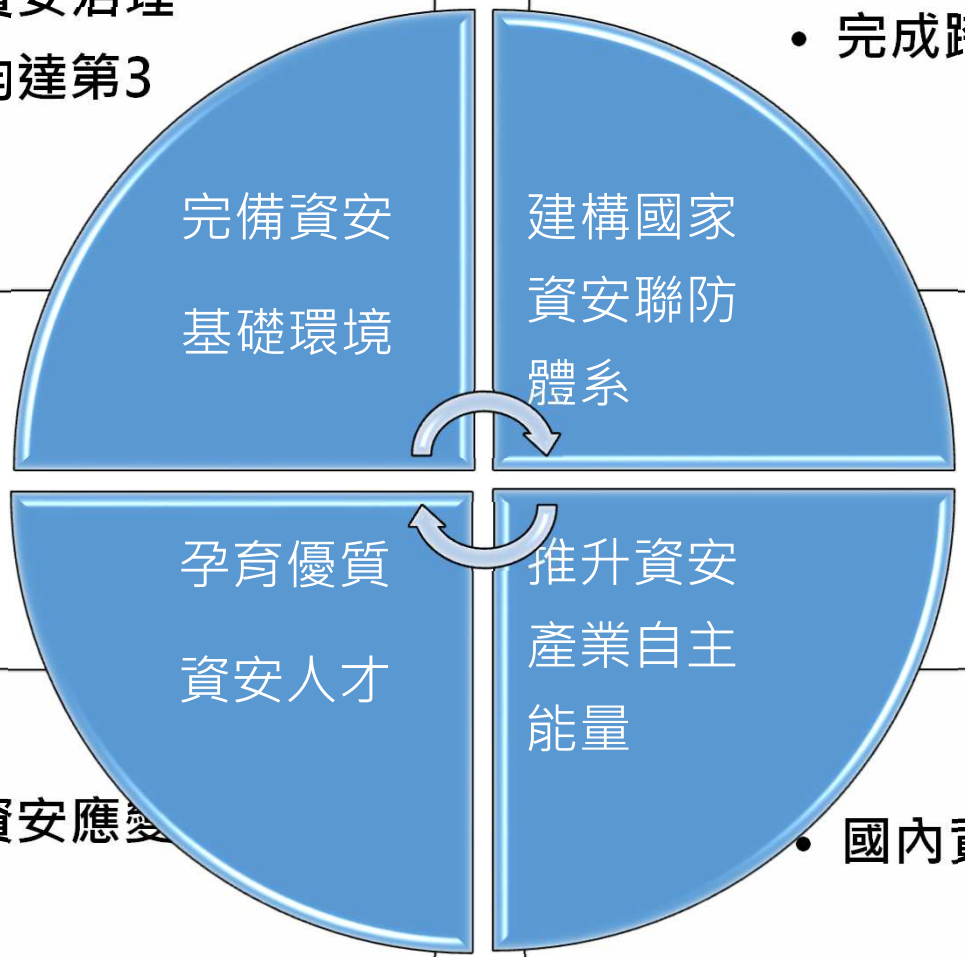
資通安全管理法與發展藍圖

行政院資通安全處
簡宏偉
106年9月22日

國家資安發展關鍵指標

- 政府機關資安治理成熟度平均達第3級以上

- 完成跨域資安聯防體系



- 建立千人資安應變小組

- 國內資安產業產值達550億元

以風險管理為核心的資安防護

- 蒐集網路流量資訊
- 分析樣態

- 監控網路流量
- 掌握攻擊潛勢

- 數位鑑識
- 追查來源
- 落實改善

- 即時通報
- 應變聯防
- 損害控制

資通安全管理法

立法目的

規範對象

公務機關

- 中央與地方機關(構)
- 公法人

非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人(政府捐助合計超過基金總額50%)

- 現行規範對象係以對於人民生活、經濟活動及公眾或國家安全有重大影響者為主要納管對象。
- 關鍵基礎設施之範圍包括能源、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、高科技園區等八個領域。

