中華民國九十年一月十七日行政院第二七一八次院會通過
中華民國九十年四月廿四日行政院　院長核定第一次修訂
中華民國九十一年六月六日行政院　院長核定第二次修訂

建立我國通資訊基礎建設安全機制計畫

行　　政　　院

中華民國九十一年六月六日

建立我國通資訊基礎建設安全機制計畫

壹、依據：

一、奉　總統八十九年八月卅日核定「建立我國通資訊基礎建設安全機制」案辦理。

二、依行政院秘書長八十九年九月十五日台八十九科字第二七一七九號函辦理。

三、依八十九年十二月二十九日行政院國家資訊通信發展推動小組委員會通過辦理。

四、奉九十年一月九日　院長核定同意辦理。

五、依九十年一月十七日行政院第二七一八次院會通過辦理。

六、奉九十年四月二十四日行政院　院長核定第一次修訂辦理。

七、奉九十一年六月六日行政院　院長核定第二次修訂辦理。

貳、前言：

隨著現代資訊化社會的來臨，許多大型企業、金融機構、政府機關以及國軍各軍事單位都相繼採用電腦資訊化作業，以減少人力、物力、財力之投資與維護，於是許多重要的資料都將儲存在電腦中或利用電腦通訊網路來傳遞。然而，這些儲存或傳遞的資料均可能涉及商業機密、個人隱私權，甚至國家安全之機密。因此，要如何防範電腦網路犯罪與危機，並維護資訊系統安全將是政府施政最迫切的課題；鑒於「七二九大停電」與「九二一大地震」對台灣社會所造成的影響記憶猶新；我們是否有能力防止中國大陸運用各種手段攻擊

台灣，尤其近年來中國大陸已認定發展資訊戰是跨世紀的重大使命，不但致力資訊戰理論研究與科技研發，並具體落實在其建軍備戰上加以驗證，其發展速度之快與影響層面之廣，不僅對台灣、甚至對亞太地區、莫不產生重大衝擊，面對中國大陸全力發展資訊戰的威脅，我國資訊及通訊安全之維護，已成為最重要的主題。

兩岸通資訊安全基礎建設發展可以說都在起步階段，也都各有所長，現階段孰強孰弱難以斷定，可以確定的是，兩岸均將挹注全力推動其安全基礎建設之發展，創造資訊優勢，以現有之資訊及通訊安全措施而言：包括利用資料加密、身分鑑別、電子簽章、防火牆及安全偵測等作為，以防止資料及系統被不法侵入、破壞。惟此安全防護均侷限於局部性，並無整體防護、識別及回復等能力，對國家通資安全之防衛應變嚴重不足。有鑑於此，為統籌強化我國資訊戰防衛能力，國家安全會議於八十九年五月奉　總統指示研提「建立我國通資訊基礎建設安全機制」建議書，並經　總統於八月三十日核定，轉送行政院國家資訊通信發展推動小組（以下簡稱「行政院NICI小組」）規劃辦理。

本計畫因攸關國家安全機制之建立，為爭時效及達成　總統之指示，行政院NICI小組於八十九年九月份起經十二次召集各部會研討相關規劃作業，提出本計畫具體可行方案，並於八十九年十二月二十九日之行政院NICI委員會中提報，獲得全體委員共識及支持，於九十年一月二日面報　院長，經　院長指導後，本計畫之資通安全通報體系即依行政體制於

九十年一月份起運作；配合本次院會將本計畫內容中之任務目標、保護範疇、組織架構、人力需求、預算需求及時程管制等資料於會議中提報後，即轉發各部會確遵執行。

參、目的：

通資訊安全基礎建設發展涵蓋範圍廣泛，舉凡政治、心理、經濟、科技和軍事等各領域，均為敵運用資訊技術手段爭奪資訊優勢的目標，而為確實掌握我國政府機關（機構）及重要民間業者之資訊及網路系統免遭受破壞或不當使用等緊急事故發生時，能迅速作必要之應變處置並在最短時間內回復正常運作，以降低該事故可能帶來之損害；故有必要建立國家層級之通資訊安全指揮機制，並結合內政、外交、國防、財政、教育、法務、經濟、交通等部會及國家安全局，針對電力、電信、金融、交通等國家基礎建設之安全防護，共同研析相關因應作為，為此行政院 NICI 小組特協調各部會積極規劃建立國家通資訊系統通報及應變機制，以為我國通資訊安全提供最佳之保障。

肆、保護範疇：

在通資訊安全的保護議題可概分為下列七個項目：

一、安全管理政策。

二、基礎環境安全。

三、人員管理安全。

四、安全規章法律。
五、硬體設備安全。
六、軟體系統安全。
七、網路通訊安全。

此外，安全的通資訊防護機制必須保護國家的利益與政府的正常運作，例如：金融體系、商務運作、政府服務、水、電、油、瓦斯等供給，緊急救援體系，交通、電信等的正常運作。在軍事方面則包括軍事的佈署能力、運作能力、動員能力以及持久的能力等。在民間方面則能保證不影響民眾的權利與日常生活。

所以在資訊戰進行時，我國至少必須能維持下面體系的正常運作：
一、政府的正常運作。
二、軍事力量的維持。
三、救援體系的正常運作。
四、人民日常生活必需品(電信、水、電、油、瓦斯、食物)的正常供給。
五、金融體系的正常運作。
六、商業的繼續進行。

當然，百分之百的通資訊安全目標是無法達成的。為確保通資訊基礎建設的安全性，防禦性通資訊系統已成為先進國家通資訊安全研究的重心之一，防禦性通資訊系統安全的目標在於：「從確保通資訊資源的合法存取，到在所有可能遭受通資訊攻擊的階段，提供完整(Complete)、未中斷的通資訊系統運作。」，其功能性典範(Functional Paradigm)可經由「防護(Resistance)」、「識別(Recognition)」、「回復(Recovery)」這三個措施加以說明。

