美國國土安全部網路安全及基礎設施安全署 (CISA)角色之初探---兼論對台灣之啟示

柯雨瑞[1]　楊語柔[2]　梁雅涵[3]

目次

中文摘要

在美國國土安全部之下，設有一個專責於網路安全及基礎設施安全之專門機構，正式名稱為網路安全及基礎設施安全署(Cybersecurity & Infrastructure Security Agency，簡稱為 CISA)，該署指出：沒有任何實體，能夠單獨保護網路之空間安全。

CISA 認為在全球互聯的世界中，關鍵基礎設施和生活方式面臨著廣泛、多元化的重大風險，並在現實世界中產生重大後果。CISA 成立聯合網路防禦協作組織平台（Joint Cyber Defense Collaborative，JCDC），以統一來自各個機關、組織的網路防衛者。這個多元化的團隊 JCDC 會主動收集、分析和共享可供實際操作的網路風險資訊，以實現同步、整體的網路安全規劃、網路防禦和回應。

再者，CISA 亦頒布 2023-2025 年戰略計劃，此一計劃是自 CISA 於 2018 年成立以來，該機構的第一個涉及網路安全及其基礎設施安全之全面戰略計劃。這是 CISA 組織發展的一個重要里程碑：CISA 戰略計劃將重點關注並指導該機構在未來 3 年之發展。2023-2025 年戰略計劃將使 CISA 在未來三年內，推動四個關鍵領域的變革：1、CISA 將引領美國政府之努力，確保網路空間的防禦和彈性；2、其次，CISA 將降低美國關鍵基礎設施的風險，增強其彈性；3、加強全國作戰協作和情資共享；4、CISA 將通過集成的模式，結合職能、能力和勞動力，統一成為一個事權合一之 CISA。

有關於本文之建議部分，如下所述：一、強化國家資通安全之組織架構；二、建構一個事權統一之網路安全防護主管機關；三、建構優質化之組織

[1]柯雨瑞，中央警察大學國境警察學系暨研究所專任教授，中央警察大學犯罪防治研究所法學博士。研究專長：國境執法、入出國(境)管理、跨國(境)犯罪及移民政策及人口販運等。

[2] 楊語柔，現為內政部警政署航空警察局後勤科巡官，中央警察大學國境警察研究所碩士生。

[3] 梁雅涵，現服務於臺南市政府警察局麻豆分局，中央警察大學國境警察研究所碩士生。

文化；四、建構一個事權統一之基礎設施安全防護主管機關；五、打造公私協力之防護安全網；六、健全化情資分享機制；七、保障隱私權、人格權、資訊權；八、打造優質工作環境，以延聘、培訓、留用資安人才。

壹、前言

美國政府有鑒於網路安全及基礎設施安全防護之重要性日增，遂於 **2018** 年，在美國國土安全部之下，成立一個新機關，名為網路安全及基礎設施安全署 **(CISA)**，就全美網路安全及基礎設施安全防護之區塊而言，**CISA** 之重要性不可言諭。**CISA** 正式成立之後，即積極任事，**CISA** 提出一個全球網路安全及基礎設施安全方案，簡稱為 **CISA Global**，此一方案之構想，**CISA** 將強化與國際合作夥伴情資交流、網路安全合作之量能，俾以履行 **CISA** 的責任、執行 **CISA** 的工作，並在 **CISA** 的任務領域內，建立統一全球網路安全及其基礎設施安全的努力。該戰略詳細說明了 **CISA** 的國際網路安全願景，並承諾網路安全所須實現之 **4** 個目標：**1**、推進業務合作；**2.** 建構合作夥伴能力；**3.** 通過利害關係人的參與，增強外展合作；**4.** 塑造全球政策生態系統。

涉及台灣網路安全及基礎設施安全防護的主管機關、組織，相關權責分散於各個單位。台灣在網路安全及其基礎設施安全防護的組織架構方面，並未向美國 **CISA** 一般，將網路安全及基礎設施安全權責，全部集中於 **CISA** 組織。

在網路安全防護之主管機關組織架構之區塊，國家資通安全戰略報告----資安即國安 **2.0** 係由總統府國家安全會議所公告及頒行之，是以，最高層級之組織，有可能係為總統府國家安全會議資通安全辦公室（簡稱資通辦）。在行政院之層級，則分別設置行政院資安處、行政院國家資通安全會報。行政院國家資通安全會報之諮詢單位，係為行政院資通安全諮詢會；而國家資通安全會報之幕僚單位，係為行政院數位發展部(資通安全署)。再者，在基礎設施安全防護的區塊，基礎設施安全防護的主管機關、協調機關、組織、相關權責分散於各個單位。由於相關權責單位未統一，倘若各單位之意見不一，上述相關機關、單位之間之意見與構想，如何進行有效之整合，值得詳加重視。

貳、美國國土安全部網路安全及基礎設施安全署 **(CISA)** 角色、任務、職掌之介紹

一、美國國土安全部網路安全及關鍵基礎設施安全署(CISA)之關鍵角色[4]

（一）是聯邦網路的營運主管機關：

CISA 主責於聯邦網路安全，負責整個聯邦網路安全的管理，與預算辦公室密切合作，保護和保衛美國的聯邦政府網路。**CISA** 尚協調國家網路防禦的執行，專責於重大網路事件的回應，並確保在聯邦、非聯邦和民營部門合作夥伴之間，共享及時可操作的情資。

（二）是關鍵基礎設施安全韌性及彈性的國家協調員：

CISA 著眼於整個威脅情況之預防與回應，並與政府和合作夥伴一起防禦當今的各式威脅，同時保護美國國家的關鍵基礎設施免受攻擊與威脅。

（三）乃專為協作和夥伴關係而成立：

[4] **Cybersecurity and Infrastructure Security Agency(2022)。About CISA。**上網瀏覽日期：**2022** 年 **11** 月 **13** 日。**https://www.cisa.gov/about-cisa**。

CISA 成立於 **2018** 年，旨在跨公共和民營部門開展工作，通過與政府、協力夥伴、學術和國際合作夥伴的合作，挑戰傳統的執法方式。隨著威脅的不斷發展，美國政府知道沒有一個組織或實體，能夠解決應對關鍵基礎設施的網路和實體之威脅。通過匯集執法部門的洞察力和能力，**CISA** 可以建立集體防禦能量，抵禦所面臨的威脅。

網路安全及關鍵基礎設施安全署**(CISA)**領導美國政府努力了解、管理和降低網路和實體基礎設施的風險。將政府的利害相關者相互聯繫串聯起來，並與資源、分析和工具進行結合，以幫助彼此建立自己的網路、通信、實體安全和彈性，從而確保為美國人民提供安全和彈性的基礎設施。於 **2021** 年，展示了 **CISA** 在 **2021** 年執行其使命的關鍵典範，包括在該機構推進戰略優先事項，以維護國家安全和有韌性的基礎設施的里程碑和成就。

2022 年 **9** 月初，**CISA** 發布 **2023** 年至 **2025** 年 **CISA** 戰略計畫，這是自該機構於 **2018** 年成立以來的第一個全面戰略計畫。該戰略計畫針對的風險環境，包括國家面臨的日益相互關聯的全球網路空間 **24/7/365** 之非對稱網路威脅，此種威脅，具有大規模的世界影響力，不容小覷。

二、美國國土安全部網路安全及關鍵基礎設施安全署 **(CISA)**之關鍵任務和使命：

（一）強化網路之安全性與韌性[5]：

隨著全球化之資訊技術越來越提升與實體基礎設施營運之整合，發生大規模或重大危害後果事件的風險增加，這些事件可能造成劇烈損害或破壞美國經濟和數百萬美國人日常生活所依賴的日常生活服務。鑑於網路事件產生的風險和潛在後果，**CISA** 可針對複雜網路產生之風險危機，提出相對應之預防措施與解決方式，以強化網路空間的安全性和韌性。

(二) 打擊網路犯罪[6]：

當今世界因全球化現象比以往任何時候都更加相互關聯。然而，儘管具有所有優勢，但增加的連接性會導致竊盜、欺詐和濫用的風險產生。隨著美國人越來越依賴現代科技技術，美國人變得更容易受到網路攻擊，例如企業安全漏洞、魚叉式網路釣魚和社交媒體欺詐。互補的網路安全和執法能力，對於保護網路空間安全至關重要。

執法部門通過調查範圍廣泛的網路犯罪（從竊盜、欺詐到剝削兒童等）以及逮捕和起訴行為人，在實現國家的網路安全目標方面發揮著重要作用。國土安全部 **(Department of Homeland Security, DHS)** 與其他聯邦機構合作，開展具有影響力的刑事調查，以打擊網路犯罪分子，優先招聘和培訓技術專家，制定標準化方法，並廣泛分享網路回應的最佳實踐和工具。刑事調查員和網路安全專家們對惡意行為者所使用的技術，及特定的網路弱點與漏洞進行深入探討，以有效地回應和調查網路攻擊事件。

另外，美國特勤局（**United States Secret Service, USSS**）和美國移民和海關執法局**(U.S. Immigration and Customs Enforcement, ICE)**等美國國土安全部**(Department of Homeland Security, DHS)**所屬之執法部門設有專門打擊網路犯

---

[5] **Cybersecurity and Infrastructure Security Agency(2022)。Cybersecurity。上網瀏覽日期：2022** 年 **11** 月 **13** 日。**https://www.cisa.gov/cybersecurity**。

[6] **Cybersecurity and Infrastructure Security Agency(2022)。Combating Cyber Crime。上網瀏覽日期：2022** 年 **11** 月 **13** 日。**https://www.cisa.gov/combating-cyber-crime**。

罪的專門部門。

（三）保護聯邦網路[7]：

聯邦機關依靠資訊技術(Information Technology, IT)系統和計算機網路進行基本操作。這些系統面臨著各式各樣的網路威脅，從不成熟的駭客到使用最先進入侵技術的入侵者。許多惡意攻擊旨在竊取資訊並破壞、拒絕訪問、降級或破壞關鍵資訊系統。

網路安全及關鍵基礎設施安全署(CISA)與每個聯邦文官部門和機構合作，採用以風險為基礎和能夠有效應對不斷變化（對網路與關鍵基礎設施造成威脅）的共同政策和最佳實踐。由於系統受到保護，因此可以在檢測到威脅事件時，內部機器會自動地發出警報，以協助保護政府資訊技術機關和民營部門的網路。CISA 將通過戰略性採購工具和服務，協助改變聯邦機構管理網路的方式，從而提高聯邦網路安全採購的速度和成本效益，並允許一致地應用最佳實踐之模式與方法。

其方式包含在線上交換（Exchange Online）的雲端式傳訊平臺中切換到新式身分驗證、建立安全雲端業務應用程序(Secure Cloud Business Applications)項目和聯邦機構 5G 技術採用等。

（四）保護重大關鍵基礎設施[8]：

國土安全部 (Department of Homeland Security, DHS)採用風險預警、防制全般危害的方法，保護網路空間中的關鍵基礎設施，強調保護隱私和公民自由、透明和可訪問的安全流程，以及建置集體行動的國內和國際夥伴關係。

國土安全部與特定機構、其他聯邦機構和民營部門合作夥伴進行協調，分享有關網路威脅和漏洞的資訊和分析成果，並更全面地了解美國全國基礎設施系統的相互依賴性。這種預防、防範、減緩、回應、調查和從網路事件中復原的集體方法，除了須優先考慮能滿足合作夥伴的需求，與利害關係夥伴們日益認識到網路和實體安全相互依存之危害性，還須使彼此成為其風險管理戰略的核心協力夥伴。

CISA 中央執法部門的使命是在於能使 CISA 成為國家第一網路防禦、事件回應和營運集成中心的角色，降低系統性網路安全和通信挑戰的風險。自 2009 年以來，CISA 中央執法部門一直是網路和通信資訊、技術專長、營運專責，透過營運 24/7 全天候情勢感知、分析和事件回應的國家中心。

CISA 中央執法部門的工業控制系統（CISA Central Industrial Control Systems）與執法機構和情報群進行合作，並協調聯邦、州、地方和政府及控制系統所有者、營運商和供應商之間，致力於降低所有關鍵基礎設施部門內部和跨部門的風險。CISA 中央執法部門的工業控制系統（CISA Central Industrial Control Systems）內部的網路安全和基礎設施保護專家們，通過回應事件和復原服務，分析對關鍵基礎設施的潛在威脅及實體影響，為關鍵系統的所有者和營運商提供幫助。此外，CISA 中央執法部門與國際和民營部門的計算機應急回應小組(Computer Emergency Response Team, CERT)合作，共享控制系統相關的安全和減緩措施。