草案整體架構

資通安全管理法草案

第1章 總則(§1~§8)	立法目的、名詞定義、規範對象、資通安全產業之推動、行政院職責、委任或委託、資安責任等級分級、情資分享機制、資通委外監督
第2章 公務機關資通安全管理(§9~§14)	資通安全維護計畫之訂定、資通安全維護計畫實施情形之查核、資通安全事件通報應變之訂定、資通安全長之設置、獎懲辦法
第3章 非公務機關資通安全管理(§15~§18)	資通安全維護計畫之訂定、資通安全維護計畫實施情形之查核、資通安全事件通報應變之訂定、行政檢查
第4章 罰則(§19~§21)	行政處分
第5章 附則(§22~§23)	施行細則、施行日期

保護客體與規範對象

保護客體

資通安全

指防止資通系統及透過其運作之資訊免於遭受未經授權之存取、使用、控制、洩漏、破壞、修改、銷毀或其他作為，以確保其機密性完整性及可用性。

規範對象

公務機關

指依法行使公權力之中央、地方機關（構）或行政法人。

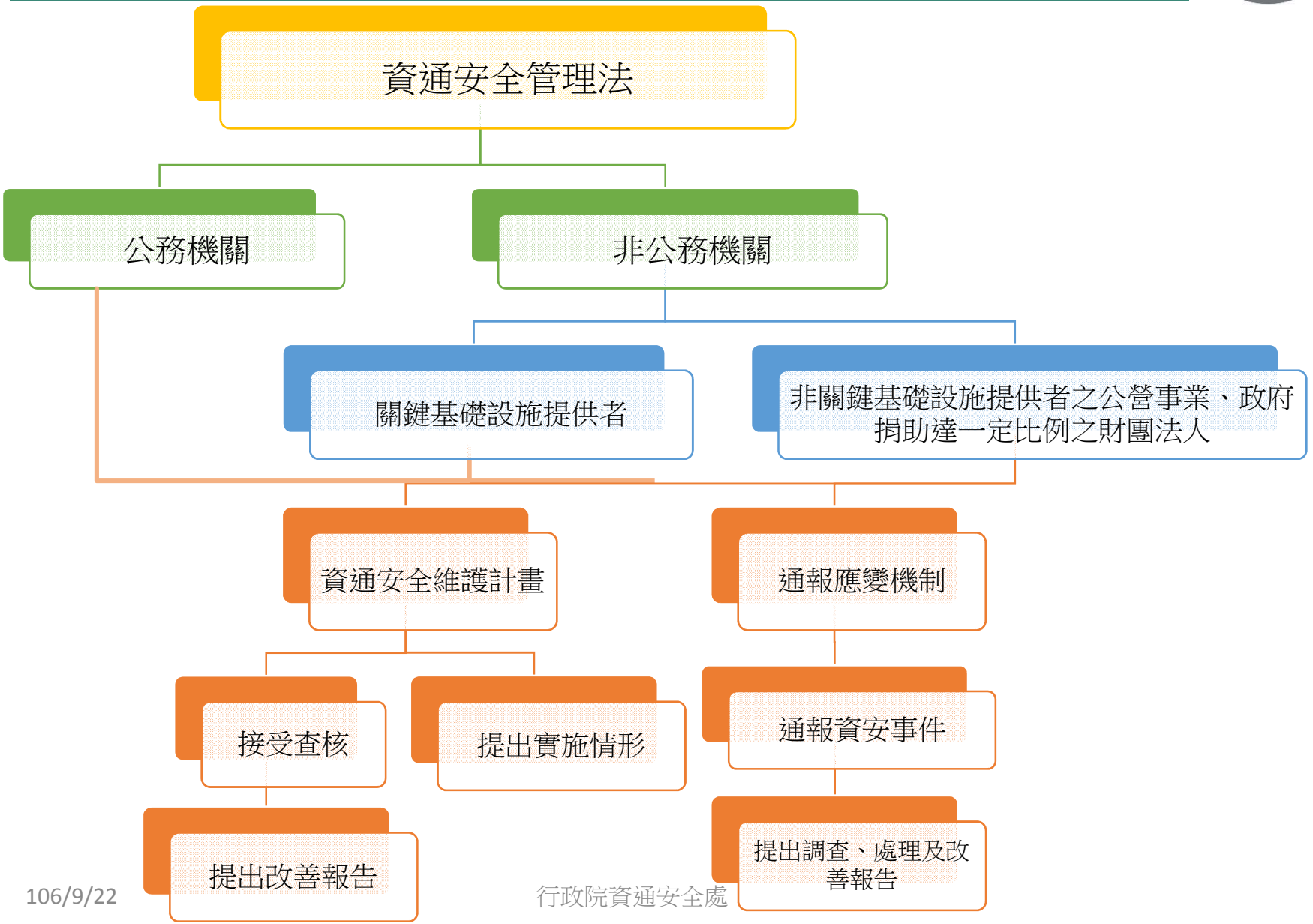
非公務機關

- 關鍵基礎設施提供者
- 非關鍵基礎設施提供者之公營事業、政府捐助達一定比例之財團法人

適用順序

公務機關 → 關鍵基礎設施提供者(區分領域，分批公告) → 非關鍵基礎設施提供者之公營事業、政府捐助達一定比例之財團法人

義務類型


資通安全管理法
公務機關
非公務機關
關鍵基礎設施提供者
非關鍵基礎設施提供者之公營事業、政府捐助達一定比例之財團法人
資通安全維護計畫
通報應變機制
接受查核
提出實施情形
通報資安事件
提出改善報告
提出調查、處理及改善報告

草案架構與內容

● 規範內容

- **資安責任等級分級**
- 資安維護計畫之制定與實施
- 年度資安維護計畫實施情形提出
- **資安稽核**
- **資安事件通報應變**
- 改善報告
- 公告
- 行政(資安)檢查