目前我國通資訊基礎建設安全的弱點，可以從防護、識別與回復三方面來說明：

(一)、通資訊基礎建設安全的防護面：

通資訊基礎建設安全之防護以抵禦攻擊為主，並以通資訊系統生存為目標。植基於此，我國除軍事單位外，其他機構少有「資訊邊疆(Information Frontier)」的概念。而先進國家已推動近二十年的通資訊系統安全認證體系中之檢測技術已成為通資訊系統安全防護基礎之存活度(Survivability)檢驗之基礎，而我國尚在萌芽中，此可顯示出我國通資訊基礎建設安全防護面之不足。

(二)、通資訊基礎建設安全之識別面：

快速且正確的偵測與辨識出惡意的使用行為對通資訊系統的存活是相當重要的，無論防護措施多完善，在不斷地發展、改進與變化中之通資訊基礎建設，要修護所有的安全

性脆弱點亦相當困難。既然無法做到全面的安全防護，就必須謹慎地注意可能出現危機癥兆的任何異常活動報告。知己知彼方能百戰不殆，我國基本的脆弱點分析亦僅少數幾個機構在試行中而已。無論是在知已還是知彼的通資訊基礎建設安全識別面之加強，已是我國通資訊安全的重要首務。

(三)、通資訊基礎建設安全之回復面：

在資訊入侵事件中，保護系統免於遭受攻擊是必要的工作，但也必須體認到不是所有的攻擊都可以在一開始便躲掉，有些攻擊是無可避免的，所以做好攻擊發生後的辨識並採取適當的回復是必要的準備。當先進國家已進入電腦與資訊系統鑑識(Forensics)技術的研發時，我國尚常發生因入侵事件發生後無法正確重建資料而誤判嫌犯的案例。如何建立蒐集稽核線索與入侵活動偵測的資料、分析與闡釋這些資料、為法律目的證據重建之鑑識技能，以及在遭受攻擊後快速且完整地回復通資訊系統等回復技能，均是我國通資訊基礎建設安全回復面必須面對的問題。

伍、計畫目標：

一、積極防衛通資設施，維護國家運行體制。

二、建立通資安全優勢，提升國家競爭力量。

三、堅實通資安全建設，健全網路社群發展。

四、主動偵測安全威脅，降低實質危害因素。
五、建構安全通報體系，強化事前預警機制。
六、保障民眾隱私權益，促進網路多元發展。
七、增強執法專業能力，有效遏止網路犯罪。

陸、執行要點：

一、編組專職人員統合推動通資訊安全工作及協調組織。
二、律定通資訊安全組織職掌及分工。
三、建立通資訊安全危機事件通報及預警機制。
四、彙整及發布通報相關資訊，供各機關參考運用及早作好預防措施。
五、執行國家重要通資訊基礎設施之安全防護，建立主動偵防能力。
六、策訂重要通資訊設施安全規範及回復重建措施。
七、檢討及增修訂通資訊安全相關法令、訂定通資訊安全技術標準及規範，建立產品檢驗及保證機制。
八、推動通資訊安全學術研究及關鍵技術研發。
九、加強通資訊安全人力培訓及觀念宣導。
十、提升執法機關之偵防能力及人力，建立跨國及區域性合作機制。

柒、行政院國家資通安全會報設置要點：（行政院台九十經字第〇六九五七九－一函核定）

一、行政院(以下簡稱本院)為積極推動國家資訊通信安全政策，加速建構國家資訊通信安全環境，提昇國家競爭力，特設國家資通安全會報（以下簡稱本會報），組織架構如附圖一。

二、本會報設綜合業務組（本院科技顧問組負責）、標準規範工作組（經濟部負責）、稽核服務工作組(本院主計處電子中心負責)、資訊蒐集工作組(本院國家科學委員會負責)、網路犯罪工作組（法務部負責）、危機通報工作組（本院主計處電子中心負責）及技術服務中心（經濟部負責），負責下列事項之政策研究、協調、聯繫、策劃、整合及推動：

（一）、提高資通安全決策層次，編組專職人員統合推動協調相關工作。

（二）、強化政府資通安全防護，律定資通安全組織職掌及分工。

（三）、建立資通安全危機事件通報及預警機制，建立全民防護體系。

（四）、彙整及發布相關資訊供各機關參考並妥採預防措施。

（五）、執行國家重要資訊通信基礎設施之安全防護，建立主動偵防能力。

（六）、策訂重要資訊通信設施安全規範及回復重建措施。

（七）、檢討及增修訂資通安全相關法令、訂定資通安全技術標準及規範，建立產品檢驗及保證機制。

（八）、推動資通安全學術研究及關鍵技術研發，促進資通安全產業發展。

（九）、加強資通安全人力培訓及觀念宣導。

（十）、提升執法機關之偵防能力及人力，建立跨國及區域性合作機制。

（十一）、推動國家憑證認證體系，建立安全及可信賴之認證環境。

（十二）、督導資通安全計劃之執行。

三、本會報置總召集一人，由本院院長兼任；副總召集人一人，由本院副院長兼任；置委員十五人，由院長指派政務委員或有關機關首長兼任，人員如附表一。

四、本會報置執行長一人，由本院國家資訊通信發展推動小組總召集人兼任，承總召集人之命，綜理本會報有關業務；置副執行長二人，分別由國家安全會議派員及本院主計處電子處理資料中心主任兼任，襄助執行長綜理本會報有關業務；本會報幕僚作業，由綜合業務組負責。