（五）發出 CISA 之行政通知書[9]：

---

[7] Cybersecurity and Infrastructure Security Agency(2022)。Securing Federal Networks。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/securing-federal-networks。

[8] Cybersecurity and Infrastructure Security Agency(2022)。Protecting Critical Infrastructure。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/protecting-critical-infrastructure。

[9] Cybersecurity and Infrastructure Security Agency(2022)。CISA Administrative Subpoena。上

網路安全及關鍵基礎設施安全署(CISA)夜以繼日地工作，以識別和管理國家大部分關鍵基礎設施系統中的網路安全漏洞。這些努力的一個關鍵要素，包括通知關鍵基礎設施實體系統中的漏洞。但是，有時 CISA 分析師會識別或接收有關易受攻擊系統的資訊信息，但無法確定系統所有者或營運商的聯繫資訊。

根據經美國政府修訂的《國土安全法》第 6 篇第 2209 節第 659 條第 p 項之規範，CISA 有權發出行政通知書，以作成識別和通知處於風險中的法人實體所需的資訊。當 CISA 發現連接到互聯網的系統存在特定安全漏洞，並且有理由相信該安全漏洞與關鍵基礎設施相關，並影響其所涵蓋的設備或系統，但卻無法識別處於風險中的實體時，CISA 有權發出行政通知書。

（六）協調利害相關者之參與[10]：

CISA 的利害相關者參與部(Stakeholder Engagement Division, SED)發展夥伴關係、促進對話、召集利害相關者並提高意識，以幫助 CISA 為美國人民建立一個安全且有彈性的基礎設施。SED 協調利害相關者的參與和夥伴關係，以支持該機構降低國家風險的努力。

三、美國國土安全部網路安全及關鍵基礎設施安全署(CISA)之關鍵組織職掌[11]：

網路安全和基礎設施安全署 (CISA)中央部門可區分為：(一)網路安全部門；(二)基礎設施安全部門；(三)緊急通訊部門；(四)國家風險管理部門；(五)利害相關者參與部門；(六)綜合營運部門等六大部門。CISA 機構組織內包含有主任、副主任、執行董事、參謀長、網路安全執行助理總監、基礎設施安全執行助理總監、緊急通訊執行助理主任、國家風險管理中心助理主任、利害相關者參與部助理主任、綜合營運部助理總監、首席對外事務官、立法事務總監、首席法律顧問、首席營運支持官、勞動力參與主管、首席人力資本官、首席財務官、首席資訊官、首席安全官、首席隱私官、首席技術官、首席收購執行官、首席平等機會官、首席學習官、第 1 至 10 區區域總監、高級選舉安全顧問與戰略、政策和計劃主管等職位。

網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/cisa-administrative-subpoena。

[10] Cybersecurity and Infrastructure Security Agency(2022)。Stakeholder Engagement Division。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/stakeholder-engagement-division。

[11] Cybersecurity and Infrastructure Security Agency(2022)。Leadership。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/leadership。

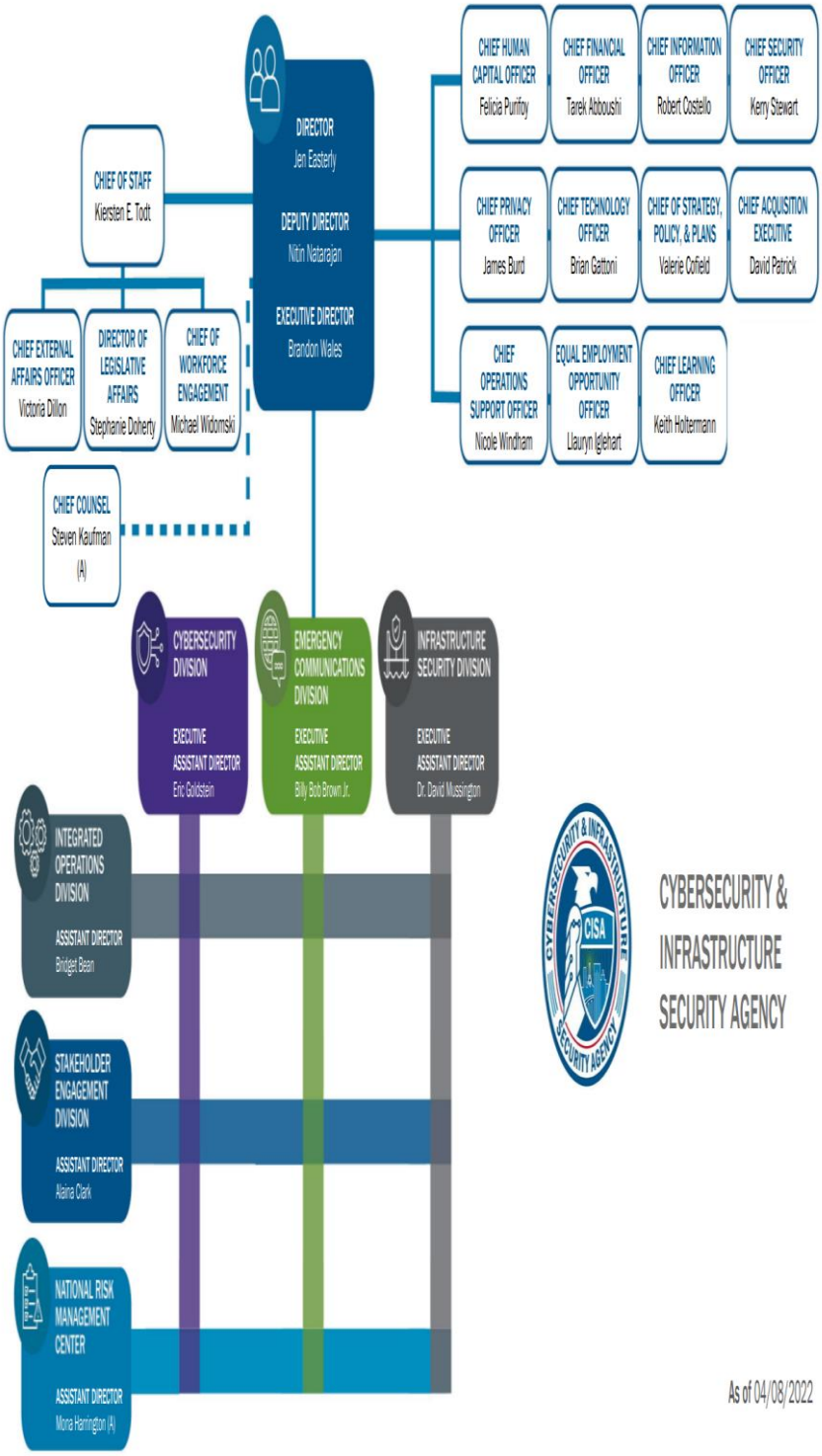

圖 1：ＣＩＳＡ組織職掌架構（CISA Organizational Chart）[12]

資料來源：Cybersecurity and Infrastructure Security Agency(2022)。CISA Organizational Chart。

[12] **Cybersecurity and Infrastructure Security Agency(2022)。CISA Organizational Chart。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/sites/default/files/publications/CISA-orgchart-names_024082020.pdf。**

（一）CISA 中央執法部門：

1.網路安全部門[13]：

CISA 主要係領導國家的戰略和統一工作，俾利加強網路生態系統的安全性、韌性、彈性和勞動力，以保護關鍵基礎設施所提供之服務和美國人的生活方式。

(1)CISA 在網路安全中的作用：

網路空間及關鍵基礎設施容易受到來自實體威脅、網路危害和廣泛風險的影響。複雜的網路參與者和獨立的民族國家利用漏洞竊取資訊和資金，研發如何破壞或威脅網路基本的服務能力。由於多種因素，網路空間特別難以保護：惡意行為者在世界任何地方皆可進行恐攻，及減少複雜網路中的漏洞和後果在預防上具有一定難度。越來越受關注的是關鍵基礎設施所面臨的網路威脅，這些基礎設施越來越容易受到復雜的網路入侵，從而帶來新的風險。鑑於網路事件的風險和潛在後果，**CISA** 加強網路空間的安全性、韌性和彈性，這是一項重要的國土安全任務。

2022 年 **9** 月初，**CISA** 發布 **2023** 年至 **2025** 年 **CISA** 戰略計畫，這是自該機構於 **2018** 年成立以來的第一個全面性戰略計畫。該戰略計畫針對的風險環境包括國家面臨的日益相互關聯的全球網路空間 **24/ 7/365** 非對稱網路之威脅。

(2)CISA 網路安全服務：

用戶可通過 **CISA** 服務目錄探索 **CISA** 提供的網路安全服務及更多內容。該目錄是 **CISA** 的全部內容，均放置在一個地方—一個單一的資源，為用戶提供所有 **CISA** 任務領域中的服務訊息。上述之 **CISA** 該目錄是互動式的，用戶只需單擊數下即可過濾並快速了解可用的服務。

(3)網路安全治理[14]：

認知到治理在應對網路風險方面的重要性，網路安全及關鍵基礎設施安全署**(CISA)**網路安全部門和國家首席資訊官協會 **(National Association of State Chief Information Officer, NASCIO)**合作制定國家網路全治理報告，及一系列國家網路安全治理案例，探索國家如何管理網路安全的研究。國土安全系統工程與發展研究所 **(Homeland Security Systems Engineering and Development Institute, HSSEDI)** 是國土安全部擁有的聯邦資助研究與發展中心 **(Federally Funded Research and Development Center, FFRDC)**，它負責開發和編撰案例研究。該報告和案例研究確定各州如何利用法律、政策、結構和流程，幫助更佳地管理網路安全，將其作為跨州政府和其他公共和民營部門利害相關者的企業範圍的戰略問題。

2.基礎設施安全部門[15]：

CISA 與各個級別的企業、社區和政府合作，幫助提高國家的關鍵基礎設施對網路和實體威脅的抵禦能力。每個人都有責任保護國家的關鍵基礎設施。

(1)2015 年特定行業計畫[16]：

---

[13] **Cybersecurity and Infrastructure Security Agency(2022)。Cybersecurity。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/cybersecurity。**

[14] **Cybersecurity and Infrastructure Security Agency(2022)。Cybersecurity Governance。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/cybersecurity-governance。**

[15] **Cybersecurity and Infrastructure Security Agency(2022)。Infrastructure Security。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/infrastructure-security。**

[16] **Cybersecurity and Infrastructure Security Agency(2022)。2015 Sector-Specific Plans。上網瀏**

CISA 作為國家基礎設施保護計畫的一部分，於 16 個關鍵基礎設施部門中，CISA 為每個部門的公共、民營部門合作夥伴及州、地方、郡和地區政府制定一項針對特定部門的防護計畫，該計畫側重於獨特的營運條件和該部門的風險格局之辨識與防護。與聯邦機構和民營部門等合作夥伴密切合作，並制定該部門或組織之特定計畫，每四年更新一次，以確保每個部門或組織都在適應不斷變化的風險環境。

2015 年部門或組織之特定計畫，為該部門確定應對當前風險環境的目標和優先事項，例如網路和實體安全之間的關係、各部門之間的相互依存、氣候變化、老化和過時的基礎設施相關的風險，及執法經驗等。這些部門扮演著與國家經濟和人身安全息息相關的關鍵角色，包括民眾每天依賴的服務，如交通、通訊、能源、水、食品、農業、化工、金融、醫療保健與其他維持經濟活力的基本服務，支撐著美國的高生活水平。

每個關鍵基礎設施部門的企業與政府合作夥伴，均可以使用各自的 2015 年部門特定計畫，制定各自的發展，以應對未來所面臨的挑戰，並在獨特的風險管理視角、優先事項和資源範圍內建立彈性與韌性。該計畫尚提出能制定有意義指標的方法，這些指標可用於衡量各部門或組織在提高關鍵基礎設施的安全性、彈性和韌性時所取得的進展。

透過應用上述計畫中的行動，協力夥伴參與者應能夠創建適合的產品和工具，以支持設施和系統所在的處所司法管轄區與發生事件的地方。這些計畫尚提供共同的語言和分類方法，並介紹國家層面的協調和其他適用於地方區域層面的合作活動。

(2)建立 **2022** 年重大關鍵基礎設施安全月[17]：

大多數美國民眾可能不會定期考慮關鍵基礎設施—也就是說，直到渠等受到損害，民眾始關注其安全性問題。暴風雨期間的停電或勒索軟件攻擊後，對醫療設施的連線受限，是現實生活中，提醒關鍵基礎設施在日常生活中係扮演重要之角色。每年之整個 11 月，CISA 邀請所有美國人記住基礎設施安全就是國家安全。全美民眾可以一起降低風險，建立彈性、韌性，保持國家關鍵基礎設施的安全，對美國的國家安全、經濟和整體生活方式均很重要。關鍵基礎設施所涵蓋之範疇，包括：從電信、化學設施、醫療保健和金融系統等的方面。它與其他關鍵基礎設施和支持系統相互依賴，並包含保持實體國家和經濟運行的所有基本服務。