- 罰則

- 行政院、委託或委任單位、各公務機關
- 中央目的事業主管機關權責
- 權限委託

- **資安責任等級分級**
- 資安維護計畫之制定與實施
- 資安長設置
- 年度資安維護計畫實施情形提出
- 資安稽核
- 改善報告
- **資安事件通報應變**
- 獎懲制度

- 資通安全專業人才之培育
- 資通安全科技之研發、整合、應用、產學合作及國際交流合作之推動
- 資通安全產業發展及推動
- 資通安全軟硬體、設備技術規範、資通安全相關服務及審驗機制之發展及推動
- 定期公布國家資通安全情勢報告及資通安全發展方案
- **建立情資分享機制**

- 委託機關應監督受託者資安之維護

註：1. **粗體藍字**部分，係以個別子法規範。
2. 其餘規範事項，由施行細則補充。

國際趨勢觀察

- 2015年通過「網路安全法」
  - 鼓勵企業主動分享資安情資，並由國土安全部建置網路威脅情資平臺
- 2016年提出「國家網路安全行動計畫」(CNAP)
  - 汰換過時IT設備、網羅頂尖人才及強化公私合作交流

- 2014年通過「網路安全基本法」
  - 強化網路安全推動體制，以利於處理與因應網路攻擊
- 2015年公布「網路安全策略」
  - 提倡產官學合作，確保IoT系統具備完善的安全規格，並鼓勵商業活動採用安全的IoT系統

- 2015年通過「資訊科技安全法」
  - 增加對德國公民、企業及政府機關的保護，降低其網路安全風險
  - 要求關建基礎設施提供者採取檢視措施，向BSI報告網路安全事件，並要求ISP通報其可能的網路安全風險之義務

- 2017年提出「網路安全法」 7/10-8/3開放公眾回饋
  - 要求關鍵基礎設施提供者報告網路安全事件，並採取措施來確保其系統的韌性(resilience)
- 2015年成立「網路安全局」(CSA)
  - 統籌國家整體的網路安全政策方針和跨部會協調