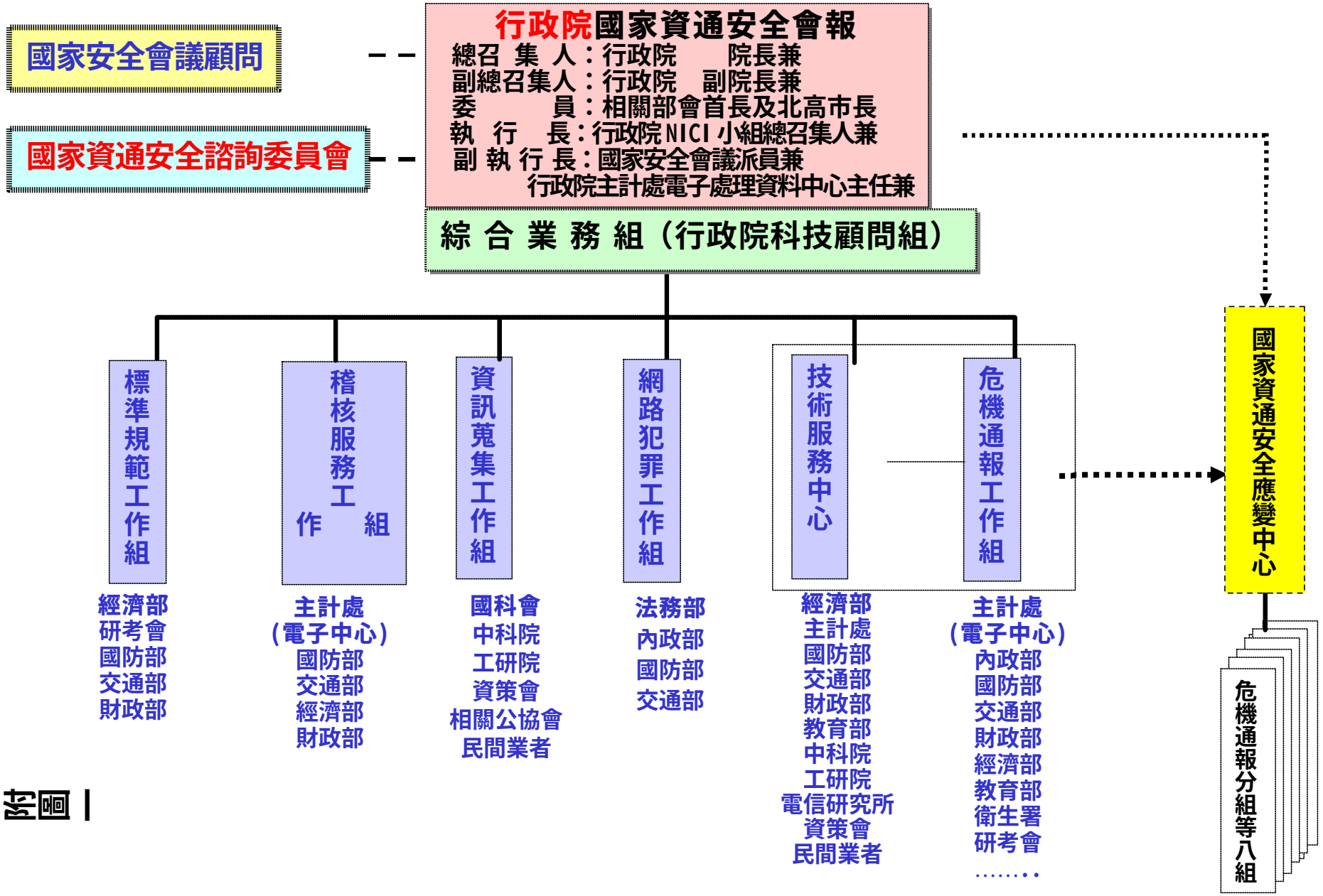
五、各工作組得置召集人一人，由主責機關之委員擔任之，並依需要訂定各組作業規範。

六、本會報為廣徵產學研各界學者專家意見，得設國家資通安全諮詢委員會，以有效推動資通安全技術相關工作，其作業注意事項另定之。

七、本會報總召集人、副總召集人、執行長、副執行長、委員及各組召集人，均為無給職。

八、本會報應定期（每半年至少一次）召開會議，審核及評估通資安全政策；有重大議題時，得視業務需要召開臨時會議。

行政院國家資通安全會報組織運作架構



表圖 1

行政院國家資通安全會報委員

單　　位	職　　稱	備　　考
行政院	院長	國家資通安全會報總召集人
行政院	副院長	國家資通安全會報副總召集人
行政院	政務委員	國家資通安全會報執行長
國家安全會議	諮詢委員	國家資通安全會報副執行長
行政院主計處電子中心	主任	國家資通安全會報副執行長
行政院	秘書長	委員
國家安全局	局長	委員
內政部	部長	委員
國防部	部長	委員
財政部	部長	委員
法務部	部長	委員
經濟部	部長	委員
交通部	部長	委員
教育部	部長	委員
行政院主計處	主計長	委員
研考會	主任委員	委員
國科會	主任委員	委員
衛生署	署長	委員
台北市	市長	委員
高雄市	市長	委員
總召集人一人、副總召集人一人、執行長一人、副執行長二人、委員十五人、合計廿人。		

