將建立內部人員操作、外部跨機關連線存取、網路拓樸合理性等確保系統運作持續性的重要因素。本計畫所發展技術與模組，所有權屬我國政府，故可提供予各級政府機關共用，以撙節整體系統改造成本，亦可用於訓練培力各級政府數位與資安人才技能，進一步強化機關系統效能與增進服務介面親和性。

歸納強化政府數位安全韌性的重要課題，本計畫提出下圖 3 角型架構，此架構的 3 個元素(資安整備、服務韌性架構設計、數位可用性巡守救援)，期可透過計畫推動強化整體政府資通安全防禦技術，並增進政府數位系統韌性，提升各級政府資通系統安全性與可靠度，並進一步提供

更契合民眾需求且穩定可靠的智慧政府服務。

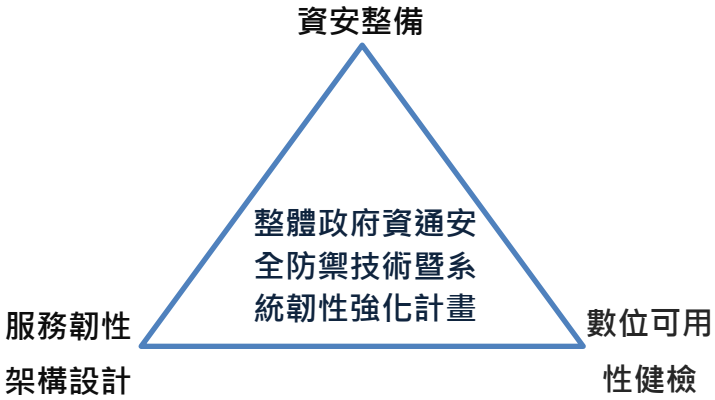

圖1　政府數位安全韌性架構

四、社會參與及政策溝通

本計畫屬政府資訊系統數位轉型與數位服務安全韌性運作推展工作，為確保政府數位化為民服務永續發展與服務品質滿足民眾需求，數位發展部資通安全署遵循智慧國家發展方案之上位政策，每年度辦理智慧國家數位治理分組會議、行政院國家資通安全會報委員會議及全國資訊主管聯席會，召集行政院所屬各部會之資訊長、資安長與資訊單位主管參與，共商政府數位發展及資通安全相關施政方針、重點政策、年度重要工作，並協調跨機關合作事項。本計畫規劃執行之推動策略、重點工作，已透過上開行政院層級之跨機關協調會議溝通，將協助政府機關加速建構完善之數位服務發展環境、打造安全可靠並具運作韌性的政府資訊系統，提供民眾安全之數位服務。

貳、計畫目標

一、目標說明

本計畫依據打造堅韌、安全、可信賴的智慧國家政策方向，推動政府資訊系統數位安全韌性相關措施，確保政府重大民生關鍵系統維持高效、安全與彈性運作，支持政府機關善用數位科技解決重大社會事件及

政府施政措施運用數位科技。

本計畫擬定4項推動策略，包含「建構政府安全與韌性環境服務機制並提供各部會服務」、「充實政府共享數位資源與資安技術」、「厚植政府資訊系統運作韌性及資安應用」及「強化政府資訊系統緊急事件應變能量」，推動政府資訊系統架構設計與流程改造、資訊系統服務介面與使用體驗優化及資通安全科技研發、應用與推廣工作，透過科技、資料與資安拓展政府數位化應用與服務面向，達到民眾安心使用數位服務、確保政府服務持續運作及保護政府及民間數位資產之目標。

二、達成目標之限制

我國推動電子化政府迄今已有20餘年，已在各項涉及民生之業務領域累積許多成功案例，如戶政、地政、稅務、公司登記、交通監理及勞保健保等，各項資訊系統均以支持機關業務運作為基礎，在既有業務職掌、法規命令、作業程序範圍內提供服務，成功運用網際網路提供民眾線上、電子化方式申辦業務。

然而政府機關各項民生關鍵系統已運作許久，面對新興科技應用趨勢、跨機關業務流程整合、資料跨域應用、新型態網路資安攻擊等挑戰總是力有未逮。但是，各類數位科技應用已深入民眾各個生活面向，民眾對政府數位服務之要求已經跳脫「有就好」，更要求快、穩、好用、安全，在政府資源、人力無法充裕挹注的限制下，政府機關僅能維持資訊系統最基本的維運作業，並且以既有系統擴建的方式，建置及運作創新服務。如此，各類系統層層附加功能的狀況，導致新增功能存在水土不服的情況，不但增加功能失效的風險，更有可能影響既有關鍵系統的效能，甚至大幅增加整體系統崩壞之風險。

有鑑於我國政府機關數位轉型能力尚待培養、資訊系統數位韌性尚須強化、數位服務安全仍須持續精進，實需專業人員長期深耕政府資訊系統永續、韌性發展之數位技術研發，為政府機關資訊技術解決方案，培養政府機關數位轉型與資訊系統韌性運作能力，進而帶動數位社會、

數位經濟、數位國民素養，共同創造安全可信賴的智慧國家。

三、績效指標、衡量標準及目標值

本計畫績效指標、衡量標準及目標值請參閱第陸章預期效果及影響。

參、現行相關政策及方案之檢討

一、現行概述

推動智慧國家乃我國政府資通訊發展重要之里程碑，自 2016 年起，行政院推動「數位國家·創新經濟推動方案」，2020 年轉型升級為「智慧國家方案」，強化政府數位基礎建設與提升數位為民服務品質，一直是行政院重點工作。智慧國家方案由行政院直接指揮與督導各相關機關辦理，有關政府數位發展相關工作，則由行政院授權國家發展委員會規劃與推動，各項相關推動工作未來將移撥數位發展部持續辦理。

有鑑於政府機關推展數位化政策，積極嘗試運用新型態數位科技提供創新，尚未考量資訊系統面對天災、人禍等不可抗力因素導致系統停止運作，衝擊國家、社會、經濟持續發展而衍生無法彌補之國家損失。本計畫規劃建立「政府安全與韌性環境服務」機制，招募具備資通訊專業技能人才，專注於強化政府資訊系統運作效能、提升資安防護能力、服務設計與共用模組建立，以精進政府數位韌性以及民眾使用數位服務體驗。

二、服務績效

國家發展委員會自 2021 年辦理「服務型智慧政府 2.0 推動計畫」，以民眾需求為出發點，強調以民生需求為依歸，善用科技打造「智慧政府服務」，加強資通安全、個人資料隱私保護及人才培育，聚焦「精進跨機服務」、「加速開放資料釋出」及「加強循證式決策」，深化智慧政府各項作為，強化數位治理效能，打造精準可信賴的智慧政府，迄今

獲得階段性成果，包括 Open Data 釋出多項高價值應用資料，如實價登錄、水庫水情、即時用電；MyData 擴大至私領域應用，如金融證券、保險期貨運用；跨機關資料傳輸服務介接逾 50 項資料，完成雲端資料中心 9 座，共整併 212 座機房等。

在資通安全方面，自 2001 年 3 月成立行政院國家資通安全會報技術服務中心(以下簡稱技服中心)以來，配合我國資安發展階段，建立各項重要資通安全機制，如成立國家電腦事件中心(TWNCERT)、國家資安監控中心(N-SOC)與國家資安資訊分享與分析中心(N-ISAC)等，現今每月協助政府機關檢測 5,000 多萬封電子郵件，阻擋各類型社交工程郵件攻擊；建構政府機關端與網路端多層次資安防護機制與聯防機制，協助主管機關掌握國家整體資安威脅情勢；提供各機關資安事件技術諮詢服務，即時進行事件應變處置，分析事件發生根因，掌握駭客攻擊手法；建立自動化資安情資分享平臺，強化資安聯防能量，並參與國際合作，建立跨國合作能量，詳見圖 2 與圖 3。

資料來源：技服中心提供

圖2　行政院國家資通安全會報技術服務中心核心任務

資料來源：技服中心提供

圖3　行政院國家資通安全會報技術服務中心發展歷程

三、現況檢討

目前政府資訊系統係由各業務機關就業務職掌範圍，規劃數位化作業程序，支援業務推動工作，並創造數位管道提供民眾與政府機關接觸。雖然各機關本於職掌推動數位化發展，可以符合實際業務需求，惟仍需要再進一步提升我國整體數位發展服務品質，說明如下：