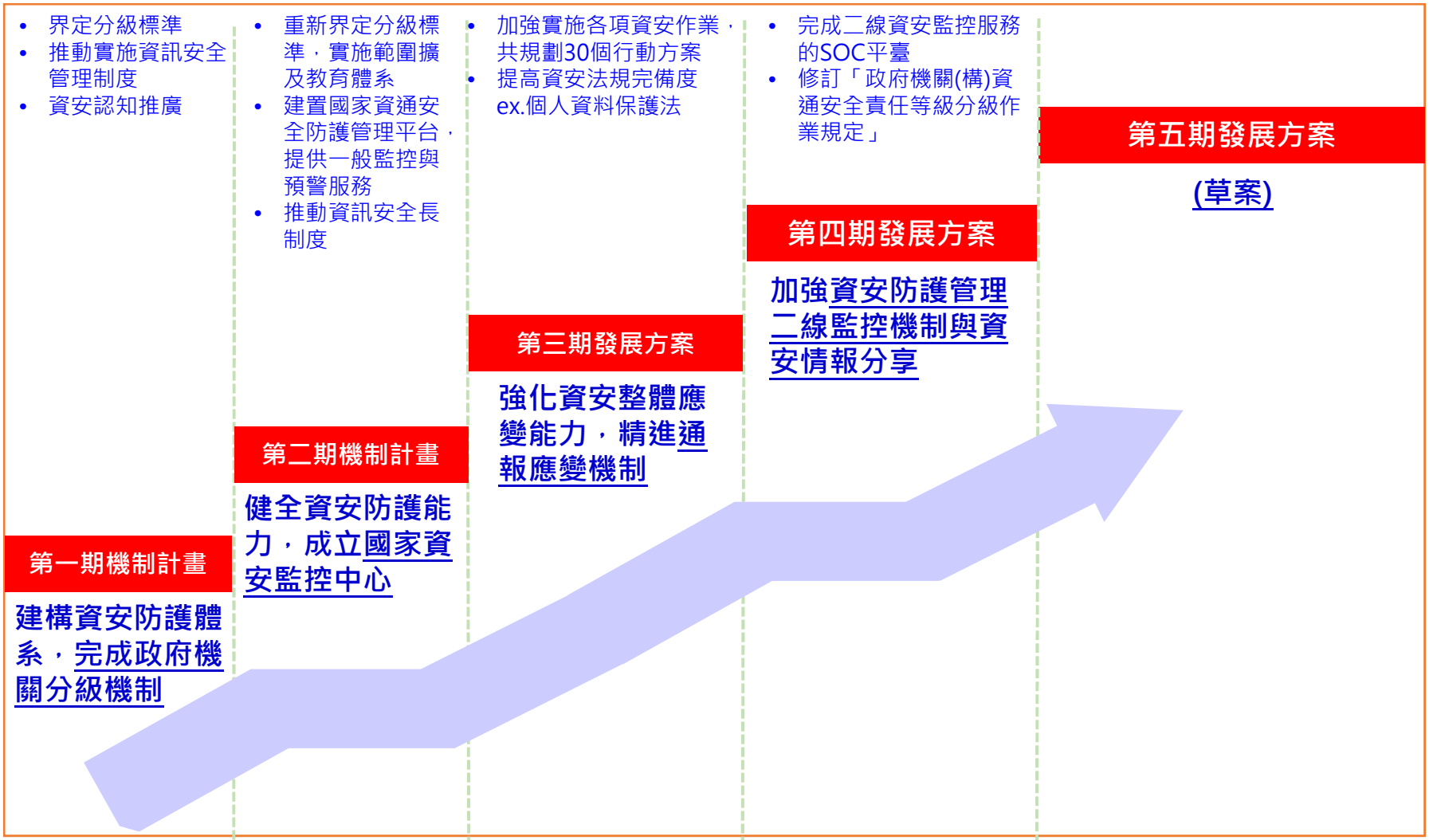
各國資安法規之義務內容比較

國家/國際組織	法律/法案	規範對象		義務					
		公務機關	其他組織	資安維護計畫	報告繳交	通報應變	稽核	資安檢查	罰則
我國	資安管理法(草案)	✓	•CI提供者 •公營事業 •政府捐助財團法人	✓	✓	✓	✓	✓	✓
美國	FISMA*	✓	NA	✓	✓	✓	✓	NA	NA
	其他	依個別法令規定		依個別法令規定					
歐盟	NIS*	✓*	•CI提供者 •數位服務提供者	✓	✓	✓	✓	✓*	✓
新加坡	網安法(草案)	✓*	•CII提供者*	✓	✓	✓	✓	✓	✓
			•資安服務提供者 •資安服務廠商	對SOC、PT等服務提供者與廠商，有證照要求等相關規定					

註：
1. 美國-聯邦資訊安全現代化法(簡稱FISMA) 、 歐盟-網路暨資訊系統安全指令(簡稱NIS)。
2. 歐盟NIS屬指令，並未限制會員國進行調查之方式(稽核、資安檢查均為可行選項)，惟要求會員國須有對受調查者為類似行政處分之權限。
3. 歐盟之公務機關指提供CI之機關；新加坡公務機關為與CII相關之機關。
4. 新加坡非公務機關之CII提供者所涉領域範圍，可由主管部首長隨時修改。

資安發展藍圖

我國資安推動進程


界定分級標準
推動實施資訊安全管理制度
資安認知推廣
第一期機制計畫
建構資安防護體系，完成政府機關分級機制