CISA 不僅需要保護關鍵基礎設施以及這些設施內和周圍的人員免受實體威脅，而且 CISA 尚需要意識到關鍵基礎設施系統集成資訊技術 (Information Technology, IT) 和營運技術所出現的新網路漏洞。

在整個月中，CISA 將努力為保護美國關鍵基礎設施的工作作好準備，經常來回查看並在社交媒體上關注相關訊息，以獲取最新資訊。

(3)重大關鍵基礎設施漏洞評估[18]：

覽日期：2022 年 11 月 13 日。https://www.cisa.gov/2015-sector-specific-plans。

[17] Cybersecurity and Infrastructure Security Agency(2022)。Infrastructure Security Month。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/infrastructure-security-month。

[18] Cybersecurity and Infrastructure Security Agency(2022)。Critical Infrastructure Vulnerability Assessments。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/critical-infrastructure-vulnerability-assessments。

網路安全及關鍵基礎設施安全署(CISA)對國家的關鍵基礎設施進行專門的安全、彈性與韌性之評估。這些評估有助於 CISA 及其合作夥伴—聯邦、州、郡、地區政府和民營企業更佳地理解和管理關鍵基礎設施的風險。這些評估檢查基礎設施的脆弱性、相互依賴性、能力差距及其中斷或遭受攻擊後之後果。漏洞之評估，結合通過基礎設施規劃資源之程序，形成綜合規劃和評估能力。這套功能、方法和工具支持高效地使用重大關鍵基礎設施之資源，以增強關鍵基礎設施對所有危害的快速恢復能力。

這些自願的、非監管的評估是國家基礎設施保護計畫，基於風險實施防護計畫的基本要素，旨在預防、阻止和減輕恐怖襲擊的風險，同時在所有危險中，實現及時、有效的回應和復原。

由於大多數美國關鍵基礎設施都是私有的，因此 CISA 評估的有效性，係取決於民營部門所有者、管理者和營運商的自願合作。CISA 的保護性安全顧問(Protective Security Advisor, PSA)在當地展開工作，促進這種合作及技術援助，以增強國家關鍵基礎設施的安全性、彈性和韌性。因應關鍵基礎設施所有者和營運商及其他州、地方、郡和地區官員的要求，CISA 通過保護性安全顧問(Protective Security Advisor, PSA)提供評估。

3.緊急通訊部門[19]：

CISA 為確保公共安全和國家安全，及社區能夠在穩定狀態和緊急行動期間無縫隙、安全地進行通信，以保障美國關鍵基礎設施的安全、可靠和有彈性，採行以下之措施：

(1)邊境互通示範項目[20]：

依據 2007 年 9 月 11 日委員會法案(PL No.110-53)的建議，授權網路安全及關鍵基礎設施安全署(CISA)建立邊境互通性示範項目(Border Interoperability Demonstration Project, BIDP)，這是一個一次性的、競爭性的項目，價值 2550 萬美元，該計畫係向加拿大和墨西哥邊境的美國社區提供資金和技術援助。該立法授權國土安全部選擇六個以上之社區參與：至少三個沿美加邊境，另外三個沿美墨邊境。

CISA 選擇的七個項目，涉及具有不同地理和人口密度的多個社區。選定的項目測試涉及新技術、治理、規劃、協調、培訓和練習之創新方法。這些項目可作為其他邊境社區的可重複模型，以實現與國內和國際機構相互之可通信性。CISA 與邊境互通性示範項目的參與者和社區進行合作，記取經驗教訓，並在整個過程中與社區共享資訊。

(2)成立應急通信準備中心[21]：

應急通信準備中心(Emergency Communications Preparedness Center, ECPC)具有可互相操作性，且最作為通信協調的聯邦機構間之聯路點。其成員代表聯邦政府在緊急通信中的廣泛作用，包括監管、制定政策、營運、撥款和技術援助。

---

[19] Cybersecurity and Infrastructure Security Agency(2022)。Emergency Communications。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/emergency-communications。

[20] Cybersecurity and Infrastructure Security Agency(2022)。Border Interoperability Demonstration Project。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/border-interoperability-demonstration-project。

[21] Cybersecurity and Infrastructure Security Agency(2022)。Emergency Communications Preparedness Center。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/ecpc。

應急通信準備中心由 14 個聯邦部門和機構組成：美國農業部、商務部、國防部、能源部、衛生和公共服務部、國土安全部、內政部、司法部、勞工部、州、交通部和財政部。聯邦通信委員會和總務管理局亦是應急通信準備中心的成員。

(3)緊急通信機制、強化與州、地方、郡和地區之協調機制[22]：

改善和加強應急通信，與可互相操作通信機制是聯邦、州、地方、郡和地區合作夥伴共同須承擔的國家責任。網路安全及關鍵基礎設施安全署(CISA)領導國家的安全/應急準備(National Security /Emergency Preparedness)之通信工作。CISA 與公共安全人員和政府官員共同開發出一個框架，以提出及實踐可操作性、相互操作性和通信連續性的解決方案。

CISA 直接與第一回應者進行社區合作，確定緊急回應者所面臨的日常挑戰。CISA 擬定政策、計劃提供資訊，並與州、地方、郡和地區(State, Local, Tribal, and Territorial, SLTT)之機構建立更牢固的關係。這些關係對於改善應急通信至關重要。CISA 中央執法部門與各級政府（聯邦、州、地方、郡和地區等）的合作夥伴進行合作，以改善公共安全通信、國家安全和應急之準備通信。

CISA 於 2019 年 9 月更新國會授權的國家應急通信計畫(National Emergency Communications Plan, NECP)。國家應急通信計畫是美國在全國範圍內增強應急通信能力和相互可操作性的總體戰略計畫。此外，CISA 協助州和地區合作夥伴制定全州通信可相互操作性計畫 (Statewide Communications Interoperability Plans, SCIPs)，透過結構化的方式推進相互的可操作性，以協助改善全國的應急通信機制。

4.國家風險管理部門[23]：

CISA 與政府、合作夥伴進行合作，識別、分析、優先考慮和管理國家關鍵基礎設施的最重大戰略風險，現今美國面臨之最重大風險如下：

(1)新冠病毒 COVID-19[24]：

CISA 認為打擊 COVID-19 虛假信息活動，解決虛假信息活動和陰謀論，並提供有關如何將傳播虛假或誤導性內容的風險，降至最低損害的公開步驟。

CISA 打擊 COVID-19 的虛假信息工具，包括：可幫助州、地方、郡和地區(State, Local, Tribal, and Territorial, SLTT)官員提高對於 COVID-19 的起源、規模、政府應對、預防和回應相關的錯誤信息、虛假信息和陰謀論的認識與偵處之執法能量。

COVID-19 繼續對關鍵基礎設施員工、國家關鍵職能部門以及關鍵基礎設施公司和營運構成風險。許多第一線關鍵基礎設施工作人員接觸 SARS-CoV-2 病毒，導致關鍵基礎設施中的多個部門出現不成比例的疾病和死亡。醫療保健工作者、執法人員、消防員以及運輸食品和農業部門的勞工，其工作性質令其

---

[22] Cybersecurity and Infrastructure Security Agency(2022)。Emergency Communications State, Local, Tribal, and Territorial Coordination。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/emergency-communications-state-local-tribal-and-territorial-coordination。

[23] Cybersecurity and Infrastructure Security Agency(2022)。National Risk Management。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/national-risk-management。

[24] Cybersecurity and Infrastructure Security Agency(2022)。Coronavirus。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/coronavirus。

繼續面臨暴露之風險。保護關鍵基礎設施勞動力，與提供風險減緩等的策略，係以減少 **COVID-19** 對關鍵基礎設施勞動力的負面影響最為重要，能持續支撐國家的關鍵功能，與關鍵基礎設施公司和營運商的運作。

CISA 創建一個網路安全清單，協助醫療保健部門減少組織漏洞並防止、阻絕惡意行為者。醫院和醫療機構正面臨著各種複雜的網路攻擊，包括網路犯罪者和民族主義者之攻擊。實施這些協議與灌輸人們數字統計的警惕文化，將使健康照護組織**(Healthcare Delivery Organization, HDO)**能夠專注於 **COVID** 疫苗和患者護理等優先須處理之事項，而不是網路攻擊事件所產生的不利影響。

(2)5G 安全性、彈性和韌性[25]：

第五代（**5G**）無線技術代表電信網路的徹底革新變革。**5G** 將改變數據傳輸之格局，乃成為創新、新興市場和經濟增長的催化劑。隨著數百億台設備通過 **5G** 連接到互聯網，這些連結機制，將為大量新興的、增強的關鍵基礎設施服務提供支持與服務。

CISA 通過國家風險管理中心**(National Risk Management Center, NRMC)**與政府及合作夥伴一起領導風險減緩工作，以確保 **5G** 技術和重大關鍵基礎設施的安全性、彈性與韌性。

(3)選舉基礎設施安全之防護[26]：

公平和自由的選舉是美國民主的標誌，美國人民對其投票價值的信心，主要依賴於使國家選舉正常運作之基礎設施的安全性、彈性與韌性。因此，既安全又具有彈性、韌性的選舉過程是至關重要的國家利益，亦是網路安全及關鍵基礎設施安全署**(CISA)**的最高優先執法事項之一。

CISA 致力於與選舉前線的執法人員（州、地方政府、選舉官員、聯邦合作夥伴和供應商）進行合作，管理國家選舉基礎設施的風險。**CISA** 在未來美國選舉的過程中，將保護其所依賴的關鍵基礎設施，避免遭到潛在的威脅和破壞，並保持選舉之透明、靈活、創新與中立。

5.利害相關者參與部門[27]：

利害相關者參與部門**(Stakeholder Engagement Division, SED)**專注於三方面的努力：

(1)戰略夥伴關係：

利害相關者參與部門與聯邦、州、地方、郡、地區**(State, Local, Tribal, and Territorial, SLTT)**、國際和民營部門組織（包括關鍵基礎設施）建立戰略合作夥伴關係。利害相關者參與部門支持服務於關鍵基礎設施部門的國家執法機關和政府委員會，促進重要資訊和資源的共享，以及實現快速的危機協調─回應與解決之道。利害相關者參與部門尚確定了合作的機會，以解決共同的需求，並將利害相關者與 **CISA** 之戰略合作夥伴主題專家聯繫起來，共同防衛基礎設施之安全。

---

[25] **Cybersecurity and Infrastructure Security Agency(2022)。5G Security and Resilience。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/5g。**

[26] **Cybersecurity and Infrastructure Security Agency(2022)。Election Infrastructure Security。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/election-security。**

[27] **Cybersecurity and Infrastructure Security Agency(2022)。Stakeholder Engagement Division。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/stakeholder-engagement-division。**

(2)利害相關者參與戰略：

利害相關者參與部門協調和管理 **CISA** 的利害相關者參與戰略計劃，根據利害相關者的需求，提供資源和活動。利害相關者參與部門的利害相關者參與計畫，包括針對網路安全、基礎設施安全和緊急通信問題，展開專門性的宣傳活動，及幫助利害相關者發展出應對這些威脅所需能力的資源。

(3)利害相關者之關係管理：

利害相關者參與部門的活動，係 **CISA** 以客戶為中心的方式，提供管理的依據，此方式稱為利害相關者關係管理，使利害相關者參與部門能有不斷擴展、參與、服務及改進產品供應之量能。

6.綜合營運部門[28]：

綜合營運部門**(Integrated Operations Division, IOD)**向州、地方政府、關鍵基礎設施社區的利害相關者和合作夥伴提供 **CISA** 之資源。透過 **CISA** 地區辦事處，綜合營運部門提供[29]：

(1)網路和實體漏洞評估。

(2)架構審查和設計主題專業之知識。

(3)事件回應和支持。

(4)制定計劃和支持。

(5)國家特別安全事件之策劃和支持。

(6)化學設施檢查和現場安全規劃，以實施化學設施反恐標準。

為確保 **CISA** 能夠為執法利害相關者提供服務，綜合營運部門支持以下活動[30]：

(1)透過 **CISA** 中央執法部門，綜合營運部門提供 **24x7x365** 的情勢感知和最新的營運報告。

(2)藉由 **CISA Intel**，綜合營運部門進行情資的報告分析，監督 **CISA** 的報告官員，並與情報界合作，以確保對 **CISA** 任務的支持。