九、本會報下各單位職掌：

（一）、綜合業務組（辦理單位：本院科技顧問組主責、本會報下各工作組配合協辦）

１、統籌國家層級資通安全基礎建設規劃作業。

２、負責資通安全會報相關行政協調作業綜合業務。

３、統合推動通資訊安全基礎建設工作及協調組織運作業務。

４、負責資通安全計劃執行管理與考核。

（二）、技術服務中心運作規劃示意圖如附圖二（辦理單位：經濟部主責、本院主計處、國防部、交通部、財政部、教育部、中科院、資策會、工研院配合協辦）

１、負責通資訊安全基礎建設技術規劃支援作業。

２、負責資通安全人力培訓。

３、負責資通安全基礎宣導及舉辦相關技術研討會。

４、建置資通安全宣導及技術網站並蒐集最新通資訊安全相關技術。

５、編訂資通安全基本作業手冊並協助各機關訂定作業系統安全等級。

６、推動資通安全關鍵技術研發及學術研究並協助發展我國通資訊安全相關產業。

７、辦理資通安全攻防模擬環境建置及相關訓練等事項。

８、建構資通安全區域聯防技術服務機制。

９、提供各界資通安全技術諮詢服務。

技術服務中心運作規劃示意圖

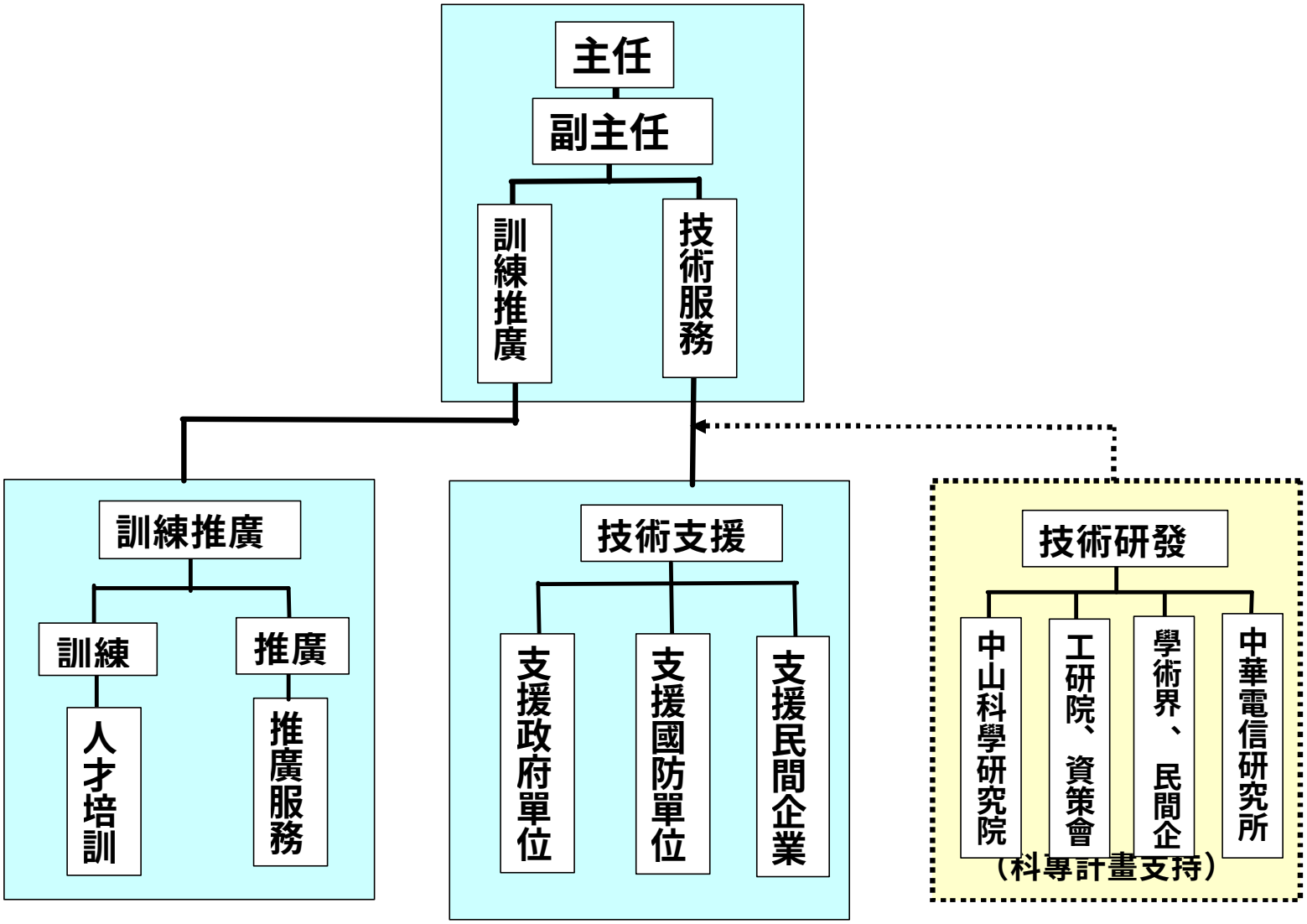


圖1-2

（三）、標準規範工作組（辦理單位：經濟部主責、本院研考會、國防部、交通部、財政部配合協辦）

１、訂定資通安全技術標準。

２、訂定各機關辦理資通安全有關作業規範。

３、規劃建置資通安全驗證方法

４、規劃建置資通安全認證程序。

（四）、稽核服務工作組（辦理單位：本院主計處主責、國防部、交通部、經濟部、財政部配合協辦）

１、培訓資通安全稽核人力。

２、協助各機關訂定作業系統安全等級

３、選定資通安全等級高之作業系統。

４、每年對重要系統不定期辦理資通安全稽核作業。

５、彙編重要系統資通安全稽核報告。

（五）、資訊蒐集工作組（辦理單位：本院國科會主責、中科院、工研院、資策會、相關公協會及民間業者配合協辦）

１、蒐集國內外資通安全相關資訊。

２、建置資通安全資料庫。

３、傳布及推廣資通安全資訊並主動提供服務。

（六）、網路犯罪工作組（辦理單位：法務部主責、調查局、內政部、國防部、交通部配合協辦）

１、指派人員負責資通安全犯罪事件偵查工作。

２、培訓執法人員辦理資通安全有關偵防能力。

３、建立跨國及區域性合作偵防機制。

４、配合研修網路犯罪相關法規。

（七）、危機通報工作組（辦理單位：本院主計處主責、內政部、國防部、交通部、經濟部、財政部、本院研考會配合協辦）

１、建立資通安全事件通報處理程序。

２、建置資通安全事件通報網站。

３、建立資通安全事件各安全等級之有關緊急應變程序。

４、協調技術服務中心提供技術服務。

５、建立事前、事中及事後各項資通安全事項通報預警及應變復原機制。

６、統計發布我國資通安全事件及應變程序。

十、國家資通安全應變中心組織架構及運作：

（一）、於國家資通安全會報下設置「國家資通安全應變中心」（以下簡稱應變中心），組織運作架構如附圖三，應變中心係一任務編組，召集人由本院NICI小組總召集人兼任，副召集人三員分別由國家安全會議派員兼任、本院主計處電子中心主任兼任及行政本院科技顧問組執行秘書兼任。