90 - 93
重新界定分級標準，實施範圍擴及教育體系
建置國家資通安全防護管理平台，提供一般監控與預警服務
推動資訊安全長制度
第二期機制計畫
健全資安防護能力，成立國家資安監控中心
94 - 97
加強實施各項資安作業，共規劃30個行動方案
提高資安法規完備度
ex.個人資料保護法
第三期發展方案
強化資安整體應變能力，精進通報應變機制
98 - 101
完成二線資安監控服務的SOC平臺
修訂「政府機關(構)資通安全責任等級分級作業規定」
第四期發展方案
加強資安防護管理二線監控機制與資安情報分享
102 - 105
第五期發展方案
(草案)
106 - 109

我國資安現況優劣勢分析

優勢S(Strength)

- 完成四階段國家資通安全發展方案，提升我國資安完備度
- 政府提高資安主導層級，建構國安級資安防護機制
- 資安會報成立關鍵資訊基礎設施安全管理組與產業發展組
- 積極推動資安管理法之立法，完備法制基礎

弱勢W(Weaknesses)

- 尚未制定明確之關鍵資訊基礎設施推動政策、防護基準及管理範例
- 缺乏完整的資安人才培育體系
- 資安產業規模及產值過小

機會O(Opportunities)

- 政府推動DiGi+方案，帶動5加2產業創新及下一階段資安需求與成長
- 產官學研對資安人才之需求殷切
- 我國資安情勢特殊，吸引他國與我國進行國際合作意願

威脅T(Threats)