(3)通過營運規劃、準備和連續性，綜合營運部門支持 **CISA** 組織法範圍內的營運優先事項，例如選舉安全、**COVID-19** 之防疫和 **2020** 年人口普查。這包括制定營運計劃和營運項目**(Concepts of Operations, CONOPS)**並監督 **CISA** 執法的連續性和準備計劃。

綜合營運部門準備、計劃、管理 **CISA** 營運、確保 **CISA** 能力和服務的完成狀態，以支持國家關鍵基礎設施的防禦和安全。一個準備就緒的組織，可以領導 **CISA** 高效能的營運，以降低風險並增強國家關鍵基礎設施的彈性[31]。

（二）CISA 地區執法部門[32]**:**

---

[28] **Cybersecurity and Infrastructure Security Agency(2022)。Integrated Operations Division。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/integrated-operations-division。**

[29] **Cybersecurity and Infrastructure Security Agency(2022)。Integrated Operations Division。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/integrated-operations-division。**

[30] **Cybersecurity and Infrastructure Security Agency(2022)。Integrated Operations Division。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/integrated-operations-division。**

[31] **Cybersecurity and Infrastructure Security Agency(2022)。Integrated Operations Division。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/integrated-operations-division。**

[32] **Cybersecurity and Infrastructure Security Agency(2022)。CISA Regions。上網瀏覽日期：2022 年 11 月 13 日。https://www.cisa.gov/cisa-regions。**

在全國範圍內，網路安全及關鍵基礎設施安全署(CISA)提供一系列網路和實體安全之服務，以支持關鍵基礎設施所有者、管理者和營運商、州、地方、郡和地區合作夥伴的安全性、彈性和韌性。**CISA** 的執法專家與地區、州、縣、郡和地方各級的關鍵基礎設施合作夥伴和社區合作，其目的如下[33]：

1.對關鍵基礎設施造成危害的準備、防疫、回應和復原工作。

2.對關鍵基礎設施進行和整合基礎設評估和分析，其評估和分析之項目，包括：依賴關係和協調聯繫之效應，以作為應急管理各個階段決策的參考。

3.促進公共和民營部門關鍵基礎設施合作夥伴之間的情資共享。

4.提高對網路安全風險和事件最新情勢之感知與偵測。

每個 **CISA** 區域總監均領導整個區域的安全專業人員，通過十個 **CISA** 區域的地方辦事處，區域執法人員透過穩定狀態和事件之回應與處理、關鍵基礎設施分析以及與關鍵基礎設施合作夥伴的戰略聯繫，管理執法任務執行。保護性安全顧問**(Protective Security Advisors, PSA)**、化學品安全檢查官**(Chemical Security Inspectors, CSI)**、網路安全顧問**(Cyber Security Advisors, CSA)**、緊急通信協調官**(Emergency Communications Coordinators, ECC)**和 **CISA** 總署工作人員，均通過區域辦事處，協調其關鍵基礎設施保護任務之進行，並就區域關鍵基礎設施工作進行協調與溝通。

四、小結：

CISA 為美國人民提供安全、彈性和韌性的關鍵基礎設施，領導國家努力理解、偵測、管理和降低其網路和實體基礎設施的風險，學習與合作夥伴一起防禦當今的威脅，並為未來構建更安全、更有彈性與韌性的基礎設施，**CISA** 是公部門和民營部門、美國和其他國家間之重要國家層級協調員。

其中，**CISA** 組織之任務與使命，係為強化網路之安全性、彈性與韌性、打擊網路犯罪、保護聯邦網路、保護關鍵基礎設施、發出行政通知書，協調利害相關者之參與等，針對複雜網路產生各式各樣之風險危機，提出相對應之預防措施，以強化網路空間的安全性、韌性與彈性，並透過網路間的橫向聯繫，共同打擊重大犯罪、保護國家關鍵基礎設施之安全。

CISA 之組織職掌，可分為：**1**、中央六大部門；**2**、地方區域辦事處。中央部門區分為：**(1)**網路安全部門；**(2)**基礎設施安全部門；**(3)**緊急通訊部門；**(4)**國家風險管理部門；**(5)**利害相關者參與部門；**(6)**綜合營運部門等六大部門，各司其職，綜理各項相關勤業務，除了加強網路安全、強化關鍵基礎設施之安全維護、嚴格控管風險等之外，仍注重利害相關者之橫向協調，以建立一個完善之防護機制；位於十個 **CISA** 區域的地方區域辦事處，就其區域之關鍵基礎設施工作進行協作，與網路安全之風險評估。

CISA 負責整個聯邦網路安全的管理，協調國家間網路安全防禦之執行，與政府和民營部門共同防禦當今的風險和威脅，同時保護國家關鍵基礎設施免受威脅之破壞。

參、美國網路安全及基礎設施安全署 **(CISA)**之**2023---2025**年戰略計劃之介紹

一、美國網路安全及基礎設施安全署 **2023---2025** 年戰略計劃之執法目的

[33] **Cybersecurity and Infrastructure Security Agency(2022)。CISA Regions。上網瀏覽日期：2022** 年 **11** 月 **13** 日。**https://www.cisa.gov/cisa-regions**。

[34]：

因應網路安全空間及基礎設施兩者容易受到來自實體和威脅等各種風險之影響，而意圖破壞網路的行為者及民族主義激進者，利用漏洞破壞前述之網路關鍵基礎設施之安全，而這兩者環環相扣且具脆弱性，影響美國民眾之日常生活，而美國民眾越來越關注基礎設施所造成的影響，故美國政府為加強網路空間安全性、韌性及彈性，在 **2018** 年成立以來發布第一個綜合戰略，於 **2022** 年的 **9** 月初，**CISA** 發布了第一個戰略計畫，針對網路安全及基礎設施之威脅如何排除之措施提出四大目標，**CISA** 提出四大戰略目標，以下介紹 **CISA** 所提的戰略變革，期許在未來三年**(2023～2025** 年**)**，能有成效的降低網路威脅對關建基礎設施的負面影響，並促進 **CISA** 與協力合作夥伴的共同努力，故該計畫傳達 **CISA** 的願景及任務，其願景係為美國民眾建立一個安全及富有彈性與韌性的關鍵基礎設施；另 **CISA** 任務係為領導美國政府了解、管理、減少網路及關鍵基礎設施遭受危害之風險。

二、網路安全及基礎設施安全署之 **2023-2025** 戰略計畫之四大目標概述

有關於美國國土安全部之網路安全及基礎設施安全署之 **2023-2025** 年戰略計畫四大目標圖，詳如下圖所示[35]：

[34] **Cybersecurity and Infrastructure Agency(2022),CISA Strategic Plan,2023-2025,** 上網瀏覽日期：**2022** 年 **11** 月 **15** 日。網址：**https://www.cisa.gov/strategy**

[35] **Cybersecurity and Infrastructure Agency(2022),CISA Strategic Plan,2023-2025,** 上網瀏覽日期：**2022** 年 **11** 月 **15** 日。網址：**https://www.cisa.gov/strategy**

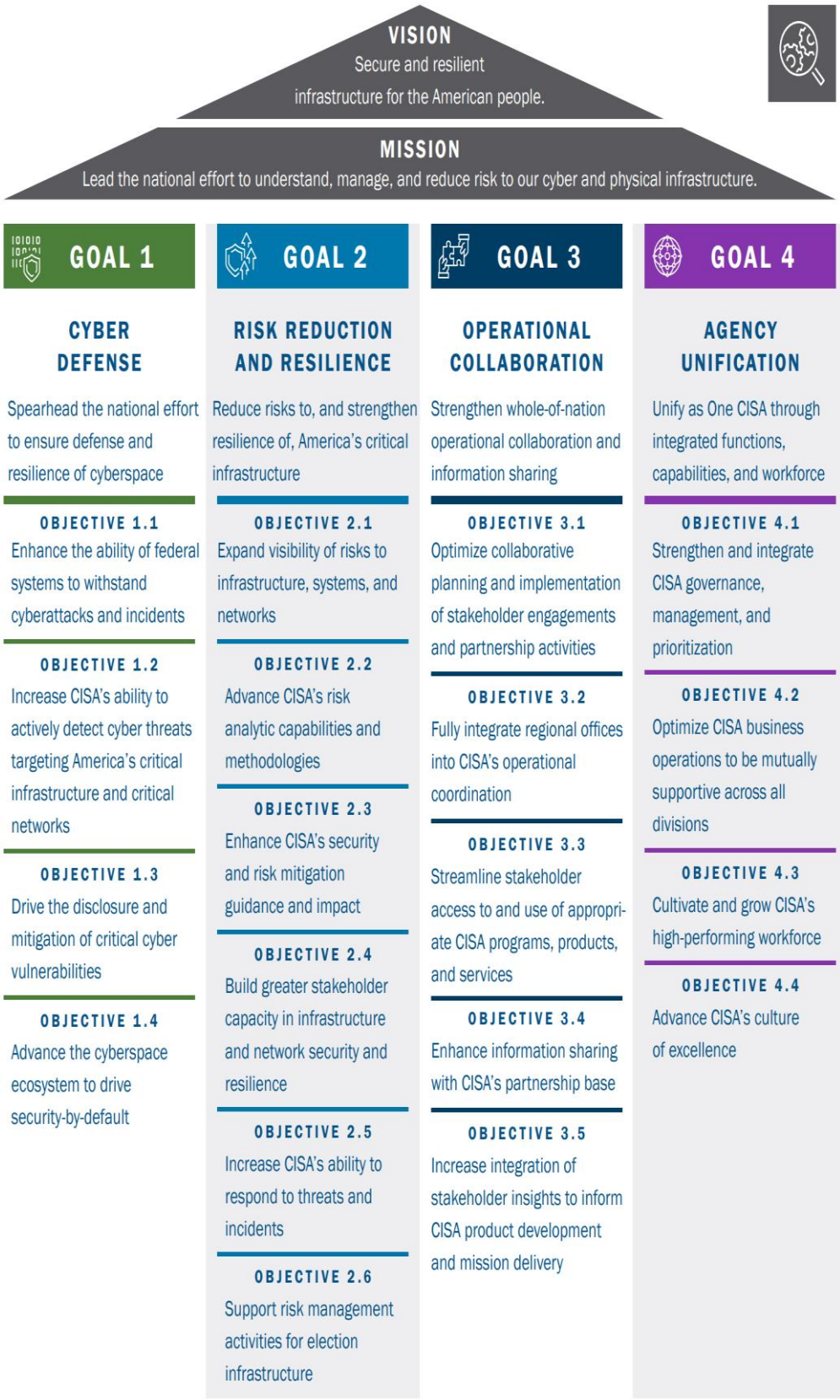

圖 2、網路安全及基礎設施安全署之 2023-2025 年戰略計畫四大目標圖示
資料來源：Cybersecurity and Infrastructure Agency(2022),CISA Strategic Plan,2023-2025。

(一)目標 1：網路防禦[36]

1、增強聯邦系統抵禦網路攻擊和重大危安事件的能力

CISA 致力於幫助聯邦機構進行必要之改革，以改善美國政府的網路防禦態勢。通過推動和促進採用現代、安全及有彈性的網路安全防禦技術來實現這一目標、提高事件回應能力、降低聯邦政府的供應鏈之風險，並提高對聯邦網路中網路威脅的可見性。CISA 將最大限度地推動和衡量聯邦文官機構，採用強而有力的網路安全防護機制。CISA 將提供擴展和創新的服務及能力，幫助聯邦及地方機關建立有效的網路防護安全計劃與機制。

2、提高主動檢測針對美國關鍵基礎設施和關鍵網路之安全造成威脅能力

美國政府面臨來自高度複雜的威脅，故持續尋求有價值的系統和資訊，具有其必要性。CISA 檢測和預防這些威脅取決於大幅擴大 CISA 的行動能見度。CISA 將推進聯邦和州、地方、部落和地區(State, Local, Tribal, and Territorial, SLTT)網路主動檢測威脅的能力。同時與企業夥伴合作，加強 CISA 對民間網路的了解，CISA 將持續創造對威脅的攔阻能力，並迅速降低危害網路安全規模

3、披露及降低重大的網路關鍵弱點

認識到每個硬體和軟體都包含漏洞，CISA 將作為值得信賴的合作夥伴，並協調相關機關公布新發現涉及網路安全之漏洞。CISA 將與公共和私人實體以及網路研究社群，進行密切合作，以識別和公佈之前未知的網路安全漏洞，然後利用廣泛的執法技能緩解來網路威脅。CISA 將與合作夥伴一起努力，利用相關管道和機制，及時地公布網路漏洞並提供可行建議，並擴大適當的減災對策。為了降低這些漏洞的頻率和嚴重程度，CISA 尚必須利用權威和能力，來識別未減緩的網路及關鍵基礎設施之安全漏洞，特別是影響關鍵基礎設施安全的漏洞與缺失，並在危害發生之前，推動緊急減災。最後，CISA 將與網路安全社區合作，利用既往之經驗，接受與實施網路安全審查委員會和其他諮詢機構的可行建議，以提升美國政府的網路及關鍵基礎設施安全防護機制。