（二）、資通安全等級概分為四級：

『A』級：影響公共安全、社會秩序、人民生命財產。

『B』級：系統停頓，業務無法運作。

『C』級：業務中斷，影響系統效率。

『D』級：業務短暫停頓，可立即修復。

（三）、除資通安全通報體系於平時依行政體制運作外，緊急狀況應變或任務需要時由危機通報工作組負責籌劃運作，並依需要進駐應變中心，應變中心下設危機通報分組、國防體系分組、行政機關分組、學術機構分組、事業機構分組（一）、事業機構分組（二）、事業機構分組（三）及事業機構分組（四）等八個分組，分別

由本院主計處、國防部、本院研考會、教育部、經濟部、交通部、財政部及衛生署等單位擔任各分組召集工作。

（四）、影響等級『B』級（含）以下時，由危機通報分組負責通報各副召集人處理，並依需要由副召集人召集各分組及相關單位召開緊急應變會議或立即進駐應變中心處理全般狀況；當危機通報分組回報影響等級達到『A』級時，由應變中心副召集人立即通報召集人, 並即刻召集各分組及相關單位進駐應變中心召開緊急應變會議處理全般狀況。

（五）、各分組每季定期召開會議檢討工作執行情形，並負責督導各體系之推動工作，以執行我國資通安全基礎建設政策。

國家資通安全應變中心

召　集　人：國家資通安全會報執行長兼
副召集人：行政院科技顧問組執行秘書兼
副召集人：行政院主計處電子中心主任兼
副召集人：國家安全會議派員兼

危機通報工作組（行政院主計處電子中心）

國家資通安全會報
技術服務中心

- **危機通報分組**
  召集單位：主計處
  一、規劃通報應變作業計畫
  二、建立通報體系
  三、辦理通報宣導研討會
  四、建立通報網站
  五、彙整及發布通報資訊
- **國防體系分組**
  召集單位：國防部
  負責國防體系資通安全危機事件通報及相關應變事項
- **行政機構分組**
  召集單位：研考會
  負責政府行政機關資通安全危機事件通報及相關應變事項
- **學術機構分組**
  召集單位：教育部
  負責學校及研究機關資通安全危機事件通報及相關應變事項
- **事業機構分組（一）**
  召集單位：經濟部
  負責電力、石油、自來水、瓦斯及主管之重要目的事業機構資通安全危機事件通報及相關應變事項
- **事業機構分組（二）**
  召集單位：交通部
  負責網路通信、航管、交通及主管之重要目的事業機構資通安全危機事件通報及相關應變事項
- **事業機構分組（三）**
  召集單位：財政部
  負責金融、證卷、關貿及主管之重要目的事業機構資通安全危機事件通報及相關應變事項
- **事業機構分組（四）**
  召集單位：衛生署
  負責醫療及主管之重要目的事業機構資通安全危機事件通報及相關應變事項

十一、國家資通安全應變中心各分組職掌：

危機通報工作組擔任國家資通安全應變中心總召集單位，並協調技術服務中心兼負中心幕僚作業，技術服務中心應負責支援應變中心軟、硬體設施規劃建置作業，危機通報分組應負責資通安全事前、事中、事後預警及應變復原機制之建立、彙總各分組有關資通安全事件通報、分析報告及提供相關技術支援等事項。