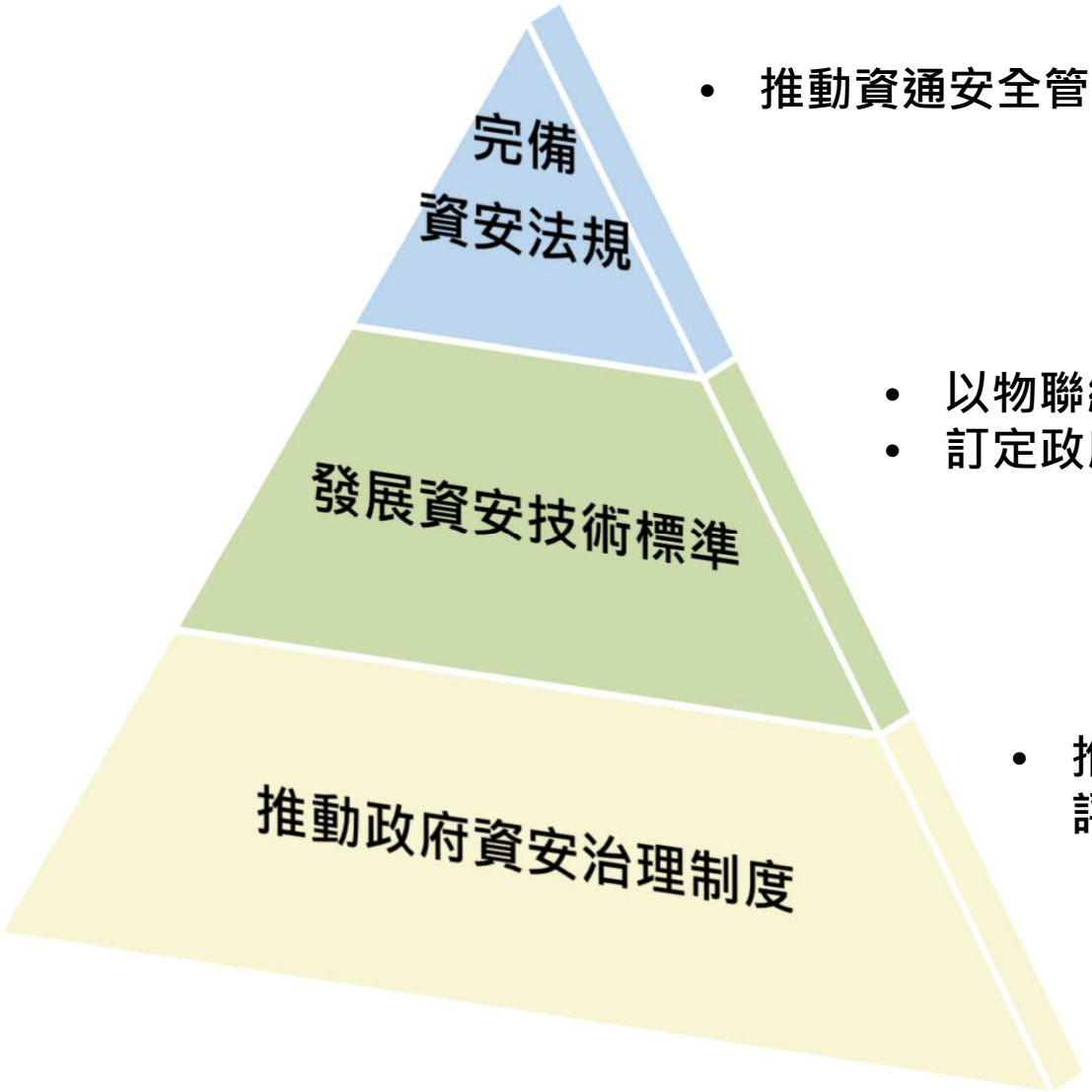
- APT與組織型駭客試圖竊取公務與商業機密威脅未減緩
- 分散式阻斷攻擊頻率與規模持續創新高
- 關鍵資訊基礎設施連網已成趨勢，遭入侵風險遽增
- 物聯網等新興資訊技術快速發展，使虛擬與實體威脅俱增

資安發展藍圖


願景
打造安全可信賴的數位國家
目標
厚植自我防護能量，保衛數位國家安全
推動策略
完備資安基礎環境
建構國家資安聯防體系
推升資安產業自主能量
孕育優質資安人才
具體措施
1. 完備我國資安相關法規及標準
2. 強化基礎通訊網路韌性及安全
3. 建立政府資安治理模式
4. 強化關鍵資訊基礎設施資安防護
5. 建立跨域資安聯防機制
6. 精進網路犯罪防制能量
7. 發展新興資安產業
8. 輔導資安產業升級
9. 鏈結產學研能量發展新興資安技術
10. 增加市場資安人才供給
11. 提升政府資安人力專業職能