(一) 受限資訊資源，機關缺乏快速建置能量

機關建置系統均須於前一年提報計畫，針對臨時性緊急需求，往往無法有充分資源挹注。是以，須有效探詢、建置、並整備共用性模組元件，且建立跨速有效之服務設計方法，以應機關臨時性緊急需求。

(二) 受限計畫期程，資訊系統缺乏長期發展規劃彈性

每年計畫工作內容皆須重新提交計畫申請，簽約時間不穩定，容易造成計畫工作需縮短執行期程，且工作內容受限合約缺乏彈性，無

法跨年度規劃各項工作。是以，須長期協助機關做自身系統健檢，及早期發現與解決問題；並且深耕資安技術研究與技術應用。

(三) 各級機關系統快速發展，惟礙於各系統發展周期不一，使整合與防護不易，亟待強化各級機關發展安全資訊系統作為

依資通安全責任等級分級辦法規定，針對自行或委外開發之資通系統應完成分級，並完成7個構面對應等級之控制措施，實務上，各資通系統技術架構不一，所涉檢核項目亦須搭配管理作業辦理，控制措施之作業情形不易確認。是以，須持續協助機關強化自行檢核確認防護基準符規性之能力，亦須滾動調修各防護基準作業，以應多元之資安風險。

(四) 因應萬物聯網環境變化，需增大資安意識推動廣度與深度，串聯各界進行資安聯防

以往囿於計畫經費、人力之限制，資安意識培訓較偏重於公務機關，惟在網網相連與萬物聯網的環境下，資安業務轉向各界聯防，資安意識推動面相應加寬變廣，偕同公私機關、產官學共同擴大資安推廣力道，從資安意識、資安案例宣導與資安參考指引，擴增觸及各個面向，提升全體資安意識，並強化各層面之資安技術管理要求。

(五) 受限組織性質，缺乏我國政府自有技術能力

現行機關之資安人力與能力有限，多數資安服務係採委外辦理，或透過協助方式委託技術服務中心提供資安服務，考量現行技服中心成員皆來自於資訊工業策進會，以往提供機關服務時，機關往往有信賴度疑慮，也不利累積我國政府自有資通安全技術能力。是以，未來將成立行政法人提供專業技術服務，除可有效累積研發我國政府資通安全技術能力外，更有助於偕同各級政府，共同強化機關之數位安全防禦，並增加數位系統快速復原之數位韌性強度。

肆、執行策略及方法

本計畫依「智慧國家方案」與「第六期國家資通安全發展方案」之戰略方針，同時配合「服務型智慧政府 2.0 推動計畫」及「資安旗艦計畫」之推動目標，研擬本計畫 4 大發展策略，包含「建構政府安全與韌性環境服務機制並提供各部會服務」、「充實政府共享數位資源與資安技術」、「厚植政府資訊系統運作韌性及資安應用」及「強化政府資訊系統緊急事件應變能量」，藉以提升政府機關資訊系統持續運作能力，精進資訊系統服務品質，增強資通安全防護量能，協助政府機關善用數位力量輔助解決社會重大事件及政府施政措施。

一、規劃構想

政府數位服務愈多元創新，其所帶來的運作持續性風險愈高，各機關勇於突破現有系統框架所建置之系統及服務，有時會因為無法與既有系統完美融合，造成運作上若有大量使用者灌入或某些軟硬體模組失效等突發事件發生時，系統往往會嚴重失靈，而使得長期極重度依賴這些系統的民眾或跨機關業務同仁，受到嚴重的影響。

有鑑於此，為確保整體政府機關系統之數位韌性，本計畫規劃將建立「政府安全與韌性環境服務」機制，招募具備數位服務設計、資訊系統架構分析、系統運作效能檢測及解決系統運作弱點之技術專家，平時定期巡迴健檢政府重大資訊系統運作情形，強化系統運作韌性；緊急時刻協助機關處置資安或系統異常事件，協助機關快速回復系統正常運作；並可協助行政院各部會依施政措施與需求，快速組建任務型資訊系統，以支援政府遂行業務。

二、分期(年)執行策略

表1　計畫分期(年)執行策略

<table>
<tr><th rowspan="2">推動策略</th><th rowspan="2">工作項目</th><th colspan="4">分期(年)執行策略</th></tr>
<tr><th>112</th><th>113</th><th>114</th><th>115</th></tr>
<tr><td>建構政府安全與韌性環境服務機制並提供各部會服務</td><td>政府安全與韌性環境服務</td><td>招募或委託技術人員約 33 人至 47 人，專職辦理政府安全與韌性環境服務任務與工作內容。</td><td colspan="3">較 112 年增加招募技術人員約至少 13 人，專職辦理政府安全與韌性環境服務任務與工作內容。</td></tr>
<tr><td rowspan="7">充實政府共享數位資源與資安技術</td><td>建構軟體物料清單</td><td colspan="4">每年整備(新增或更新)30 項軟體模組物件。</td></tr>
<tr><td>資訊專案文件與開源碼詮釋資料中文化</td><td colspan="4">每年完成資訊專案文件與開源碼詮釋資料中文化 5 案。</td></tr>
<tr><td>擴充政府設計系統元件</td><td colspan="4">每年調校(新增與編修)政府系統設計元件 10 案。</td></tr>
<tr><td>電腦組態基準研究</td><td>發展「作業系統」與「應用程式」類別電腦組態基準。</td><td>發展「應用程式」與「網通設備」類別電腦組態基準。</td><td>發展「網通設備」與「瀏覽器」類別電腦組態基準。</td><td>發展「瀏覽器」與「作業系統」類別電腦組態基準。</td></tr>
<tr><td>資通安全弱點研析</td><td colspan="4">關注重大弱點與發布警訊，每年完成至少 2 個重大弱點研析與實作驗證</td></tr>
<tr><td>攻擊研析與偵測防護</td><td colspan="4">透過駭侵樣本，萃取威脅情資特徵，製作並部署偵測規則，每年完成產出 2 項偵測規則。</td></tr>
<tr><td>資安參考指引發展</td><td colspan="4">因應國際資安威脅趨勢及新興科技發展，並參照資安規範整體發展藍圖增修參考指引</td></tr>
<tr><td>厚植政府資訊系統運作韌性</td><td>盤點數位韌性巡航服務對象及維護</td><td>盤點民生關鍵資訊系統背景資料 13 項</td><td colspan="3">每年盤點民生關鍵資訊系統背景資料 20 項</td></tr>
</table>

推動策略	工作項目	分期(年)執行策略			
		112	113	114	115
及資安應用	系統背景資訊				
	培養數位韌性領航員	完成數位韌性領航員訓練課程至少 6 名	每年完成數位韌性領航員訓練課程至少 10 名(含複訓)		
	執行年度數位韌性巡航計畫	至少 3 項民生關鍵資訊系統以及 20 項機關業務運作系統之巡航作業，並提供技術輔導與執行改善複審作業。	每年至少 6 項民生關鍵資訊系統以及 33 項機關業務運作系統之巡航作業，並提供技術輔導與執行改善複審作業。		
	網路攻防演練	執行演練作業，蒐整機關為民服務資通系統弱點樣態，提供各界參考。			
	維運國家資通安全通報應變網站	執行公務機關與特定非公務機關資安事件通報與諮詢作業。			
	資安技術檢測服務	提供 5 個政府機關或關鍵基礎設施資安技術檢測服務。			
強化政府資訊系統緊急事件應變能量	政府資訊系統緊急事件服務	主動監測民生關鍵資訊系統運作效能，發生系統效能異常事件 1 小時內通報業務主管機關與系統維護廠商。接獲業務主管機關申請查處異常事件後 4 小時內抵達現場或 2 小時內以線上(視訊)方式進行處置。			
	資安事件處理與鑑識分析	持續依需求執行事件處理，提供遠端分析與現場鑑識服務。			

三、執行步驟及方法

(一) 建立政府安全與韌性環境服務機制與其運作模式

1. 任務分類

(1) 服務設計與技術研發組

推動數位服務設計及數位服務流程再造，並探詢、建置、整備共用模組，協助政府機關規劃資訊系統架構，針對資訊系統利害關係人與其任務性質，融合資訊系統雲端化、行動化、去中心化之發展趨勢，設計數位服務使用介面與資訊系統作業程序、資安防護措施，並就標的系統規劃策略面、管理面及技術面之資料治理工作。