（一）危機通報分組：（本院主計處擔任召集單位）

負責規劃通報作業計畫、建立通報體系、辦理通報宣導講習、建立通報網站、彙整、發布通報資訊。

（二）國防體系分組：（國防部擔任召集單位）

負責國防體系有關通資訊安全危機事件通報及相關應變事項。

（三）行政機關分組：（本院研考會擔任召集單位）

負責政府行政機關有關通資訊安全危機事件通報及相關應變事項。

（四）學術機構分組：（教育部擔任召集單位）

負責學校及研究機構有關通資訊安全危機事件通報及相關應變事項。

（五）事業機構分組（一）：（經濟部擔任召集單位）

負責電力、石油、自來水、瓦斯及主管之重要目的事業機構資通安全危機事件通報及相關應變事項。

（六）事業機構分組（二）：（交通部擔任召集單位）

負責網路通信、航管、交通及主管之重要目的事業機構資通安全危機事件通報及相關應變事項。

（七）事業機構分組（三）：（財政部擔任召集單位）

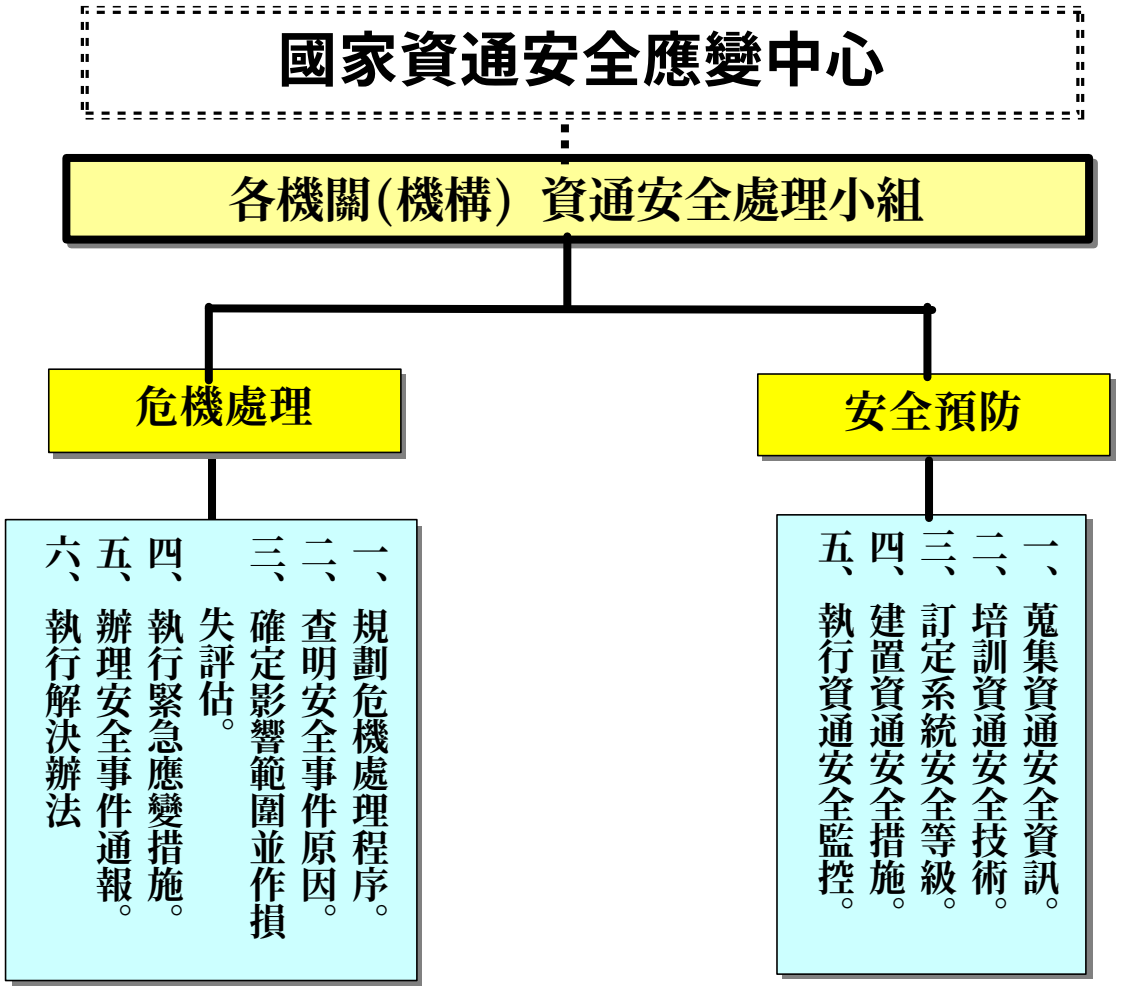
負責金融、證卷、關貿及主管之重要目的事業機構資通安全危機事件通報及相關應變事項。

（八）事業機構分組（四）：（衛生署擔任召集單位）

負責醫療及主管之重要目的事業機構資通安全危機事件通報及相關應變事項。

十二、政府各機關（機構）應成立「資通安全處理小組」，亦屬常態任務編組，負責處理安全預防及危機處理相關事宜，其組織架構及職掌如附圖四。

政府各機關（機構）「資通安全處理小組」組織架構及職掌



圖表

十三、各機關資通安全處理小組職掌：

(一)、安全預防：負責蒐集資通安全資訊、培訓資通安全技術、訂定各機關系統安全等級、建置資通安全措施、執行資通安全監控等事項。

(二)、危機處理：負責規劃危機處理程序、查明危機事件原因、確定影響範圍並作損失評估、執行緊急應變措施、辦理危機通報、執行解決辦法等事項。

捌、運作方式：

一、危機通報工作組應建立「資通安全通報聯絡網」，由中央各部、會、行、處、局、署、院轄市及縣（市）政府等機關指定聯絡人員，並將基本資料請依附表二格式填妥，逕送各分組召集單位，彙整後由本院主計處彙整建檔備用。

二、國家資通安全應變中心於各資通安全等級緊急狀況應變時，由危機通報工作組負責運作編成，並協調各分組及技術服務中心與聯繫各部會、業務單位之安全處理小組通力合作，以解決危機事件。

三、各機關應將發生資通安全事件之事實、可能影響之範圍、採取之應變措施等事項，即時填具「資通安全事件通報單」，如附表三，並透過上網、電話、傳真或電子郵件等方式傳送至「國家資通安全應變中心」及其主管機關；當系統回復正常運作時，亦需將解決辦法透過「資通安全事件通報單」傳送，以解除列管。

四、各機關如因資通安全事故發生且危及人員生命或設備遭到破壞等涉及民刑事案件時，應及時通報檢調單位請求處理；如引發重大災害時，同時向現行災害防救體系提報，請求支援處理。

五、國家資通安全應變中心對於需要支援之單位，視需要項目，由危機通報工作組及技術服務中心協調各工作組、分組提供支援。

六、資訊蒐集工作組及技術服務中心應蒐集彙整資通安全通報資訊，協調危機通報工作組及技術服務中心主動於有關網站公告或透過「資通安全通報聯絡網」通報相關單位，並由國家資通安全應變中心副召集人（本院主計處電子中心主任）透過媒體對外發布有關訊息。