4、推動網路空間安全系統，設定全天候型之驅動安全性

美國各地的公共和專用網路防禦者依靠許多常用工具、流程和資源來執行其工作。CISA 開發和採用最先進的網路防禦和運營工具、服務和功能，以推動技術系統中的預設安全性。CISA 尚支援技術給供應商和網路防禦者，幫助渠等能確保支援軟體和硬體的產品、服務、網路和系統的安全性。CISA 已經認知到安全的網路系統，及關係到人，亦關係到技術，CISA 將支持各國努力通過網路之教育資源，使國家網路之勞動力，能夠填補關鍵技能的短缺。最後， CISA 認識到技術產品的設計和開發必須優先考慮安全性，確保有力的控制，並減少漏洞的發生。

(二)目標 2：降低風險及其原復能力[37]

1、擴展關鍵基礎設施的系統、網路、威脅的可見性

CISA 了解倘若欲有效辨識關鍵基礎設施之風險，基於收集正確的數據和意見，使 CISA 能夠推動評估、分析和決策，此需要加深 CISA 對國家網路與物

[36] Cybersecurity and Infrastructure Agency(2022),CISA Strategic Plan,2023-2025, 上網瀏覽日期：2022 年 11 月 15 日。網址：https://www.cisa.gov/strategy

[37] Cybersecurity and Infrastructure Agency(2022),CISA Strategic Plan,2023-2025, 上網瀏覽日期：2022 年 11 月 15 日。網址：https://www.cisa.gov/strategy

理關鍵基礎設施資產和系統的深入瞭解，並確定可能影響該關鍵基礎設施的潛在和未來風險之來源。CISA 有必要收集儲存涉及國家關鍵基礎設施之重要數據，並且扮演好此種收集與儲存之角色。CISA 將推進管控、監督的工具、理論和運營能力，以評估基礎設施的關鍵性，全面識別、盤點重要之關鍵基礎設施，並瞭解基礎設施的脆弱性。CISA 將研發、部署創新工具並推進合作夥伴關係，以了解網路和物理威脅及漏洞。CISA 將不斷識別新生成或新出現的風險，以免它們對 CISA 的網路安全基礎設施構成威脅。最後，隨著 2022 年《關鍵基礎設施網路事件報告法》的通過，CISA 正在改善政府對重大網路安全事件的可見性，以便 CISA 與其他機構可以與協力夥伴合作，並採取行動，有效地保護 CISA 免受類似事件的侵害。

2、增進 CISA 的風險分析能量和方法論

網路和基礎設施安全之防禦，取決於 CISA 能深入地瞭解國家和部門層面的風險，特別是那些對關鍵系統、網路和基礎設施具有系統性威脅的風險。CISA 必須完善風險分析之能力和方法，以促進 CISA 對面臨的風險的能進行深入瞭解。在通過目標 2.1 之實現，及擴大風險可見性的基礎上，CISA 確保將關鍵基礎設施資訊和識別工作納入分析方法，以利 CISA 在作出決策前，能進行全面性、廣泛性之分析。CISA 部門擁有獨特的技術專長之處，在於特定的計劃具有量身定製的風險分析能力，以排定跨機構間戰略層面的風險管理優先事項。

3、增強 CISA 的安全性和降低威脅衝擊的指導方針

為了加強對關鍵基礎設施的保護，在適當的情況下，CISA 將在內部設置針對威脅、危害和風險之評估與分析，CISA 為協力夥伴提供安全和風險緩解之指導與說明。為了改善和降低風險對 CISA 的影響，CISA 將提供可操作的專業知識和緩減措施，以解決基礎設施安全所面臨威脅及強化應急通信系統。CISA 將發布重要指南，以推動有效的 IT 網路風險管理。CISA 將本指南的重點，放在對 CISA 的合作夥伴至關重要且 CISA 已確定為優先事項的風險上。除了建置指導安全決策的標準和提供可行之建議外，CISA 亦努力建立績效目標及增加跨部門網路安全之機制。CISA 將確保高風險化工設施的安全符合化學設施反恐標準(CHEMICAL FACILITY ANTI-TERRORISM STANDARDS，CFATS)和其他法規。在適當和必要的情況下，CISA 尚將提供重點性的技術之援助與評估，以顯著提高網路與關鍵基礎設施之安全性和復原力。

4、在基礎設施及網路區塊建立更佳夥伴關係之量能

CISA 是值得信賴的合作夥伴，有能力幫助關鍵基礎設施擁有者和運營商，建立測量方法之能力與標準，以辨識有關其自身面臨的風險並作出決策，以衡量安全性之影響及增強韌性。為了有效地滿足渠等的需求，CISA 向不同合作夥伴或部門提供的關鍵產品和服務，必須適當地給予與擴展 CISA 的關鍵設施防護計劃和風險管理措施。網路安全、基礎設施安全和應急通信方面的相關產品，以滿足 CISA 不斷增長合作夥伴的需求。這將包括 CISA 與部門風險管理機構(SECTOR RISK MANAGEMENT AGENCIESSRMA，SRMA)的互動與聯繫，以及 CISA 為其他部門提供適切的支援。CISA 將提供有實質影響力的能力和服務，以滿足合作夥伴最緊迫和不斷變化的安全需求，包括回應內部威脅、預防公共集會場所的安全。CISA 尚必須回應緊急需求，訂製 CISA 的產品，以應對新的風險，例如提供專門針對這些系統面臨的網路安全風險的新型應急通信

產品。另外，涉及執法能量之區塊，尚需要將 CISA 的產品範圍，擴大到新的協力夥伴，並將 CISA 內部的網路安全服務，擴展到非聯邦之協力夥伴上。

5、提高 CISA 應對威脅和危安事件的能力

CISA 創置維護一個 24/7/365 運營態勢和回應協調中心，以協調，綜合的方式，回應不斷發展的網路和實體事件或威脅。CISA 必須加強和擴大 CISA 的總署和區域執法能力，以支持 CISA 的協力夥伴有能力應對恐怖主義、針對性的暴力襲擊、重大自然災害等人身威脅和重大危安事件。此將包括 CISA 作為八大關鍵基礎設施部門的部門風險管理機構(SECTOR RISK MANAGEMENT AGENCIESSRMA，SRMA)之角色，以及 CISA 能支援其他部門和機構之發揮 SRMA 的作用。在重大網路危安事件期間，CISA 隨時準備支援公共和私人實體的需求，包括在適當的情況下建置具實用性的事件回應機制，以限制重大危安事件之負面影響，最大限度地減少運營停機時間，並實現快速復原之目標。對於自然重大災害等，CISA 同樣必須部署現有資源，及運用專門知識，包括通過國家應急框架中的緊急支援職能，為應急人員提供支援。此外，CISA 將擴大 CISA 重要的緊急通信支援服務的範圍，以確保與回應者進行連接，並確保公共安全實體可以在活動期間快速相互通信與聯繫。作為選舉基礎設施子部門的部門風險管理機構(SECTOR RISK MANAGEMENT AGENCIESSRMA，SRMA)，CISA 是聯邦政府管控選舉基礎設施風險的主控中心，並確保負責選舉事務之官員及其與私營部門之合作夥伴擁有管理風險所需的資訊。憑藉 CISA 與上述選舉官員和供應商的自願夥伴關係，CISA 向聯邦調查局、美國選舉援助委員會、情報部門等聯邦合作夥伴提出必要的援助與服務，並深獲好評

6、強化各地選舉活動之關鍵基礎設施的危害管理

作為選舉基礎設施安全維護工作負責子部門的部門風險管理機構(SECTOR RISK MANAGEMENT AGENCIESSRMA，SRMA)，CISA 是聯邦政府負責選舉基礎設施風險管控的主管機關，並確保負責選舉官員及其私營部門之合作夥伴，擁有管理風險所需的系統性資訊。

(三)目標 3：營運合作夥伴關係[38]

1、優化協力夥伴之共同共同參與與夥伴關係活動的合作規劃及實施

為了優化 CISA 之協力夥伴的共同參與和建立夥伴關係的價值，CISA 必須在內部的機構建立，部門風險管理機構(SECTOR RISK MANAGEMENT AGENCIESSRMA，SRMA)以及更廣泛的合作夥伴之社區中，推動計劃，優先考慮和協調協力夥伴之共同參與。CISA 將在 CISA 服務的協力夥伴中建立 CISA 的優質品牌，令渠等對 CISA 建立信心。CISA 將運用協力基關之數據和見解、客戶需求、運營要求，確定目標的優先順序。

2、將全美各個區域辦事處充分整合納入 CISA 的協調辦公室之中

CISA 區域辦事處執法人員對外協調聯繫之能力至關重要;他們改善 CISA 對產品和服務的獲取，建立合作夥伴關係，並在全國範圍內發展降低風險與彈性能力。CISA 將加強總署與 CISA 辦事處的區域執法人員之間的整合。CISA 將建立協調總署部門和地區之間參與執法行動的流程之機制，並相互支援運營

[38] Cybersecurity and Infrastructure Agency(2022),CISA Strategic Plan,2023-2025, 上網瀏覽日期：2022 年 11 月 15 日。網址：https://www.cisa.gov/strategy。

之管理。為了優化 CISA 計劃、產品和服務的交付與運行，CISA 將加強現有的國家級夥伴關係管理框架與地區之間的聯繫，直接將 CISA 各部門和政府協調委員會等要素擴展到各個地區。CISA 尚將創建內部業務管理之論壇、機制和流程，使全國各個協力夥伴參與計劃和協調變得簡單、高效和互利。

3、夥伴關係能有效率地取得瀏覽 CISA 的計畫、產品及服務

CISA 的計劃、產品和服務為 CISA 的各個合作夥伴提供必要的見解與協助，以便在資產、系統和企業層面就網路和實體之基礎設施上，能有效地降低風險、防禦，彈性作出及時、明智、正確的決策。為了能夠高效、方便地使用這些資源，CISA 將努力按照客戶的條件，向他們提供這些資源。在可能、合適適法的情況下，CISA 將根據客戶的具體需求和情況，為其提供量身定製的產品資訊交付之。為此，CISA 的資源目錄將始終可用、準確、可定製且引人入勝、易於瀏覽。CISA 將在整個機關內，廣泛而一致地行銷 CISA 的計劃、產品和服務，以擴大 CISA 在核心利益相關者群體中的實質影響力，同時尋求增加代表性不足的社區及非傳統利益相關者的公平瀏覽和使用。

4、與 CISA 的合作夥伴提升情資分享之機制

提高 CISA 和利害相關者情資分享之機制，CISA 必須加強與外部合作夥伴的溝通能力，包括及時的重大危安事件之報告和威脅情資之共享，同時，共同分享情其他信息和數據。如欲促進更多的信息共享，須要 CISA 繼續建立新的合作框架，例如加強與聯合網絡防禦合作組織（JOINT CYBER DEFENSE COLLABORATIVE，JCDC）、部門風險管理機構 (SECTOR RISK MANAGEMENT AGENCIESSRMA，SRMA)和聯邦網絡密切合作中心。CISA 亦使現有結構日趨成熟，例如與以下機關進行情資分享：聯邦高級領導委員會（FEDERAL SENIOR LEADERSHIP COUNCIL；FSLC），信息共享和分析組織(INFORMATION SHARING AND ANALYSIS ORGANIZATIONS；ISAO)。

CISA 採用「增強」模式來進行情資分享，所謂之增強乃指加快速度、提高準確性，並重視情資共享的有效性和合作，同時利用 CISA 的權限，保護個人隱私、公民權利和公民自由。

5、增強合作夥伴的洞察能力與 CISA 進行合作並致力於網路產品開發及發展

來自外部利害相關人的見解，改進於支援任務交付的 CISA 產品及服務。一些利害相關者以訪談和發佈之方式，對 CISA 直接反饋。復次，其他人則提供更間接的見解與意見，例如通過與 CISA 的合作夥伴共同合作之中，通過從評估數據中吸取的經驗教訓向 CISA 提出回饋。CISA 將積極尋求利害相關人的反饋，以確保 CISA 不斷完善化和改進 CISA 的產品，俾利 CISA 成為網路和實體基礎設施領域之中值得信賴的執法專家，亦即 CISA 提供切實的存在價值。CISA 將加強利害相關人的見解、資訊和數據的整合，以協助 CISA 能作出正確之決策以及完整化、精進化之 CISA 的產品、服務和重點領域的優先次序排定、開發、修改和定製。