(2) 服務韌性與資安防護調和組

輔導政府機關重大資訊系統精進營運韌性，辦理民生關鍵業務之大型資訊系統或跨機關業務流程整合系統(以下簡稱民生關鍵資訊系統)健檢作業，依據資訊系統被賦予之角色、任務為基礎，檢視資訊系統執行情形、測試運作效率、資通安全風險與弱點，針對運作效率不如預期或系統異常、資安漏洞等事件，追蹤問題成因及提出解決方案，並視需要提供技術支援，協助資訊系統維運機關要求其資訊維護廠商落實改善。

(3) 事故應變與協力復原組

因應社會重大事件或政府施政緊急工作，協助業務主管機關建構支援性、應急性之資訊系統；或就現有資訊系統無法因應重大事件之處，鑑識其功能缺口或待改善事項，協助規劃精進措施，並提供技術支援協助主管機關盡速落實精進措施。

2. 運作模式

(1) 平時由「服務設計與技術研發組」及「服務韌性與資安防護調和組」定期或依機關申請，提升政府資訊系統數位韌性力(事故應變與協力復原組人力可支援調和組)。

「服務設計與技術研發組」例行性工作為協助探詢、建置與整備政府機關資訊系統共用資訊資源，以及資訊系統資安環境研析，包括「建構軟體物料清單」、「資訊專案文件與開源

碼詮釋資料中文化」、「擴充政府設計系統元件」、「電腦組態基準研究」、「資通安全弱點研析」、「攻擊研析與偵測防護」及「資安參考指引發展」。

「服務韌性與資安防護調和組」須辦理每年度數位韌性巡航作業相關工作，包括「盤點數位韌性巡航服務對象及維護系統背景資訊」、「擬定年度數位韌性巡航計畫」、「培養數位韌性領航員」、「執行年度數位韌性巡航計畫」、「提供數位韌性技術支援與輔導服務」及「執行改善情形複審作業」等一整套協助政府機關民生關鍵資訊系統服務品質之相關工作，另將藉由年度巡航作業，將「網路攻防演練」、「支援關鍵基礎設施資安防護」、「資安通報與諮詢」及「資安技術檢測服務」等資通安全技術應用。

前述例行性工作雖由兩個組進行，但其內容與 3 個組皆有關連，因此須由 3 個組合力共同完成，並且將執行成果做為日後緊急應變之基礎資訊與元件。

(2) 政府資訊系統發生緊急事件，由「服務韌性與資安防護調和組」及「事故應變與協力復原組」協同主責機關快速回復系統運作。

「服務韌性與資安防護調和組」平時主動或依機關申請即時監測民生關鍵資訊系統運作情形，當發生資訊系統運作異常影響民眾個人權益或生活便利性時，主動通知業務主管機關與資訊系統維護廠商共謀解決方案，並且將平時偵測、蒐集及分析取得之民生關鍵資訊系統運作效能資訊，提供予該次資訊系統運作異常事件，以協助進行「事件與鑑識分析」查處異常事件根因，並視異常狀況複雜程度「籌組專家團隊對症下藥」，協同「服務韌性與資安防護調和組」、主責機關、甚至資安技術團隊，快速反應正確解決問題，以求盡速完成系統回復至可

運作狀態。

(3) 發生社會重大事件或政府施政緊急措施而須建置臨時性系統，則由「服務設計與技術研發組」及「事故應變與協力復原組」協同主責機關建置任務性資訊系統

政府安全與韌性環境服務團接獲行政院指示建置任務性資訊系統(如建構口罩實名制系統、紓困身分比對系統)後，將即時啟動相關工作，包括「籌設跨機關協調溝通小組」、「規劃資訊系統架構」、「善用開源軟體或元件建構系統功能」、「優化使用者操作介面及操作體驗」、「檢測任務性資訊系統功能、資安防護及運作效能」及「交付系統予業務主管機關營運」，以求最短時間內，與主責機關共同提出民眾所需之資訊服務。

(二) 充實政府共享數位資源與資安技術

1. 建構軟體物料清單(Software Bill of Materials；SBOM)

蒐集、整理政府資訊系統可利用之開源軟體，並對其建立 SBOM 記錄構成軟體的元件和關聯表，記錄項目如名稱、版本、來源、可識別代碼、相依性及供應商等資料，並以具有可讀性之 SBOM 報告格式呈現，協助政府機關資訊系統使用的開源軟體具有完整性和可追溯之來源。

2. 資訊專案文件與開源碼詮釋資料中文化

為精進政府機關資訊系統服務品質，世界各國或NGO、NPO組織陸續發布資訊系統共用程式源碼及其技術說明文件，提供外界再利用，如 GOV.UK Notify、GOV.UK Forms、Matrix Client 等。政府安全與韌性環境服務團將我國政府機關資訊系統特性或需求，蒐集世界各團體釋出之資訊專案文件與開源碼詮釋資料，並轉譯為中文內容，提供政府機關資訊系統引用相關開源碼之參考資料。

3. 擴充政府設計系統元件

為了提供更一致、順暢的使用者體驗，制定專屬的網站設計系統，規劃與整理政府系統設計元件庫，讓系統操作者使用網頁為基礎的數位服務時，可獲得一致性之服務感受。政府安全與韌性環境服務團將持續定義政府網站原則（principle）與樣式（style），如顏色、排版或間距，並提供可重複使用的元件（component）及規範互動模式（pattern），讓政府機關網站具有一致性的風格與設計，降低使用者的學習成本，民眾能更容易的使用政府機關網站。

4. 電腦組態基準研究

我國自 2013 年起針對作業系統、瀏覽器、網通設備及應用程式等面向資通訊終端設備，發展電腦組態基準，包含安全組態設定內容與設計部署方式，並配合「資通安全管理法」之推動，提供技術諮詢服務，以協助機關與重要設施環境導入相關資安防護設定，強化資安防護水準，提升民眾使用政府機關服務系統與基礎設施之安全性。2023 年起仍將持續擇定重要之作業系統、瀏覽器、網通設備及應用程式項目進行研究發展，以供各界參考使用。

5. 資通安全弱點研析

蒐集國內外之資安弱點情資，如 National Vulnerability Database、駭客論壇、新聞媒體及資安論壇等，針對重大弱點進行研析與評估可能造成之影響，並蒐集弱點修補方式、緩解措施或檢測工具，適時發布警訊通知各界及早因應，以提升弱點修補速度。

針對掌握之上述弱點情資，評估是否為我國資通訊環境常用系統或應用程式之潛在重大弱點，蒐集相關檢測工具或攻擊程式，架設模擬環境與進行弱點利用可行性測試，並產出重大弱點研析與實作報告公布於官網，協助公私部門進行弱點檢測、評估及修補作業，強化資安防護能量。

6. 攻擊研析與偵測防護

透過分析資安事件處理、中繼站調研、資安健診及外部情資等各項來源所蒐集之駭侵樣本，萃取網路攻擊威脅情資特徵，製作並部署偵測規則於政府骨幹偵測機制，同時配合各項來源情資進行關聯，進一步分類歸納駭侵活動之特徵，針對發動攻擊之族群進行辨識與追蹤，強化我國資訊網路防護能量。

7. 資安參考指引發展

本項工作由資安專業人員與相關領域之專家，持續針對最新之技術發展、資源配置之最適性，並考量公私部門之不同屬性與特色，提出各項資安技術於實務面建議，供政府機關與民間企業均能從中汲取最佳之建議，適當因應變遷之資安環境。因應國際資安威脅趨勢及新興科技發展，規劃資安規範整體發展藍圖，並考量內外在環境變化與技術發展等因素，編撰及修訂資安相關參考指引，以強化資安防護與管理。

(三) 厚植政府資訊系統運作韌性及資安應用

日常例行性工作包括協助探詢、建置與整備資訊資源、辦理數位韌性巡航作業及資通安全技術應用等相關工作。

1. 辦理年度數位韌性巡航作業相關工作

(1) 盤點數位韌性巡航服務對象及維護系統背景資訊

盤點行政院及其所屬機關涉及民生關鍵資訊系統，調查其基礎背景資料並建檔，如資訊系統支援之業務項目、利害關係人、資通安全等級、資訊傳輸電路資訊、資訊機房所在地、伺服器類型、作業系統類型與版本、系統維運主管機關與其主辦人員資料及系統維運廠商資料等。