七、技術服務中心應透過資通安全區域聯防技術服務機制及提供技術支援各個通報及應變體系處理危機事件。

八、國家資通安全會報應定期（每半年至少乙次）召開會議審核與評估通資訊安全政策。

九、危機通報工作組應依資通安全事件通報及應變處理作業流程，如附圖五，彙總資通安全事件、分析報告，並評估相關通資訊安全政策。

（單位全銜）　資通安全通報網聯絡人員調查表

姓　名	職　稱	電　話	傳真電話	行動電話	電　子　信　箱

附表11

機關(機構)名稱__資通安全事件通報單

洽詢電話：_____ 傳真：_____

e-mail: _____ 或逕送：台北市廣州街二號

填報時間：____年____月____日____時____分 編號：_____

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱：_____ E-MAIL：_____

聯絡人：_____電話：_____傳真：_____

二、資通安全事件通報事項：

1.事件發生時間：____年____月____日____時____分

2.主機(伺服器)資料：

◎IP 位址(IP Address)：_____

◎網域名稱(Domain name)：_____

◎ 主機(伺服器)廠牌、機型：_____

◎ 作業系統名稱、版本、序號：_____

◎ 網際網路資訊位址(Web URL)：_____

◎ 已裝置之安全機制：_____

3．資通安全事件資料：

◎ 安全等級：□『A』級；□『B』級；□『C』級；□『D』級

◎ 影響等級：□ 『A』級：影響公共安全、社會秩序、人民生命財產。

□ 『B』級：系統停頓，業務無法運作。

□ 『C』級：業務中斷，影響系統效率。

□ 『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 可能影響範圍及損失評估：

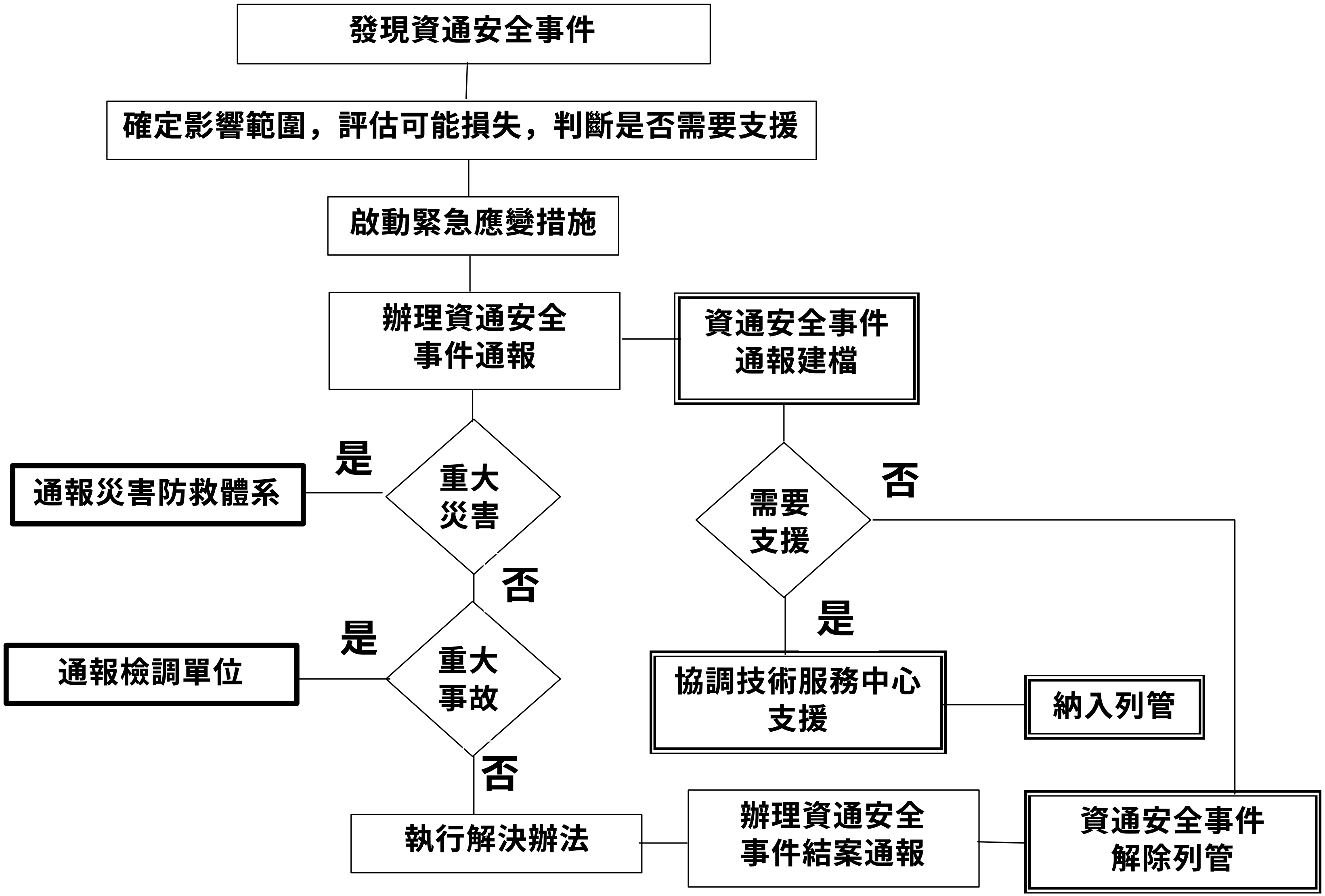
◎ 應變措施：

三、期望支援項目：

四、解決辦法：

五、已解決時間：____年____月____日____時____分

資通安全事件通報及應變作業流程



附圖五

玖、資源需求與預定時程進度：

一、資源需求：

本計畫之細部規劃將由各相關工作組提送工作計畫書後，提出相關預算需求，並檢討由原有單位預算自行檢討支應或另行呈報籌措預算來源。

二、綜合業務組與技術服務中心工作推動人力來源需求規劃：

技術服務中心編設人員依年度及中程計畫職掌任務需求而定，綜合業務組人員及所需資源由技術服務中心及相關單位檢討支援，負責資通安全相關規劃、推廣訓練及技術服務等相關工作。