(四)目標 4：事權統一[39]

1、強化和整合 CISA 治理、管理和設定執法施政優先之順序

CISA 致力於有效地解決阻礙 CISA 任務有效執行的障礙，同時通過專業知

[39] Cybersecurity and Infrastructure Agency(2022),CISA Strategic Plan,2023-2025, 上網瀏覽日期：2022 年 11 月 15 日。網址：https://www.cisa.gov/strategy。

識，承擔明確的責任。CISA 將通過各級實施跨任務授權辦公室會議和交流計劃，並建立治理和管理結構，提供必要的數據和 SOP 流程，以制定優先決策來實現此一目標。CISA 將努力劃定工作路線，分配組織和個人責任，以推動集體決策，並記錄和整合 SOP 流程，以確保最佳實踐的標準化（例如薪資單、發票等），進行有效的內部控管，並支援正確的執法決策。隨著 CISA 的發展，CISA 將戰略性地向 MEO 提供必要之資源，以便 CISA 根據執法需要之擴展執法量能，以便更佳地實現 CISA 的使命。

2、優化 CISA 工作能量並與全國相關部門互相支援

美國政府需要 CISA 的卓越執法表現。CISA 必須促進員工榮譽感，CISA 必須確保員工對於 CISA 的向心力。CISA 的員工必須擁有專業的認證，獲得專業發展和教育的機會。

3、培育和增強 CISA 高效能的工作力與執法能力

員工之專業知識和技能非常重要，CISA 必須確保他們在工作品質中能有效地應用這些技能。CISA 將在成功培養和發展工作力，及文化的基礎上吸引和留用於 CISA 之中，國家最有才華的網路和基礎設施之執法捍衛者。CISA 將實施世界級的人才生態系統，統一涵蓋招聘、延攬、僱用、培訓、認可、晉陞、留用和培訓計劃。為了防止未來出現威脅到 CISA 競爭能力的各式阻礙，CISA 將積極尋找、延聘、識別和培訓來自非傳統場所的網路安全及關鍵基礎設施防護之潛在人才。CISA 認識並準備作好迎接各式來自網路關鍵基礎設施之挑戰，從各個領域尋找人才，並建置良善之升遷管道。CISA 將在整個組織中深化 CISA 的指導和輔導計劃，同時獎勵於 CISA 執法工作中傑出的執法人員。CISA 會創造一個友善、高效的環境，讓高績效團隊，可以通過提高透明度和運營效率，令 CISA 不斷茁壯成長。CISA 將通過創造更強大的職業規劃及開發更多的跨部門工作機會，來為 CISA 的員工創造公平升遷的機會，以促進職業之生涯規劃與發展，俾利 CISA 員工之工作升遷獲得保障，亦大大提升 CISA 之工作能量。

4、提升 CISA 優秀的組織文化

CISA 優質之組織文化的力量，對 CISA 使命之達成至關重要，亦是 CISA 作為成功的基礎。CISA 將繼續通過傳播 CISA 的核心價值觀和核心原則，以建立 CISA 優質之組織文化。CISA 的組織文化將融入 CISA 的日常任務、任務實踐功能、對合作夥伴和利害相關者的服務、CISA 的日常執法活動之中。CISA 將優先建置一個心理層面上，相當安全的環境 ，在這個優質之工作環境中，可以做真實的自己，員工可感到被關心、被支援、被賦予權責相稱之執法權力，在職場上，並始終受到尊嚴、尊重、平等、溫馨的對待，在職場上他們感受到對自己是達成 CISA 法定任務之主角，有責任感及榮譽感。CISA 將通過系統地減輕員工之工作倦怠和提供各式心理健康之資源，優先建議整個 CISA 機構健康和彈性的組織文化。推進公平、公正、透明的組織文化，要求 CISA 的領導者及管理幹部，在獎勵、決策過程、溝通和員工待遇方面，力求透明度、依法行政和公平性。為了推動組織績效，CISA 將營造一個具有組織學習能力、反饋、成長和創新的優質環境。利用 CISA 的卓越組織文化，CISA 將成為網路社區公認的領導及領航者，亦是聯邦政府內部公務員的首選職場，因 CISA 具有優質化、人性化之組織文化，能產生高效能之工作成果，達到 CISA 之法定任務、目標與使命。

三、小結

(一)CISA 在網路防禦區塊確保國防及網路復原力及韌性

不僅增強主動監測威脅的能力，並提可對網路危害危險的警覺性，隨時隨地的監控及預防。

(二)CISA 提出有效降低風險及其復原能力

CISA 蒐集正確資訊及數據，並推動評估、分析及決策以降低未來可能發生之風險或潛在危害。

(三) CISA 強化與合作夥伴關係的勤業務合作和情資分享

CISA 讓合作夥伴可以有效率取得並瀏覽相關計畫、產品及服務，且不僅政府機關合作，更涉及到與新機關合作，並建立合作框架。

(四)透過整合功能，將團隊整合成一個具有組織素養之團體。

肆、台灣網路安全及基礎設施安全防護機制之現況

一、台灣網路安全防護機制之現況

就網路安全防護機制之組織架構而論，台灣負責網路安全防護機制之相關機關、單位，共計有：總統府國家安全會議(國家資通安全辦公室)、國安局、行政院資安處、刑事局、調查局、國防部資通電軍、通傳會、行政院數位發展部資通安全署等機關及單位，合力共同組成之，目前，網路安全防護之區塊，我國並未設置一個權責、事權統一之機關。雖然，**2021** 年版本之國家資通安全戰略報告指出，國家通訊傳播委員會係擔任關鍵基礎設施之資安防護的主管機關。亦即，國家通訊傳播委員會之角色，係著重於關鍵基礎設施安全防衛中之資安防護，而非著重於全般性之網路安全防護。本文認為，仍宜仿照美國國土安全部網路安全及基礎設施安全署之模式，建置一個網路安全防護權責、事權統一之機關為佳的。

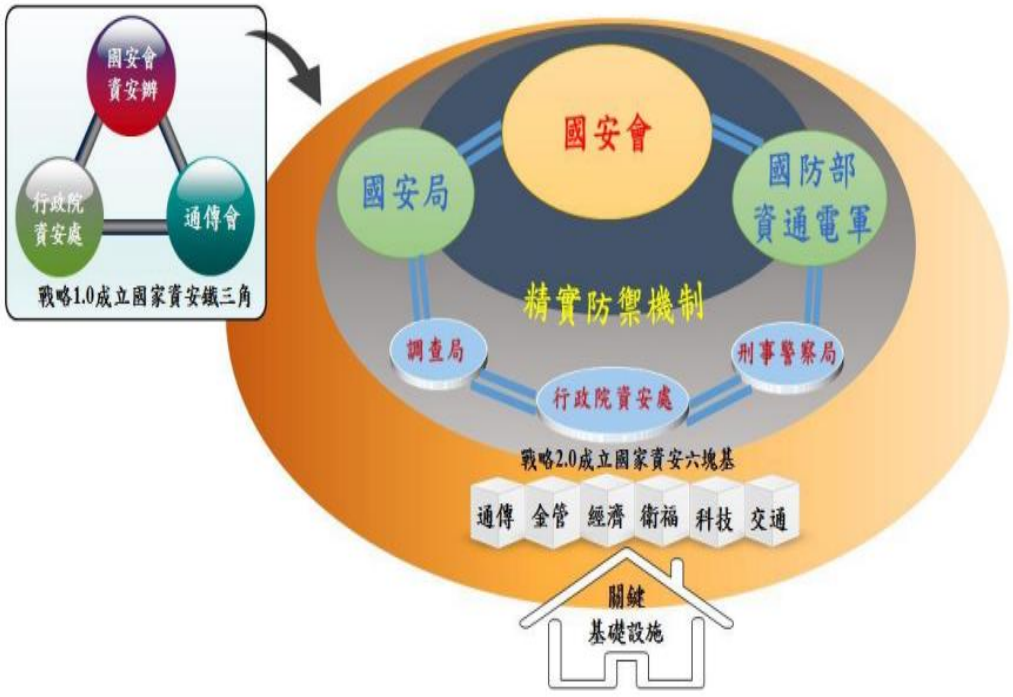

圖 3、資安組織之六塊基礎聯防體系架構圖[40]

資料來源：國土安全辦公室（**2018**），國家關鍵基礎設施安全防護指導綱要。

[40] 國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安全會議國家資通安全辦公室出版。

在網路、資通安全防護之法制部分，目前，共計有以下之相關法制：1. 資通安全管理法 (民國 107 年 06 月 06 日)；2.中央銀行所管特定非公務機關資通安全管理作業辦法 (民國 110 年 04 月 15 日)；3.內政部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 12 日)；4.公司或有限合夥事業投資智慧機械與第五代行動通訊系統及資通安全產品或服務抵減辦法 (民國 111 年 07 月 04 日)；5. 公務機關所屬人員資通安全事項獎懲辦法 (民國 110 年 08 月 23 日)；6.文化部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 18 日)；7.司法院所管特定非公務機關資通安全管理作業辦法 (民國 108 年 04 月 18 日)；8.外交部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 01 月 31 日)；9.交通部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 25 日)；10.行政院原子能委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 04 日)；11.行政院農業委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 13 日)；12.行政院環境保護署所管特定非公務機關資通安全管理作業辦法 (民國 108 年 05 月 07 日)；13.法務部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 05 月 17 日)；14.金融監督管理委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 27 日)；15.客家委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 05 月 21 日)；16.科技部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 23 日)；17.原住民族委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 06 日)；18. 特定非公務機關資通安全維護計畫實施情形稽核辦法 (民國 110 年 08 月 23 日)；19. 財政部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 26 日)；20.國防部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 27 日)；21.國軍退除役官兵輔導委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 06 月 20 日)；22.國家通訊傳播委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 04 月 01 日)；23. 國家資通安全研究院設置條例 (民國 111 年 01 月 19 日)；24.教育部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 04 月 25 日)；25. 經濟部所管特定非公務機關資通安全管理作業辦法 (民國 111 年 01 月 25 日)；26.資通安全事件通報及應變辦法 (民國 110 年 08 月 23 日)；27.資通安全情資分享辦法 (民國 110 年 08 月 23 日)；28.資通安全責任等級分級辦法 (民國 110 年 08 月 23 日)；29.大陸委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 18 日)；30.資通安全管理法施行細則 (民國 110 年 08 月 23 日)；31.電信事業資通安全管理辦法 (民國 109 年 07 月 09 日)；32. 僑務委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 13 日)；33.數位發展部資通安全署組織法 (民國 111 年 01 月 19 日)；34.數位發展部資通安全署處務規程 (民國 111 年 08 月 08 日)；35. 數位發展部資通安全署編制表 (民國 111 年 08 月 08 日)；36.衛生福利部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 04 月 19 日)；37. 關鍵電信基礎設施資通設備測試機構及驗證機構管理辦法 (民國 110 年 01 月 29 日)。

在網路、資通安全防護之戰略計畫部分，目前，計有由國家安全會議國家資通安全辦公室於 2021 年 9 月所頒布之國家資通安全戰略報告---資安即國安 2.0[41]。

[41] 國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安

2021 年版本之國家資通安全戰略報告，特別強調主動式防禦趨勢，亦即，運用資安情報、數據及資安之分析技術，事先辨別網路攻擊者，採取事前之網路、資通安全之各式防護之作為，這些主動式防禦、應變措施，計包括：1、鑑識潛在入侵者；2、清除後門與惡意程式；3、主動阻斷攻擊來源；4、重新配置資安防護縱深，如下圖所示[42]。