(2) 擬定年度數位韌性巡航計畫

每年由政府機關主動報名，或由數位發展部擇定民生關鍵資

訊系統辦理健康檢查服務，依據年度重點健檢項目設計檢查事項與評估基準，健檢範圍包括網路傳輸環境設定、資訊系統架構、系統功能運作效能、資料庫系統輸出入效率、終端使用者操作效能、資料管理合宜性及系統弱點檢測等項目。

(3) 培養數位韌性領航員

為培養機關人員具備資訊系統數位韌性健檢能力，數位發展部將自行政院及其所屬機關遴選簡任層級資訊處理職系人員擔任數位韌性領航員，由政府安全與韌性環境服務團培養巡航能力與傳承實務經驗等工作。

(4) 執行年度數位韌性巡航計畫

依據數位發展部核定年度數位韌性巡航計畫以及年度領航員名單，由政府安全與韌性環境服務團執行數位韌性健檢作業，協助業務主管機關診斷資訊系統脆弱點，彙整健檢報告並提出資訊系統健康升級方案，提供業務主管機關具體改善系統脆弱項目，並適時將共用程式庫、設計系統等共享資源納入改善建議。

(5) 提供數位韌性技術支援與輔導服務

政府安全與韌性環境服務團依受檢機關需要提供技術支援顧問服務，協同業務主管機關及其資訊系統服務廠商共同改善資訊系統脆弱點。

(6) 執行改善情形複審作業

透過檢視文件、工具驗證及領航員實地查驗等方式，檢視數位韌性健檢查獲之系統脆弱點的補強情形，倘未改善或改善情形不如預期者，再進行技術支援與輔導工作，並納入次年數位韌性巡航計畫之健檢標的。

2. 辦理常規性資安技術與支援服務

(1) 網路攻防演練

針對重要機關為民服務資通系統，以模擬駭客方式進行資通系統攻擊演練，同時透過社交工程簡訊與郵件演練，主動發掘潛藏於重要機關為民服務資通系統弱點，並測試機關人員資安意識。針對重要機關為民服務資通系統之攻擊演練，係藉由記錄實際入侵手法與發送警訊，提供各機關進行資安事件通報應變處置演練，強化資通系統資安防護。

(2) 維運國家資通安全通報應變網站

依據「資通安全事件通報及應變辦法」相關規定，協助公務機關與特定非公務機關於資安事件發生時，於限定時間內完成復原或損害管制，並提供損害管制建議。維運國家資通安全通報應變網站做為公務機關與特定非公務機關之通報管道，提供公務機關、關鍵基礎設施領域之中央目的主管機關、納管之公營事業與財團法人進行資安事件通報，以利機關迅速通報，並進行緊急應變處置。

(3) 資安技術檢測服務

協助政府機關與關鍵基礎設施執行資安技術檢測服務，針對終端設備、網路架構、網域主機、資通系統及資料庫等構面執行檢測，以找出潛在資安風險與提供改善建議。藉由技術檢測執行，提升受檢單位之安全控制措施落實程度，強化資通安全，以提供社會大眾更安全可靠之資通服務系統與基礎設施服務。

(四) 強化政府資訊系統緊急事件應變能量

主動即時監測民生關鍵資訊系統運作情形，發生資訊系統運作異常影響民眾個人權益或生活便利性時，主動通知業務主管機關與資訊系統維護廠商共謀解決方案。

1. 偵測、蒐集及分析民生關鍵資訊系統運作效能

以不影響民生關鍵資訊系統運作為前提，佈設資訊系統運作效能偵測機制，偵測點包括網際網路端(終端使用者)、網路閘口端、網頁端、資料庫系統端與資料儲存設備端，蒐集系統效能數據，分析資訊系統效能值與異常臨界值。

2. 協助查處異常事件根因

數位發展部與業務主管機關獲得合作共識後，由政府安全與韌性環境服務團與資訊系統維護廠商組成聯合診斷團隊，共同查處系統異常運作情形，優先釐清異常問題肇因於資訊系統資安弱點或是系統運作脆弱點，對症下藥籌組專家團隊協處。

3. 事件處理與鑑識分析

依據機關資安事件通報所需之技術支援，或因應特定單位檢測與中繼站調研需求成立協處專案，提供遠端分析與現場鑑識之技術協助，評估影響範圍，分析所取得包含流量、檔案系統、記憶體、日誌紀錄等事證，查找事件根因並提出改善建議，俾利儘速進行應變，降低事件帶來之影響與衝擊。

4. 籌組專家團隊對症下藥

邀請領域專家與業務主管機關及系統維運廠商共同籌組專家團隊，就業務面、流程面與技術面商議解決策略，提出解決方案後交由業務主管機關與系統維運廠商據以改善，或視需要由政府安全與韌性環境服務團建立臨時性系統功能模組，提供業務主管機關緊急應用。

(五) 針對社會重大事件或政府施政緊急措施建置任務性資訊系統

數位發展部與業務主管機關獲得合作共識後，協調各相關業務機關研商資訊系統功能及執行程序，由政府安全與韌性環境服務團建置任務性資訊系統銜接各相關業務機關之作業程序、資訊系統及業務資

料，經各業務機關測試確認功能符合需求後上線運作，系統交由業務主辦機關持續營運維護。

1. 籌設跨機關協調溝通小組

依據社會重大事件或政府施政緊急措施為基礎，邀請相關部會首(次)長、業務與資訊單位主管成立協調溝通小組，共同商議任務性資訊系統擔任之角色、釐清利害關係人需求、規劃以數位為優先之作業程序、例外處理規則及劃分各利害關係人應配合事項與權利義務。

2. 規劃資訊系統架構

依據業務性質與利害關係人需求，以數位首選(digital by default)之原則設計資訊系統架構，從資料蒐集階段到處理、儲存階段及後續再利用階段，盡可能以數位方式替代人工作業，運用 API 資料介接方式即時與外部資訊系統進行資料傳輸，提升業務運作效率與正確率。

3. 善用開源軟體或元件建構系統功能

為加速資訊系統開發效率，提升系統架構彈性，任務性資訊系統以「快速建置」、「安全至上」、「簡化程序」及「輕量管理」為原則，運用敏捷式資訊系統開發模式，並善用政府安全與韌性環境服務團檢測之開源軟體或元件，建置資訊系統功能。

4. 優化使用者操作介面及操作體驗

針對任務型資訊系統重複出現的使用介面元素，優先使用政府設計系統元件庫所列各式使用者操作介面元件，統一規格與互動方式，使其具有一致性與邏輯性。

5. 檢測任務性資訊系統功能、資安防護及運作效能

資訊系統建置過程定期進行元件測試、功能測試及整合測試，

確認系統功能運作邏輯符合預期，檢測資訊系統運作效能瓶頸點，並解開瓶頸封印，資訊系統上線前進行資通安全相關檢測工作，確保系統上線展現高效率、好品質、強資安之成效。

6. 交付系統予業務主管機關營運

任務型資訊系統之規格文件、架構資料、網路拓樸、程式原始碼、元件關聯拓樸、資料流程圖及資料庫規格等相關系統資料，提供業務主管機關持續營運與調整，或做為未來正式業務資訊系統之建構基準。

伍、期程與資源需求

一、計畫期程

本計畫為 4 年期中長程個案計畫，執行期程自民國 112 年起至 115 年。

二、所需資源說明

本計畫為 4 年期計畫，規劃「建構政府安全與韌性環境服務機制並提供各部會服務」、「充實政府共享數位資源與資安技術」、「厚植政府資訊系統運作韌性及資安應用」及「強化政府資訊系統緊急事件應變能量」等 4 項策略推動計畫各項重點工作，並依計畫預定時程逐年編列預算(112 年計畫經費預估總表詳見表 2)，本(112)年各項策略所需資源分述如下：

表2　112 年計畫經費預估總表

單位：千元

項次	推動策略	112 年預算需求
1	建構政府安全與韌性環境服務機制並提供各部會服務	122,200

項次	推動策略	112 年預算需求
2	充實政府共享數位資源與資安技術	36,309
3	厚植政府資訊系統運作韌性及資安應用	58,002
4	強化政府資訊系統緊急事件應變能量	38,326
合計		254,837