三、預定時程管制：

(一)、第一階段執行計畫（九十年一月一日｜九十一年十二月三十一日）
—於民國九十一年十二月前建立國家資通安全基本防護能力。

1、九十年一月完成通報體系建立。
2、成立行政院資通安全會報(已於九十年一月院會通過後編成)。
3、成立國家資通安全應變中心(已於九十年一月院會通過後編成)。
4、九十年十二月三十一日前完成我國資通技術研發策略及系統弱點評估。
5、九十年十二月三十一日前完成認證、保證、信息分享體系建立。
6、九十一年十二月三十一日前完成政府 PKI 基礎建設(配合電子化政府完成 CA 認證機制)。
7、各單位規劃第二階段執行計畫（初稿於九十一年八月三十一日前完成）。
8、綜合業務組提出資通安全推動方案報告(預計九十一年九月前完成)。

(二)、第二階段執行計畫（九十二年一月一日｜九十三年十二月三十一日）

—於民國九十三年十二月前建立國家資通安全整體防護體系。

１、九十二年十二月三十一日前完成入侵偵防及緊急應變計畫。

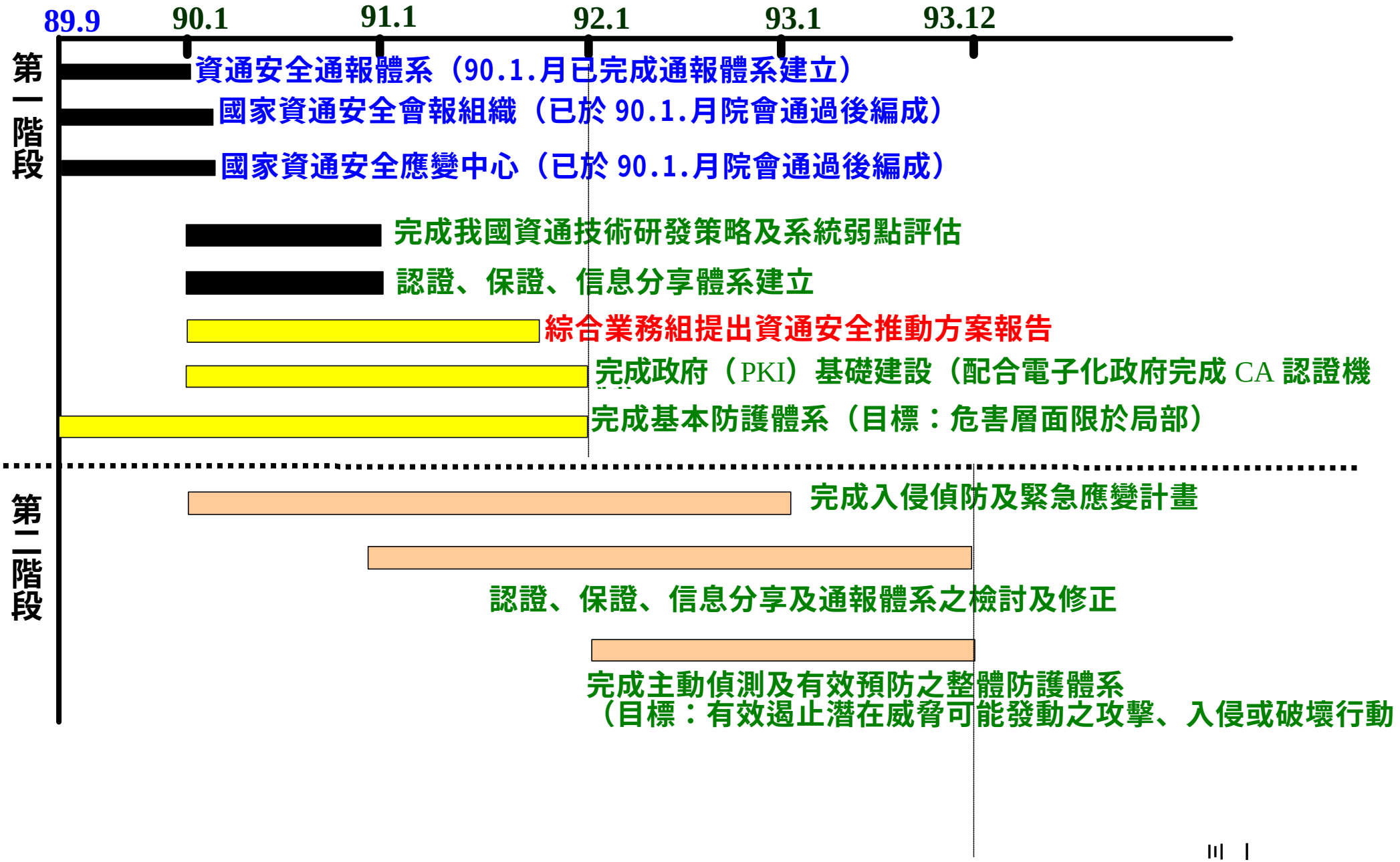
２、九十三年十二月三十一日前完成認證、保證、信息分享及通報體系之檢討及修正。

３、九十三年十二月三十一日完成主動偵測及有效預防之整體防護體系。

（目標：有效遏止潛在威脅可能發動之攻擊、入侵或破壞行動）

４、九十三年十二月三十一日完成建立防護體系之計畫目標。

四、主要工作預定時程


89.9
90.1
91.1
92.1
93.1
93.12
第一階段
資通安全通報體系（90.1.月已完成通報體系建立）
國家資通安全會報組織（已於 90.1.月院會通過後編成）
國家資通安全應變中心（已於 90.1.月院會通過後編成）
完成我國資通技術研發策略及系統弱點評估
認證、保證、信息分享體系建立
綜合業務組提出資通安全推動方案報告
完成政府（PKI）基礎建設（配合電子化政府完成 CA 認證機
完成基本防護體系（目標：危害層面限於局部）
第二階段
完成入侵偵防及緊急應變計畫
認證、保證、信息分享及通報體系之檢討及修正
完成主動偵測及有效預防之整體防護體系
（目標：有效遏止潛在威脅可能發動之攻擊、入侵或破壞行動