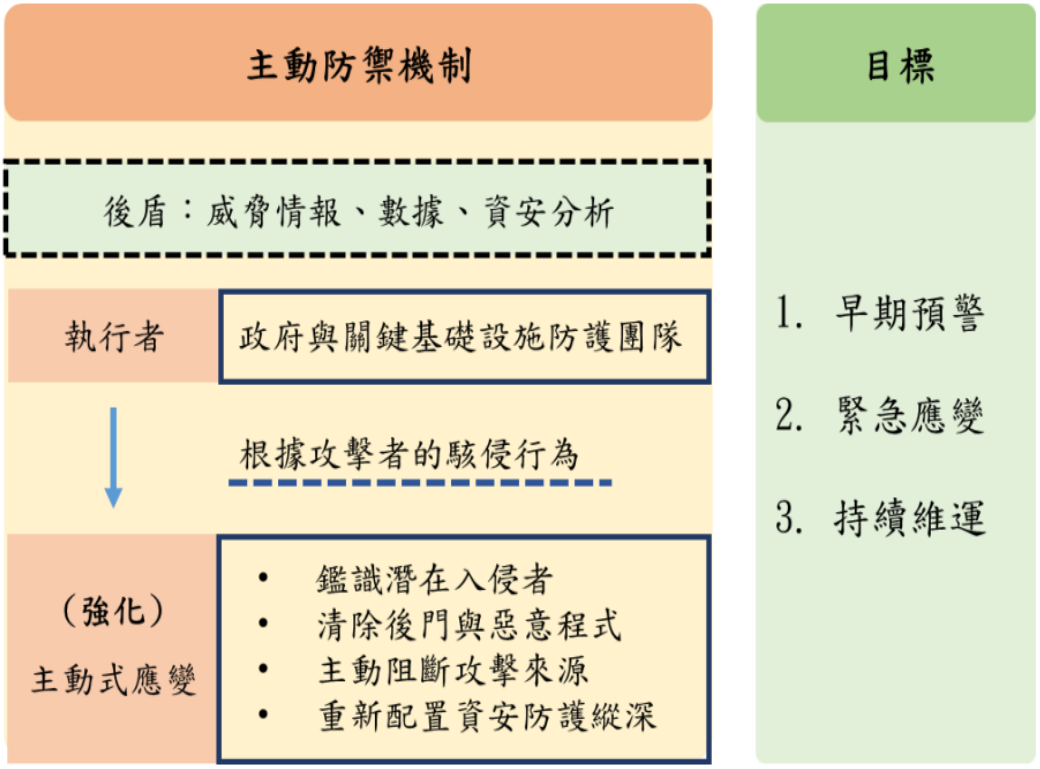

圖 4、網路、資通安全主動式防禦示意圖
資料來源：國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要。

復次，2021 年版本之國家資通安全戰略報告之願景，係為「打造堅韌、安全、可信賴之智慧國家」。為了達到此一願景，2021 年版本之國家資通安全戰略報告設定三大目標[43]：
目標一：充實資安卓越人才（People）；
目標二：強化人民家園安全防護、鞏固資安外交網路防禦（Protection）；
目標三：促進產業繁榮發展（Prosperity）。

為了達到目標一：充實資安卓越人才（People）之任務，我國特強調強化資安能力，培育資安卓越與實戰人才，實際之作法，包括：於數位發展部下新設「國家資通安全研究院」，另外，成立防衛後備動員署，精進關鍵基礎設施資安協防機制，詳如下表所示[44]。

全會議國家資通安全辦公室出版。
[42] 國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安全會議國家資通安全辦公室出版。
[43] 國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安全會議國家資通安全辦公室出版。
[44] 國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安

表 1、資安人培 2.0 策略

資安及國安戰略1.0	單位培育對象	資安及國安戰略2.0
資安暑期課程	**教育部** 在學資安人才	**完善資安高教環境** • 於4年內擴增師資員額 • 延攬國際頂尖師資
虛擬資安研訓院	**數位發展部/經濟部** 資安跨域在職人才	**成立國家資通安全研究院** • 前瞻資安技術研發人才培育 • 招募民間專家組織國家資安戰隊 • 資安競賽以戰代訓培養實戰人才
資通電軍指揮部	**國防部** 資安戰士	**設立防衛後備動員署** • 培訓後備網路戰士 • 精進關鍵基礎設施協防機制

資料來源：國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要。

再者，為了目標二：強化人民家園安全防護、鞏固資安外交網路防禦（Protection）之任務，我國亦特別著重於促進資安國際合作，建構國內外聯防體系，詳如下圖所示[45]：

全會議國家資通安全辦公室出版。

[45] 國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安全會議國家資通安全辦公室出版。

圖 5、資安國際合作策略 2.0
資料來源：國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要。

為了達到目標三：促進產業繁榮發展（**Prosperity**）之任務，我國亦特別重視落實六大核心戰略產業之中，須將資安導入之，詳如下圖[46]：

[46] **國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安全會議國家資通安全辦公室出版。**

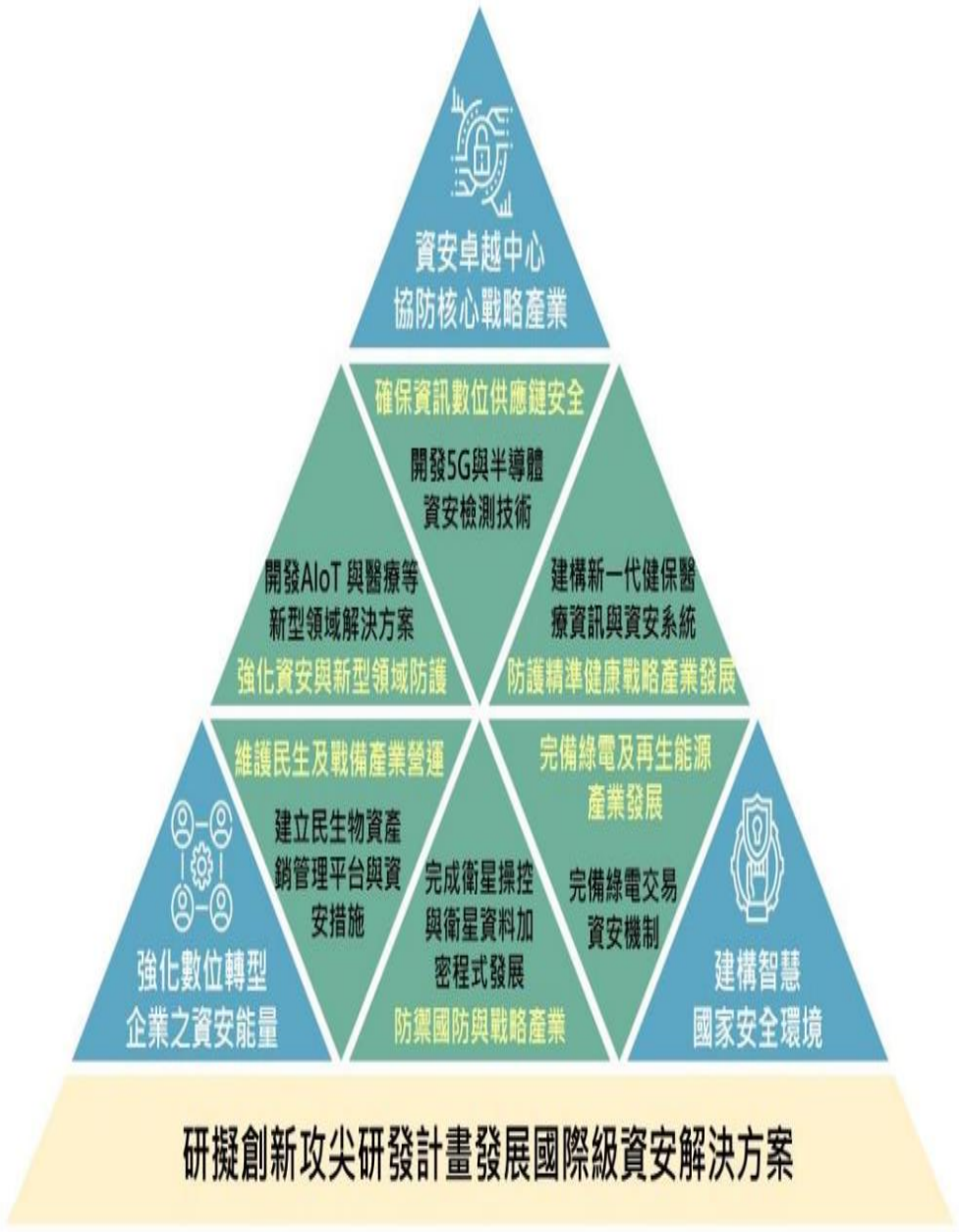

圖 6、六大核心戰略產業資安導入示意圖
資料來源：國土安全辦公室（**2018**），國家關鍵基礎設施安全防護指導綱要。

資安即國安戰略 **2.0** 推動之策略部分，計分為五大策略[47]：
策略一：**Talent**－培育資安卓越人才，建構聯合作戰機制；
策略二：**Resilience**－提升防護韌性；
策略三：**Unity**－促進資安國際合作，建構國內外聯防體系；
策略四：**Security**－發展精實防禦機制，打擊網路犯罪；

[47] **國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安全會議國家資通安全辦公室出版。**

策略五：Technology－產業落實資安、驅動資安產業。

再者，資安即國安戰略 2.0 推動做法部分，如下所述[48]：
(一)充實資安卓越人才：培育資安卓越人才，聯合作戰機制
(二)強化人民家園安全防護、鞏固資安外交網路防禦
(三)促進產業繁榮發展：產業落實資安，驅動資安產業

有關於「資安即國安戰略 1.0」與「資安即國安戰略 2.0」之差異與比較部分，詳如下表所示：

表 2、「資安即國安戰略 1.0」與「資安即國安戰略 2.0」之差異與比較表

	資安即國安戰略 1.0	資安即國安戰略 2.0
組織	成立行政院資通安全處	1. 加速成立數位發展部暨相關資安管理部門 2. 政府機關六塊基礎團隊堅實合作
法制	1. 實施資通安全管理法 2. 修正國家安全法及國家情報工作法	法遵的落實 （關鍵基礎設施、委外與供應鏈、資料庫等）
人才	成立資通電軍	強化資安卓越人才培育 促進公私團隊協力互助
產業	強化自主資安產業	六大核心戰略產業資安部署

資料來源：國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要。

二、台灣關鍵基礎設施安全防護機制之現況

涉及國家關鍵基礎設施(Critical Infrastructure, CI)之定義方面，2018 年版本之國家關鍵基礎設施安全防護指導綱要指出，所謂之國家關鍵基礎設施(Critical Infrastructure, CI) [49]：「係指公有或私有、實體或虛擬的資產、生產系統以及網絡，因人為破壞或自然災害受損，進而影響政府及社會功能運作，造成人民傷亡或財產損失，引起經濟衰退，以及造成環境改變或其他足使國家安全或利益遭受損害之虞者。」

其次，有關於國家關鍵資訊基礎設施(Critical Information Infrastructure，CII)之定義，2018 年版本之國家關鍵基礎設施安全防護指導綱要指出[50]：「涉及核心業務運作，為支持國家關鍵基礎設施持續營運所需之重要資通訊系統或調度、控制系統(Supervisory Control and Data Acquisition，SCADA)，亦屬國家

[48] 國家安全會議國家資通安全辦公室(2021)，國家資通安全戰略報告---資安即國安 2.0，國家安全會議國家資通安全辦公室出版。
[49] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。
[50] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。

關鍵基礎設施之重要元件(資通訊類資產)，應配合對應之國家關鍵基礎設施統一納管。」

為完善規劃國家關鍵基礎設施安全防護事項，以強化國家關鍵基礎設施安全防護功能，我國政府於 **2018** 年 **5** 月 **18** 日修正國家關鍵基礎設施安全防護指導綱要，其政策重點特色如下[51]：

1、以全災害[52]防護概念，實施關鍵基礎設施風險管理

國家關鍵基礎設施安全防護應採取「全災害」防護的概念，從設施內部與外部進行風險辨識，並應將風險管理與持續營運管理的方法導入國家關鍵基礎設施安全防護工作之中。

2、發展應變戰術與戰略，研擬各層級安全防護計畫

為有效執行國家關鍵基礎設施安全防護管理工作，應全面性、有系統的進行設施盤點工作，俾依照設施重要性進行分級管理，並建立完整的國家關鍵基礎設施資料庫，定期更新，各設施領域管理層級應掌握設施系統之間相依關係與失效影響性，並依實際風險辨識結果，依管理範圍發展包含預防、整備、保護、復原的應變戰術與戰略，研擬具體可執行的安全防護計畫。

3、 強化領域間合作聯防，建立資訊分享機制

各主、次領域[53]主管機關應協同國家關鍵基礎設施提供者[54]，建立並強化單位內部與外部、中央與地方等跨領域聯防機制，積極推動公、私部門合作，鼓勵私部門共同參與。跨領域、跨公私部門之間應分享風險資訊，並應建立威脅預警與安全防護資訊分享平台，健全資訊分享機制，提升國家關鍵基礎設施安全防護的整體性。

4、有效整備安全防護資源，提升持續運作能力

各主、次領域主管機關及國家關鍵基礎設施提供者應積極協調整備安全防護之資源與支援，有效保護國家關鍵基礎設施與重要資產之安全。應建立對策計畫，設法減緩設施功能中斷影響，提升政府及社會功能的持續運作能力，進而保障人民生命財產與福祉，維護國土安全與國家安全。

依據國家關鍵基礎設施安全防護指導綱要之說明，我國國家關鍵基礎設施採三層次架構之分類模式，詳如下述[55]：

(一) 第一層是主領域：依功能屬性分為能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區，共八項主要領域。