(一) 建構政府安全與韌性環境服務機制並提供各部會服務

本策略主要招募或委託政府安全與韌性環境服務團專業技術人員 47 人，每人年薪暫估新臺幣(以下幣別均同)200 萬元，另加勞健保、年終獎金及績效獎金與招募人力衍生之行政費用，每人每年約 260 萬元(200 X 1.3 = 260)，總計 122,200 千元。

表3　策略 1 經費預估表

單位：千元

項次	工作項目	經常門	資本門
1	聘請專業人員建立服務團隊	122,200	-
總計		122,200	-

(二) 充實政府共享數位資源與資安技術

本策略主要包含建構軟體物料清單、資訊專案文件與開源碼詮釋資料中文化、擴充政府設計系統元件、電腦組態基準研究、資通安全弱點研析、攻擊研析與偵測防護及資安參考指引發展等 7 項工作，各項工作之經資門詳見表 4。

表4　策略 2 經費預估表

單位：千元

項次	工作項目	經常門	資本門
1	建構軟體物料清單	4,034	-
2	資訊專案文件與開源碼詮釋資料中文化	2,690	-
3	擴充政府設計系統元件	5,715	-
4	電腦組態基準研究	7,195	-
5	資通安全弱點研析	10,422	-
6	攻擊研析與偵測防護	5,379	-
7	資安參考指引發展	847	-
總計		36,309	-

(三) 厚植政府資訊系統運作韌性及資安應用

本策略主要工作有「辦理年度數位韌性巡航作業相關工作」及「辦理常規性資安技術與支援服務」，各項工作之經資門詳見表 5。

表5　策略 3 經費預估表

單位：千元

項次	工作項目	經常門	資本門
1	辦理年度數位韌性巡航作業相關工作		
1-1	盤點數位韌性巡航服務對象及維護系統背景資訊	1,345	-
1-2	擬定年度數位韌性巡航計畫	672	-
1-3	培養數位韌性領航員	672	-
1-4	執行年度數位韌性巡航計畫	5,379	-
1-5	提供數位韌性技術支援與輔導服務	10,758	-

項次	工作項目	經常門	資本門
1-6	執行改善情形複審作業	6,724	-
小計		25,550	-
2	辦理常規性資安技術與支援服務		
2-1	網路攻防演練	23,534	-
2-2	維運資安事件通報應變網站	2,690	-
2-3	資安技術檢測服務	6,228	-
小計		32,452	-
總計		58,002	

(四) 強化政府資訊系統緊急事件應變能量

本策略主要工作包含「偵測、蒐集及分析民生關鍵資訊系統運作效能」、「協助查處異常事件根因」、「事件處理與鑑識分析」及「籌組專家團隊對症下藥」等 4 項工作，各項工作之經資門詳見表 6。

表6　策略 4 經費預估表

單位：千元

項次	工作項目	經常門	資本門
1	偵測、蒐集及分析民生關鍵資訊系統運作效能	18,827	-
2	協助查處異常事件根因	6,724	-
3	事件處理與鑑識分析	7,396	-
4	籌組專家團隊對症下藥	5,379	-
總計		38,326	-

三、經費來源及計算基準

(一) 經費來源

本計畫 4 年總經費為 1,391,837 千元，第 1 年預算為 254,837 千元，第 2 年至第 4 年預算為每年 379,000 千元，經費來源擬爭取社會發展計畫預算，依計畫預定時程逐年編列預算辦理。

(二) 計費基準

本計畫 112 年所需經費計新臺幣 254,837 千元，經費類別均屬經常門費用。

四、經費需求(含分年經費)

本計畫各年度經費需求及經資門分配說明詳見表 7。

表7　各年度經費需求表

單位：千元

年度 類別	112	113	114	115
經常門	254,837	379,000	379,000	379,000
資本門	-	-	-	-
各年度小計	254,837	379,000	379,000	379,000
			全計畫總計	1,391,837

陸、預期效果及影響

一、預期效益

(一) 強化政府數位韌性，獲取民眾信任

延攬資訊專業人才支援政府機關強化資訊系統運作韌性，籌獲最新資通訊技術能量，彌補政府機關數位服務發展缺口，提升政府資訊系統為民服務運作效能與服務品質，降低政府與民眾對立與猜忌立場。

(二) 充實政府數位資源與資安技術，提升政府資訊資源應用效率

整備開源軟體、元件程式碼，蒐集設計系統共用元件，並提供中文化技術文件，提供政府機關建構數位系統使用，透過一致且便於操作之設計系統元件，提升民眾使用政府資訊系統之數位體驗；建立一致性安全組態架構與組態管理程序，避免因設定錯誤所導致之系統運作風險，強化整體資安防護能量，降低因人為失誤而系統運作失效機會提升機關為民服務之系統與基礎設施安全性，並提供政府強化資通訊環境組態安全設置之參考依據。

(三) 定期系統健檢作業與網路攻防演練，提升同仁檢測資訊系統運作韌性能力

訓練政府機關同仁具備資訊系統韌性運作自檢能力，並每年定期辦理民生關鍵資訊系統及政府業務資訊系統健檢作業，邀請政府機關同仁實際參與檢查工作，讓同仁具備挖掘資訊系統問題與風險之能力，亦鼓勵政府機關自我檢視資訊系統運作情形，主動掌握系統運作情形。主動發掘政府機關提供民眾使用之資通系統漏洞，並強化政府機關對於資安事件應變處置及復原能力，提升社會大眾使用政府機關資通系統之安全。

(四) 及時檢測系統運作情形並協助事件處理，降低異常事件造成系統停擺風險

運用系統運作效能監控工具，從民眾端、網路端、系統端及資料庫端定期蒐集資訊系統運作績效，發現違反常規之系統狀態，主動協助政府機關檢查系統異常根因，協助政府機關釐清異常事件概況與影

響範圍，並提供相對應建議，以提升應處效率，降低異常事件所造成之衝擊與危害，同時將此資訊與來源相關情資進行關聯與分析，以掌握資安威脅趨勢。

二、主要績效指標(KPI)

本計畫分項目標與主要績效指標如下：

表8　分項目標與主要績效指標

策略項目	指標項目	衡量方式	目標值			
			112	113	114	115
充實政府共享數位資源與資安技術	整備軟體模組物件	累計整備(新增或更新)軟體模組物件之數量，以開源軟體或其他可共享之資源為主，提供政府機關加值應用	30	60	90	120
	重大弱點研析及駭客攻擊偵測規則研製	累計公布重大弱點研析成果及產出偵測駭客攻	2	4	6	8

		擊規則模型，供公私部門進行偵測與修補，以提升資安防護能量				
厚植政府資訊系統運作韌性及資安應用	數位韌性巡航作業	累計擇定政府民生關鍵資訊系統及機關業務運作系統健檢作業，提升政府數位韌性運作	23	62	101	140
	資安技術檢測服務	累計提供政府機關或關鍵基礎設施資安技術檢測服務	5	10	15	20
強化政府資訊系統緊急事件應變能量	支援解決政府資訊系統異常運作	主動支援受監測之政府機關資料系統	● 發生系統效能異常事件 1 小時內通報業務主管機關與系統維護廠商。 ● 接獲業務主管機關申請查處異常			

		發生運作異常之時效	事件後 4 小時內抵達現場或 2 小時內以線上(視訊)方式進行處置。

柒、財務計畫

本計畫全程所需經費計新臺幣 1,391,837 千元，採「建構政府安全與韌性環境服務機制並提供各部會服務」「充實政府共享數位資源與資安技術」、「厚植政府資訊系統運作韌性及資安應用」及「強化政府資訊系統緊急事件應變能量」等 4 項策略，分 4 年推動與執行，各年度經費皆本於撙節用度之原則詳加推算，務使公務預算發揮最大效益，未來於本計畫執行過程中，亦將落實檢討相關經費支用情形，期透過適時評估及檢討，覈實計畫預算編列，以符實際需要(各項策略財務規劃，請參閱第伍章期程與資源需求)。

捌、附則

一、替選方案之分析及評估

本計畫需求事項均屬我國推動智慧國家方案，提升政府資訊系統數位韌性與資安防護建設應行事項，亟需爭取經費挹注，以提升我國數位競爭力，尚無其他可替選之方案。

二、風險管理

本計畫訂定風險管理在於透過系統化之風險評鑑方法(ISO 31000)，釐清計畫所可能面臨之風險；採國際標準化組織(ISO)之高階管理架構，以風險管理角度考量組織全景議題，同時藉由風險評鑑結果決定資訊資產之可接受風險等級，並針對高於可接受等級風險項目，控制其風險在可接受之程度內，確保計畫所屬資訊資產安全之目的。

(一) 風險管理流程

1. 風險管理作業項目

風險管理程序區分為組織全景議題審查作業、關鍵(核心)業務審查作業，及資訊資產風險評鑑作業，資訊資產風險評鑑作業包含建立資產清單、資產價值鑑別、威脅、弱點鑑別、計算風險值、決定風險等級，依據高風險之項目擬定風險處理計畫，據以執行安控措施，最後施行有效性評估，形成 PDCA 之持續改善機制。

2. 審查頻率

原則上每半年進行一次審查，或視需要不定期進行組織全景議題審視或風險評鑑作業。

(二) 風險管理作業說明

1. 組織全景議題審查作業

組織全景議題則蒐集與本計畫工作項目相關之議題，並評估該議題之威脅、可能發生之機率及發生後對本計畫之衝擊，同時擬定因應作法或建議，經代表核定，以決定該次高風險議題，並制訂因應作法。

(1) 議題評價說明

表9　議題威脅發生之可能性

等級	價值	機率
低	1	發生的機率 ≦10%
中	2	發生的機率 >10%~≦30%
高	3	發生的機率 >30%

表10 議題威脅發生後對本計畫之衝擊

等級	價值	衝擊
低	1	對機關之營運、資產或信譽等方面將產生有限範圍之影響
中	2	對機關之營運、資產或信譽等方面將產生嚴重之影響
高	3	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

(2) 組織全景風險值

將威脅發生機率與威脅發生後對本計畫之衝擊等 2 個項目評定分數相乘即為風險值，其公式表示如下：

風險值=威脅發生機率×威脅發生後對本計畫之衝擊

(3) 組織全景決定風險等級

研析所有風險值範圍與影響，訂定風險等級與風險值區間，俾了解各項組織全景議題之風險等級。依據風險評鑑結果，將風險值區分 3 個風險等級(詳見表 11)，並彙整風險分布報告，陳管理代表決定「可接受風險等級」。

(4) 組織全景風險值區間

表11 組織全景風險值區間

風險等級	說明
低風險	風險值≤2
中風險	風險值>2~≤4
高風險	風險值>4

(5) 組織全景風險處理計畫

高於可接受風險等級之議題由評估者研擬風險處理計畫，若風險仍無法被減緩時，需向管理階層事前諮詢與授權，經核決後，採取因應措施或修改相關文件。

(6) 關鍵(核心)業務審查作業

關鍵(核心)業務由工作項目評估，並由代表核定，以決定出該年度關鍵(核心)業務，做為業務持續運作計畫(BCP)之依據。

三、機關配合事項或民眾參與情形

本計畫屬國家層級智慧國家專業發展推動，強固政府機關資訊系統運作韌性及資通安全防護相關事務，協助政府機關加速建構完善之數位服務，各機關支持本計畫各項工作，落實建構強韌之政府數位服務，所有工作均屬政府機關協同合作工作，未涉及民眾使用之介面。

四、中長程個案計畫自評檢核表及性別影響評估檢視表

本計畫自評檢核表如附件一，性別影響評估檢視表如附件二。

五、其他有關事項

本計畫如有調整必要，得經報奉核可後修正。

附件1 自評檢核表

中長程個案計畫自評檢核表

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
1、計畫書格式	(1)計畫內容應包含項目是否均已填列(「行政院所屬各機關中長程個案計畫編審要點」（以下簡稱編審要點）第 5 點、第 10 點)	V				本計畫為新興計畫，非屬延續性計畫。
	(2)延續性計畫是否辦理前期計畫執行成效評估，並提出總結評估報告(編審要點第 5 點、第 13 點)		V			
	(3)是否本於提高自償之精神提具相關財務策略規劃檢核表？並依據各類審查作業規定提具相關書件		V			
2、民間參與可行性評估	是否填寫「促參預評估檢核表」評估（依「公共建設促參預評估機制」）		V			非屬公共建設促參對象。
3、經濟及財務效益評估	(1)是否研提選擇及替代方案之成本效益分析報告(「預算法」第 34 條)		V			經評估無相關替選方案與財務計畫。
	(2)是否研提完整財務計畫		V			
4、財源籌措及資金運用	(1)經費需求合理性(經費估算依據如單價、數量等計算內容)	V				1. 本計畫未涉基金應用自償性收益。 2. 本計畫非屬公共建設計畫，亦不具自償性。
	(2)資金籌措：本於提高自償之精神，將影響區域進行整合規劃，並將外部效益內部化		V			
	(3)經費負擔原則： a.中央主辦計畫：中央主管相關法令規定 b.補助型計畫：中央對直轄市及縣(市)政府補助辦法、本於提高自償之精神所擬訂各類審查及補助規定	V (a)				
	(4)年度預算之安排及能量估算：所需經費能否於中程歲出概算額度內容納加以檢討，如無法納編者，應檢討調減一定比率之舊有經費支應；如仍有不敷，須檢附以前年度預算執行、檢討不經濟支出及自行檢討調整結果等經費審查之相關文件	V				
	(5)經資比 1：2（「政府公共建設計畫先期作業實施要點」第 2 點）		V			

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
	(6)屬具自償性者，是否透過基金協助資金調度		V			
5、人力運用	(1)能否運用現有人力辦理	V				本計畫未涉人力請增事宜。
	(2)擬請增人力者，是否檢附下列資料： a.現有人力運用情形 b.計畫結束後，請增人力之處理原則 c.請增人力之類別及進用方式 d.請增人力之經費來源		V			
6、營運管理計畫	是否具務實及合理性(或能否落實營運)	V				
7、土地取得	(1)能否優先使用公有閒置土地房舍		V			1. 本計畫未涉土地取得。 2. 本計畫非屬補助型計畫。
	(2)屬補助型計畫，補助方式是否符合規定（中央對直轄市及縣(市)政府補助辦法第 10 條）		V			
	(3)計畫中是否涉及徵收或區段徵收特定農業區之農牧用地		V			
	(4)是否符合土地徵收條例第 3 條之 1 及土地徵收條例施行細則第 2 條之 1 規定		V			
	(5)若涉及原住民族保留地開發利用者，是否依原住民族基本法第 21 條規定辦理		V			
8、風險管理	是否對計畫內容進行風險管理	V				詳見風險管理章節。
9、環境影響分析(環境政策評估)	是否須辦理環境影響評估		V			本計畫非屬環境影響評估法第 5 條規定應辦理環境影響評估範圍。
10、性別影響評估	是否填具性別影響評估檢視表	V				
11、無障礙及通用設計影響評估	是否考量無障礙環境，參考建築及活動空間相關規範辦理		V			本計畫未涉房舍建築，故不適用於無障礙及通設計影響評估。
12、高齡社會影響評估	是否考量高齡者友善措施，參考 WHO「高齡友善城市指南」相關規定辦理		V			本計畫未涉高齡友善城市面向，故不適用。
13、涉及	是否檢附計畫範圍具座標之向量圖檔		V			本計畫未涉

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
空間規劃者						房舍建築及空間規劃。
14、涉及政府辦公廳舍興建購置者	是否納入積極活化閒置資產及引進民間資源共同開發之理念		V			本計畫使用現有房舍。
15、跨機關協商	(1)涉及跨部會或地方權責及財務分攤，是否進行跨機關協商		V			本計畫未涉財務分攤問題。
	(2)是否檢附相關協商文書資料		V			
16、依碳中和概念優先選列節能減碳指標	(1)是否以二氧化碳之減量為節能減碳指標，並設定減量目標		V			本計畫內容未涉二氧化碳減量相關事項。
	(2)是否規劃採用綠建築或其他節能減碳措施		V			
	(3)是否檢附相關說明文件		V			
17、資通安全防護規劃	資通系統是否辦理資通安全防護規劃	V				

附件2 性別影響評估檢視表

中長程個案計畫性別影響評估檢視表【一般表】

【第一部分－機關自評】：由機關人員填寫

【填表說明】各機關使用本表之方法與時機如下：

一、計畫研擬階段

（一）請於研擬初期即閱讀並掌握表中所有評估項目；並就計畫方向或構想徵詢作業說明第三點所稱之性別諮詢員（至少１人），或提報各部會性別平等專案小組，收集性別平等觀點之意見。