---

[51] 行政院(2018)。國家關鍵基礎設施安全防護指導綱要。上網瀏覽日期：2022 年 11 月 14 日。**file:///D:/%E4%BD%BF%E7%94%A8%E8%80%85%E8%B3%87%E6%96%99%E5%9C%A8%E6%AD%A4/a591262/Downloads/%E5%9C%8B%E5%AE%B6%E9%97%9C%E9%8D%B5%E5%9F%BA%E7%A4%8E%E8%A8%AD%E6%96%BD%E5%AE%89%E5%85%A8%E9%98%B2%E8%AD%B7%E6%8C%87%E5%B0%8E%E7%B6%B1%E8%A6%81_1070518%E8%A8%82%E6%AD%A3_%20(4).pdf**。

[52] 全災害：指天然災害、資安攻擊、意外事件、人為攻擊、非傳統 攻擊及軍事威脅等災害，係關鍵基礎設施辨識風險與威脅的主要依據。

[53] 主管機關：各次領域由直接掌理、輔導該次領域之全部或一部分 國家關鍵基礎設施的中央目的事業主管機關或直轄市、縣（市） 政府擔任主管機關。

協調機關：原則上各主領域設一協調機關，負責協調該領域內所 屬次領域主管機關，以共享資源與資訊，訂定共同風險管理標準。

[54] 國家關鍵基礎設施提供者(簡稱設施提供者)：指維運或提供關鍵 基礎設施之全部或一部，經中央目的事業主管機關指定，並報行 政院核定者。

[55] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。

(二) 第二層是次領域：各主領域之下再依功能業務區分次領域，例如能源領域下再區分為電力、石油、天然氣等次領域。

(三) 第三層是次領域下的功能設施與系統：係指維持次領域重要功能業務運作所必須之設施設備、運輸網絡、資通訊系統、控制系統、指管系統、維安系統、關鍵技術等。

就基礎設施安全防護機制之組織架構而論，台灣負責基礎設施安全防護機制之機關，主要係為行政院國土安全政策會報，並由行政院國土安全辦公室擔任國土安全政策會報之幕僚單位。再者，行政院國土安全辦公室亦設置一個專家小組，名為：「行政院國家關鍵基礎設施安全防護專案小組」，該小組由行政院國土安全辦公室邀集專家學者、主領域協調機關代表組成。「行政院國家關鍵基礎設施安全防護專案小組」之任務、使命，係修定國家關鍵基礎設施安全防護工作計畫、教育訓練、演練計畫、國家關鍵基礎設施指導綱要及其附件，當完成上述事項之修正之後，並報請行政院國土安全政策會報加以審查、核准[56]。

此一國家關鍵基礎設施安全防護專案小組會議之任務，如下所述[57]：

1、研擬國家關鍵基礎設施安全防護政策及法令之相關事項。

2、研擬國家關鍵基礎設施風險管理及預警機制之相關事項。

3、研擬國家關鍵基礎設施安全防護作為與緊急應變之相關事項。

4、協調聯繫各情報及治安機關協力維護國家關鍵基礎設施之事項。

5、關於國家關鍵基礎設施安全防護之統合指導、協調、支援事項。

6、關於國家關鍵基礎設施相關資訊之蒐集處理事項。

7、其他有關國家關鍵基礎設施安全防護與演習、訓練事項。

在法制部分，我國主要之基礎設施安全防護法令，係為：1、電信管理法；2、關鍵電信基礎設施指定及防護管理辦法；3、行政院國土安全政策會報設置及作業要點；4、中央災害應變中心作業要點；5、國土安全應變機制行動綱要；6、國家資通安全通報應變作業綱要；7、國土安全緊急通報作業規定；8、資通安全管理法，及上文所提及之網路、資通安全防護之相關法制。

另外，在關鍵基礎設施防護相關之計畫、手冊、建議、檢核表部分，則分別如下所述：1、國家關鍵基礎設施安全防護指導綱要[58]（國土安全辦公室於民國 103 年 12 月 29 日函頒，民國 107 年 05 月 18 日訂正）：2、關鍵基礎設施領域分類；3、關鍵基礎設施盤點作業須知；4、關鍵基礎設施安全防護計畫書架構；5、關鍵基礎設施防護演習指導手冊；6、關鍵資訊基礎設施資安防護建議；7、關鍵基礎設施自我安全防護檢核表等。

國家關鍵基礎設施安全防護(Critical Infrastructure Protection, CIP)的目標在於[59]：

一、 維護國家與社會重要功能持續運作，確保攸關國家安全、政府治理、公共安全、經濟與民眾信心之基礎設施與資產的安全。

二、 以全災害為安全防護考量，掌握設施相依關係，辨識潛在威脅與災害影響，降低設施脆弱性，縮減設施失效影響範圍與程度，提高應變效率並加速復原。

---

[56] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。

[57] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。

[58] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。

[59] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。

三、 促進夥伴關係，健全跨領域、跨公私部門合作與資訊分享，進行實體、資通訊以及人員的保防與安全防護，預防因應各類災害所造成的衝擊影響，強化設施的安全性(Security)和韌性(Resilience)。

其次，涉及國家關鍵基礎設施安全防護(Critical Infrastructure Protection, CIP)的之管理要領，如下圖所示[60]：

圖 7、國家關鍵基礎設施安全防護(Critical Infrastructure Protection, CIP)之管理要領六大流程圖

伍、結論與建議

有關於網路安全及關鍵基礎設施安全署(CISA)對臺灣的啟示部分，自成立網路安全及關鍵基礎設施安全署後，美國始重視網路安全與重大關鍵基礎設施之安全維護，針對潛在的網路威脅、可能造成關鍵基礎設施癱瘓之弱點等風險，透過理解、分析、回應、減緩等完善之防護機制，強化關鍵基礎設施之韌性與安全性，並在聯邦、非聯邦和民營部門間，透過健全的橫向聯繫系統，分享及時可操作的情資。此將影響臺灣逐漸將重心移轉至關鍵基礎設施之資安防護，我國關鍵基礎設施依功能屬性區分為八大領域：能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關及高科技園區等，因應我國資安威脅加劇，政府將連結 8 大關鍵基礎設施領域之主管部會，擴大建立國家資安聯防運作機制，由情報資訊驅動國家政府、關鍵基礎設施主管機關及提供者三大層級，形成資安聯防與合作網路，組成國家資安聯防體系，進行資安聯防及情資共享，以強化網路的安全性和韌性與重大關鍵基礎設施之安全維護。[61]其組織架構亦可激勵我國有更進一步之組織改革，決策者可參酌美國 CISA 相關部門之成立，制定出完整又明確之機關組織架構，以有效管理我國網路安全與重大關鍵基礎設施安全維護之議題，如改制成國安國土安全組織或增設相關的部署機關等，並在組織架構的移植中，可依據我國在全球國際情

[60] 國土安全辦公室（2018），國家關鍵基礎設施安全防護指導綱要，國土安全辦公室出版。

[61] 數位發展部資通安全署(2022)。關鍵基礎設施資安防護。上網瀏覽日期：2022 年 11 月 14 日。https://moda.gov.tw/ACS/operations/ciip/650

勢的情況作適當之調整，以建立一個較完善的聯防機制。

我國與美國國土安全部 **CISA** 有關網路安全及關鍵基礎設施安全維護機制之相同、差異處，詳如下述：

一、我國與美國國土安全部 **CISA** 有關網路安全及關鍵基礎設施安全維護機制相同處：

（一）將風險管理與持續營運管理之模式，運用至關鍵基礎設施安全防護，依管理範圍發展包含預防、整備、保護、復原的應變戰術與戰略，使執法人員確實執行風險辨識、風險管理、風險處置等步驟，以回應潛在之威脅與災害。

（二）建立中央與地方、公部門與民營部門等跨領域聯防機制，彼此互相分享風險資訊，並成立威脅預警與安全防護資訊共享平台，透過健全資訊分享機制，以提升國家關鍵基礎設施防護的安全性、韌性與彈性。

（三）我國與美國 **CISA** 均有針對網路及實體關鍵基礎設施進行威脅評估，對於複雜網路或實體威脅所產生的風險危機，依照其重要性進行分級管理，提出相對應之預防措施與解決方式，以強化重大關鍵基礎設施的安全性和韌性。

二、我國與美國國土安全部 **CISA** 有關網路安全及關鍵基礎設施安全維護機制相異處：

美國 **CISA** 有明確規劃出較完整之組織架構，如中央執法部分之六大部門，包括：**(**一**)**網路安全部門；**(**二**)**基礎設施安全部門；**(**三**)**緊急通訊部門；**(**四**)**國家風險管理部門；**(**五**)**利害相關者參與部門；**(**六**)**綜合業務部門等及地方執法之地區辦事處；但我國卻尚未制定出完整又明確之機關組織架構，決策者可參酌美國相關部門之成立，俾利後續針對關鍵基礎設施之安全防護，建立有高效能的機關單位，如改制成國安國土安全組織或增設相關的部署機關等，並在組織架構的移植中，可依據我國在全球國際情勢的情況（中臺關係）作適當之調整。

復次，本文之建議如下：

一、強化國家資通安全之組織架構：國家資通安全戰略報告----資安即國安 **2.0** 中所建構六塊基礎聯防體系**(**簡稱六塊基**)**，計由總統府國家安全會議**(**資通安全辦公室**)**、行政院資安處、國安局、刑事局、調查局、國防部資通電軍等六個機關及單位組成，號稱為六塊基。但六塊基卻未納入通傳會、行政院數位發展部資通安全署，恐有爭議性，本文贊同將通傳會、行政院數位發展部資通安全署納入之，成為八塊基礎聯防體系。

二、建構一個事權統一之網路安全防護主管機關：台灣網路安全防護的主管機關、組織，究竟何者係為主管機關？缺乏明確的規範與建置。有可能之主管機關，係為總統府國家安全會議資通安全辦公室或行政院國家資通安全會報，兩者之權責劃分，有待進一步精進之，用以釐清何者始為台灣網路安全及其基礎設施安全防護的主管機關。

三、建構優質化之組織文化：在美國網路安全及基礎設施安全署**(CISA)** 的 **2023---2025** 年戰略計劃中之第四個目標，**CISA** 專注於創建一個網路安全機關之組織文化，**CISA** 組織文化乃 **CISA** 職員熱愛他們所做的事情，**CISA** 職員尊重他們的同事，不寫黑函，惡意中傷同事，執行公務之際，充分由他們的領導者加以授權之，**CISA** 職員並覺得他們每天正在發揮其職務上應有之功用。台灣之國家資通安全戰略報告，亦可將如何建構、提升優質

組織文化納入之，對於網路安全及基礎設施安全防護的效果，會有更佳化之實效。

四、建構一個事權統一之基礎設施安全防護主管機關：在基礎設施安全防護的區塊，本文建議我國宜仿照美國 **CISA** 之作法，建構一個事權統一之主管機關為佳。

五、打造公私協力之防護安全網：建立類似 **CISA** 之網路安全機制並打造公私協力之概念、提高各項網路安全漏洞防禦之能力，由於我國目前有行政院數位發展部資通安全署負責網路安全，但因應兩岸關係、駭客問題等，致使我國資安威脅加劇，從 **CISA** 之戰略計畫中，可以效仿除了國家政府之外，可與民間企業夥伴合作，形成資安聯防與網路，組成國家資安聯防體系，進行資安聯防及情資分享，並聯結國際，以了解新的網路風險及漏洞。

六、健全化情資分享機制：全面整合政府機構相關單位之情資分享機制，以利相互交換情資。因網路安全狀況變化多端，已非政府機構單獨可以處理的，各單位間交換情資外，以隨時隨地監控網路狀況，如有異常情況，可隨時隨地提供相關支援，有效地保護網路安全及關鍵基礎設施，並建立各區協調能力，以相互支援及營運。

七、保障隱私權、人格權、資訊權：全面地、並有效地情資分享下並保障相關人權 **CISA** 戰略報告中提到採用「增強模式」進行情資分享，而在分享的同時，如何兼顧有效分享情資並能保障隱私權、人格權等相關權利，是我我國可以向 **CISA** 所效仿的。

八、打造優質工作環境，以延聘、培訓、留用資安人才：政府機關善用資源，延聘、培訓、留用優秀人才，並建立良好之組織文化，以提升機關之素養及能量。**CISA** 在戰略中提到相關輔導計畫，讓執法人員有被尊重、平等的對待，而留住資訊相關人才，因此，建議應提供良好並有技術性的暢通管道，並確保透明的管理機制；而在獎懲方面，也可以有合理的評定標準，能達到高度的工作效果。