（二）請運用本表所列之評估項目，將性別觀點融入計畫書草案：

1、將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節。

2、將達成性別目標之主要執行策略納入計畫書草案之適當章節。

二、計畫研擬完成

（一）請填寫完成【第一部分－機關自評】之「壹、看見性別」及「貳、回應性別落差與需求」後，併同計畫書草案送請性別平等專家學者填寫【第二部分－程序參與】，宜至少預留１週給專家學者（以下稱為程序參與者）填寫。

（二）請參酌程序參與者之意見，修正計畫書草案與表格內容，並填寫【第一部分－機關自評】之「參、評估結果」後通知程序參與者審閱。

三、計畫審議階段：請參酌行政院性別平等處或性別平等專家學者意見，修正計畫書草案及表格內容。

四、計畫執行階段：請將性別目標之績效指標納入年度個案計畫管制並進行評核；如於實際執行時遇性別相關問題，得視需要將計畫提報至性別平等專案小組進行諮詢討論，以協助解決所遇困難。

註：本表各欄位除評估計畫對於不同性別之影響外，亦請關照對不同性傾向、性別特質或性別認同者之影響。

計畫名稱：提升政府資通訊系統數位韌性計畫			
主管機關 （請填列中央二級主管機關）	行政院數位發展部	主辦機關（單位） （請填列擬案機關／單位）	行政院數位發展部

看見性別：檢視本計畫與性別平等相關法規、政策之相關性，並運用性別統計及性別分析，「看見」本計畫之性別議題。	
評估項目	評估結果
1-1【請說明本計畫與性別平等相關法規、政策之相關性】性別平等相關法規與政策包含憲法、法律、性別平等政策綱領及消除對婦女一切形式歧視公約（CEDAW）可參考行政院性別平等會網站（https://gec.ey.gov.tw）。	因應國際性別主流化潮流，推動性別平等政策綱領，建構性別友善職場環境，鼓勵女性參與決策，於各層級合議式決策機制(委員會)內，應
評估項目	評估結果
1-2【請蒐集與本計畫相關之性別統計及性別分析（含前期或相關計畫之執行結果），並分析性別落差情形及	1. 本計畫政策規劃者共４人，女性有２人占比

原因】 請依下列說明填寫評估結果： a. 歡迎查閱行政院性別平等處建置之「性別平等研究文獻資源網」(https://www.gender.ey.gov.tw/research/)、「重要性別統計資料庫」(https://www.gender.ey.gov.tw/gecdb/)（含性別分析專區）、各部會性別統計專區、我國婦女人權指標及「行政院性別平等會─性別分析」(https://gec.ey.gov.tw)。 b. 性別統計及性別分析資料蒐集範圍應包含下列3類群體： ①政策規劃者（例如:機關研擬與決策人員；外部諮詢人員）。 ②服務提供者（例如:機關執行人員、委外廠商人力）。 ③受益者（或使用者）。 c. 前項之性別統計與性別分析應儘量顧及不同性別、性傾向、性別特質及性別認同者，探究其處境或需求是否存在差異，及造成差異之原因；並宜與年齡、族群、地區、障礙情形等面向進行交叉分析（例如：高齡身障女性、偏遠地區新住民女性），探究在各因素交織影響下，是否加劇其處境之不利，並分析處境不利群體之需求。前述經分析所發現之處境不利群體及其需求與原因，應於後續【1-3找出本計畫之性別議題】，及【貳、回應性別落差與需求】等項目進行評估說明。 d. 未有相關性別統計及性別分析資料時，請將「強化與本計畫相關的性別統計與性別分析」列入本計畫之性別目標（如2-1之ｆ）。	50%，已超過1/3。 2. 本計畫完成後，不以特定性別、性傾向或性別認同者為受益對象。 3. 過去五年(103年至107年)資訊通訊科技領域之畢業生男女性別比率約為7比3。本計畫辦理時，將鼓勵女性參與，且參與率不低於30%。
評估項目	評估結果
1-3【請根據1-1及1-2的評估結果，找出本計畫之性別議題】 性別議題舉例如次： a. 參與人員 政策規劃者或服務提供者之性別比例差距過大時，宜關注職場性別隔離（例如：某些職業的從業人員以特定性別為大宗、高階職位多由單一性別擔任）、職場性別友善性不足（例如：缺乏防治性騷擾措施；未設置哺集乳室；未顧及員工對於家庭照顧之需求，提供彈性工作安排等措施），及性別參與不足等問題。 b. 受益情形 ①受益者人數之性別比例差距過大，或偏離母體	1. 本計畫決策人員女性比例超過1/3，機關執行人員將鼓勵女性參與，且參與率不低於30%，無性別參與不足等問題。 2. 本計畫完成後，不以特定性別、性傾向或性別認同者為受益對象。 3. 本計畫辦理時，將建議執行機關於公共空間營造性別友善環境，並鼓勵弱勢性別族群參與。

之性別比例，宜關注不同性別可能未有平等取得社會資源之機會（例如:獲得政府補助；參加人才培訓活動），或平等參與社會及公共事務之機會（例如:參加公聽會/說明會）。 ②受益者受益程度之性別差距過大時（例如:滿意度、社會保險給付金額），宜關注弱勢性別之需求與處境（例如:家庭照顧責任使女性未能連續就業，影響年金領取額度）。 c. 公共空間 公共空間之規劃與設計，宜關注不同性別、性傾向、性別特質及性別認同者之空間使用性、安全性及友善性。 ①使用性：兼顧不同生理差異所產生的不同需求。 ②安全性：消除空間死角、相關安全設施。 ③友善性：兼顧性別、性傾向或性別認同者之特殊使用需求。 d. 展覽、演出或傳播內容 藝術展覽或演出作品、文化禮俗儀典與觀念、文物史料、訓練教材、政令/活動宣導等內容，宜注意是否避免複製性別刻板印象、有助建立弱勢性別在公共領域之可見性與主體性。 e. 研究類計畫 研究類計畫之參與者（例如:研究團隊）性別落差過大時，宜關注不同性別參與機會、職場性別友善性不足等問題；若以「人」為研究對象，宜注意研究過程及結論與建議是否納入性別觀點。	
貳、回應性別落差與需求：針對本計畫之性別議題，訂定性別目標、執行策略及編列相關預算。	
評估項目	評估結果
2-1【請訂定本計畫之性別目標、績效指標、衡量標準及目標值】 請針對 1-3 的評估結果，擬訂本計畫之性別目標，並為衡量性別目標達成情形，請訂定相應之績效指標、衡量標準及目標值，並納入計畫書草案之計畫目標章節。性別目標宜具有下列效益： 1. 參與人員 ①促進弱勢性別參與本計畫規劃、決策及執行，納入不同性別經驗與意見。 ②加強培育弱勢性別人才，強化其領導與管理知能，以利進入決策階層。 ③營造性別友善職場，縮小職場性別隔離。 2. 受益情形 ①回應不同性別需求，縮小不同性別滿意度落差 ②增進弱勢性別獲得社會資源之機會（例如:獲得	1. 本計畫係為執行國家資通安全研究院主要業務，包含研發資通安全科技，推動資通安全技術應用、移轉、產學服務及國際合作交流。計畫規劃階段決策人員女性占比已達 50%，未來機關執行人員將鼓勵女性參與，且參與率應不低於 30%，且計畫完成後，不以特定性別、性傾向或性別認同者為受益對象，故本次不另外訂定性別目標。

政府補助；參加人才培訓活動）。 ③增進弱勢性別參與社會及公共事務之機會（例如:參加公聽會/說明會，表達意見與需求）。 3. 公共空間 回應不同性別對公共空間使用性、安全性及友善性之意見與需求，打造性別友善之公共空間。 4. 展覽、演出或傳播內容 ①消除傳統文化對不同性別之限制或僵化期待，形塑或推展性別平等觀念或文化。 ②提升弱勢性別在公共領域之可見性與主體性（如作品展出或演出；參加運動競賽）。 5. 研究類計畫 ①產出具性別觀點之研究報告。 ②加強培育及延攬環境、能源及科技領域之女性研究人才，提升女性專業技術研發能力。 6. 強化與本計畫相關的性別統計與性別分析。 7. 其他有助促進性別平等之效益。	2. 本計畫辦理時，將建議執行機關了解弱勢性別族群之需求，營造性別友善環境，鼓勵弱勢性別族群參與。
評估項目	評估結果
2-2【請根據 2-1 本計畫所訂定之性別目標，訂定執行策略】 請參考下列原則，設計有效的執行策略及其配套措施： a. 參與人員 ①本計畫研擬、決策及執行各階段之參與成員、組織或機制（如相關會議、審查委員會、專案辦公室成員或執行團隊）符合任一性別不少於三分之一原則。 ②前項參與成員具備性別平等意識/有參加性別平等相關課程。 b. 宣導傳播 ①針對不同背景的目標對象（如不諳本國語言者；不同年齡、族群或居住地民眾）採取不同傳播方法傳布訊息（例如：透過社區公布欄、鄰里活動、網路、報紙、宣傳單、APP、廣播、電視等多元管道公開訊息，或結合婦女團體、老人福利或身障等民間團體傳布訊息）。 ②宣導傳播內容避免具性別刻板印象或性別歧視意味之語言、符號或案例。 ③與民眾溝通之內容如涉及高深專業知識，將以民眾較易理解之方式，進行口頭說明或提供書面資料。 c. 促進弱勢性別參與公共事務 ①計畫內容若對人民之權益有重大影響，宜與民眾進行充分之政策溝通，並落實性別參與。 ②規劃與民眾溝通之活動時，考量不同背景者之	1. 本計畫係為執行國家資通安全研究院主要業務，包含研發資通安全科技，推動資通安全技術應用、移轉、產學服務及國際合作交流。計畫規劃階段決策人員女性占比已達 50%，未來機關執行人員將鼓勵女性參與，且參與率應不低於 30%，且計畫完成後，不以特定性別、性傾向或性別認同者為受益對象。 2. 本計畫辦理時，將建議執行機關了解弱勢性別族群之需求，營造性別友善環境，鼓勵弱勢性別族群參與。

參與需求，採多元時段辦理多場次，並視需要提供交通接駁、臨時托育等友善服務。 ③辦理出席民眾之性別統計；如有性別落差過大情形，將提出加強蒐集弱勢性別意見之措施。 ④培力弱勢性別，形成組織、取得發言權或領導地位。 d. 培育專業人才 ①規劃人才培訓活動時，納入鼓勵或促進弱勢性別參加之措施 （例如:提供交通接駁、臨時托育等友善服務；優先保障名額；培訓活動之宣傳設計，強化歡迎或友善弱勢性別參與之訊息；結合相關機關、民間團體或組織，宣傳培訓活動）。 ②辦理參訓者人數及回饋意見之性別統計與性別分析，做為未來精進培訓活動之參考。 ③培訓內涵中融入性別平等教育或宣導，提升相關領域從業人員之性別敏感度。 ④辦理培訓活動之師資性別統計，做為未來師資邀請或師資培訓之參考。 e. 具性別平等精神之展覽、演出或傳播內容 ①規劃展覽、演出或傳播內容時，避免複製性別刻板印象，並注意創作者、表演者之性別平衡。 ②製作歷史文物、傳統藝術之導覽、介紹等影音或文字資料時，將納入現代性別平等觀點之詮釋內容。 ③規劃以性別平等為主題的展覽、演出或傳播內容（例如:女性之歷史貢獻、對多元性別之了解與尊重、移民女性之處境與貢獻、不同族群之性別文化）。 f. 建構性別友善之職場環境 委託民間辦理業務時，推廣促進性別平等之積極性作法（例如：評選項目訂有友善家庭、企業托兒、彈性工時與工作安排等性別友善措施；鼓勵民間廠商拔擢弱勢性別優秀人才擔任管理職），以營造性別友善職場環境。 g. 具性別觀點之研究類計畫 ①研究團隊成員符合任一性別不少於三分之一原則，並積極培育及延攬女性科技研究人才；積極鼓勵女性擔任環境、能源與科技領域研究類計畫之計畫主持人。 ②以「人」為研究對象之研究，需進行性別分析，研究結論與建議亦需具性別觀點。	
評估項目	評估結果
2-3【請根據 2-2 本計畫所訂定之執行策略，編列或調整相	本計畫係為執行國家資通

關經費配置】 各機關於籌編年度概算時，請將本計畫所編列或調整之性別相關經費納入性別預算編列情形表，以確保性別相關事項有足夠經費及資源落實執行，以達成性別目標或回應性別差異需求。	安全研究院主要業務，包含研發資通安全科技，推動資通安全技術應用、移轉、產學服務及國際合作交流，且計畫完成後，不以特定性別、性傾向或性別認同者為受益對象，故本次不另外訂定性別目標。

【注意】填完前開內容後，請先依「填表說明二之（一）」辦理【第二部分－程序參與】，再續填下列「參、評估結果」。

參、評估結果

請機關填表人依據【第二部分－程序參與】性別平等專家學者之檢視意見，提出綜合說明及參採情形後通知程序參與者審閱。

3-1 綜合說明		
3-2 參採情形	3-2-1 說明採納意見後之計畫調整（請標註頁數）	1. 附 2-2、由「女性參與率不應低於 30%」改為「參與人員之任一性別比率不低於三分之一」。 2. 附 2-5、納入「本計畫參與人員皆具備性別平等意識且參與過相關性別課程訓練，俾利將性別平等觀念於執行時融入此項工作計畫。
	3-2-2 說明未參採之理由或替代規劃	無
3-3 通知程序參與之專家學者本計畫之評估結果： 已於　年　月　日將「評估結果」及「修正後之計畫書草案」通知程序參與者審閱。		

填表人姓名：蘇煒哲 職稱：分析師 電話：02-33568207 填表日期：111 年 8 月 6 日

本案已於計畫研擬初期■徵詢性別諮詢員之意見，或□提報各部會性別平等專案小組（會議日期：____年____月____日）

性別諮詢員姓名：張瓊玲 服務單位及職稱：臺灣警察專科學校海洋巡防科教授

身分：符合中長程個案計畫性別影響評估作業說明第三點第 1 至 3 款（如提報各部會性別平等專案小組者，免填）

（請提醒性別諮詢員恪遵保密義務，未經部會同意不得逕自對外公開計畫草案）

【第二部分－程序參與】：由性別平等專家學者填寫

程序參與之性別平等專家學者應符合下列資格之一： ■1.現任臺灣國家婦女館網站「性別主流化人才資料庫」公、私部門之專家學者；其中公部門專家應非本機關及所屬機關之人員（人才資料庫網址:http://www.taiwanwomencenter.org.tw/）。 ■2.現任或曾任行政院性別平等會民間委員。 ■3.現任或曾任各部會性別平等專案小組民間委員。	
（一）基本資料	
1.程序參與期程或時間	111 年 8 月 4 日 至 111 年 8 月 5 日
2.參與者姓名、職稱、服務單位及其專長領域	張瓊玲、臺灣警察專科學校海洋巡防科教授、經濟部等性別平等專案小組委員、工業局性別平等工作小組委員。 性別政策與公共政策；性別主流化政策；性別影響評估擬議與審查；CEDAW 與友善家庭方案；文官體制與人力資源管理
3.參與方式	□計畫研商會議 □性別平等專案小組 ■書面意見
（二）主要意見（若參與方式為提報各部會性別平等專案小組，可附上會議發言要旨，免填 4 至 10 欄位，並請通知程序參與者恪遵保密義務）	
4.性別平等相關法規政策相關性評估之合宜性	合宜
5.性別統計及性別分析之合宜性	合宜
6.本計畫性別議題之合宜性	合宜
7.性別目標之合宜性	合宜
8.執行策略之合宜性	請酌做修正
9.經費編列或配置之合宜性	合宜
10.綜合性檢視意見	本計畫之性別影響評估內園所列之文字：「未來，機關執行人員將鼓勵女性參與，且參與率應不低於 30%」，請改為：「未來，機關執行人員將鼓勵女性參與，且參與人員之任一性別比率應不低於三分之一」。另外，請於 2-2 欄內之說明清楚敘明「本計畫參與人員皆具備性別平等意識且參與過相關性別課程訓練，俾利將性別平等觀念於執行時融入此項工程計畫」等文字說明。
（三）參與時機及方式之合宜性	合宜
本人同意恪遵保密義務，未經部會同意不得逕自對外公開所評估之計畫草案。 （簽章，簽名或打字皆可）___張 瓊 玲_	