推動策略一：
完備資安基礎環境

完備資安基礎環境



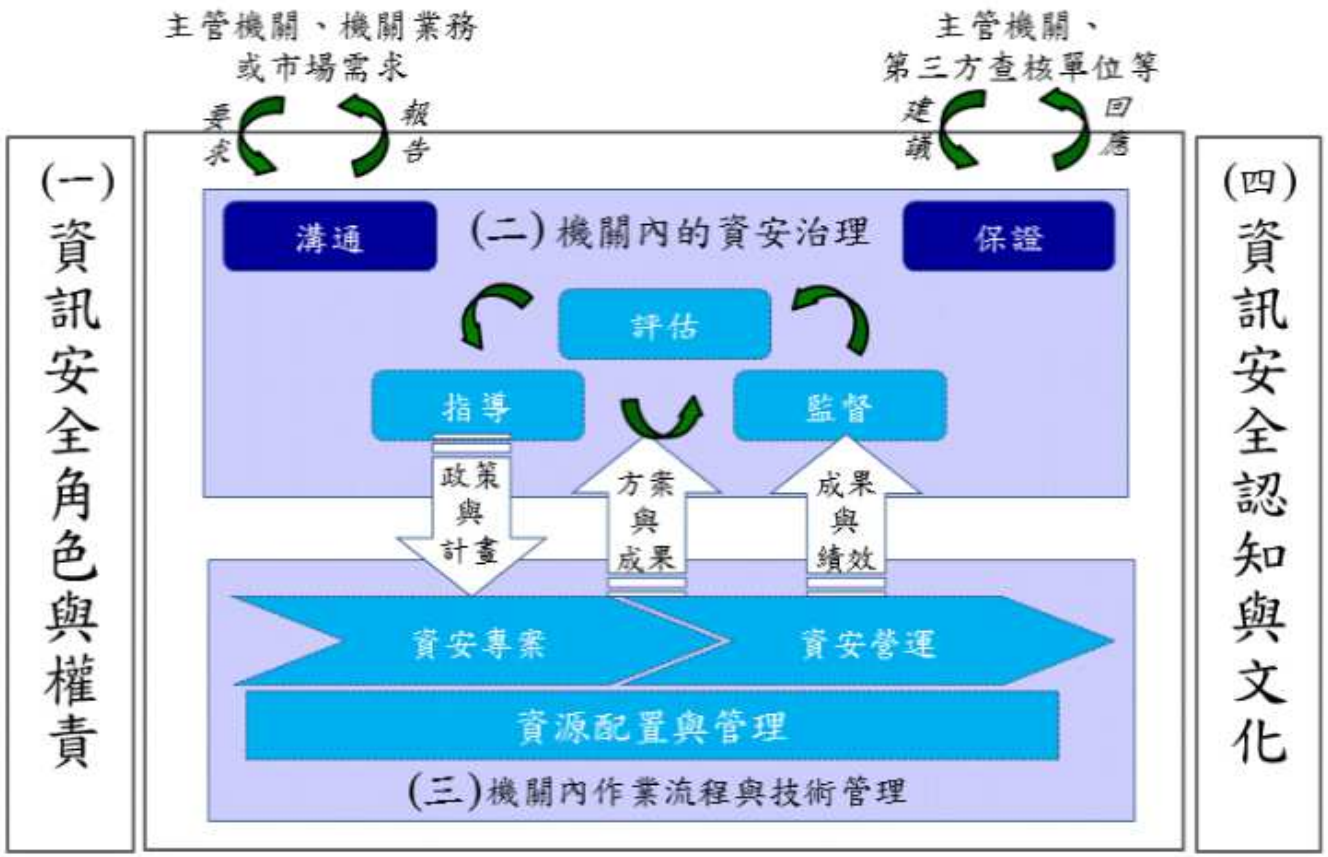
- 推動資通安全管理法立法

- 以物聯網為優先，訂定資安產品驗證標準
- 訂定政府機關資安相關管理及技術規範

- 推動政府機關導入資安治理成熟度評估模型

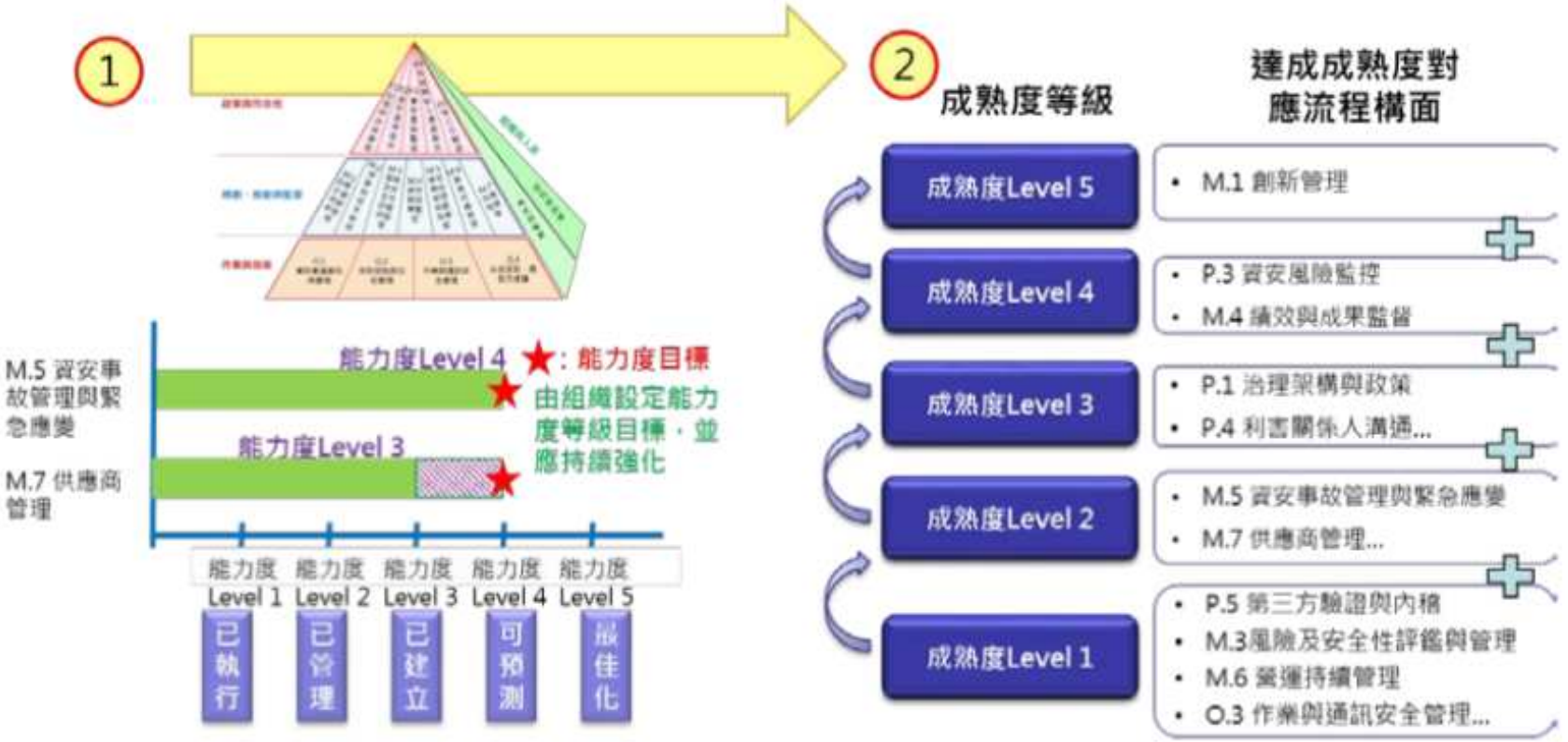
資安治理成熟度係評估組織推行資安治理成效之度量值，藉以規劃未來資安相關重點工作及推動方向

資安治理架構與模型


主管機關、機關業務
或市場需求
要求
報告
主管機關、
第三方查核單位等
建議
回應
(一)資訊安全角色與權責
溝通
(二)機關內的資安治理
保證
評估
指導
監督
政策與計畫
方案與成果
成果與績效
資安專案
資安營運
資源配置與管理
(三)機關內作業流程與技術管理
(四)資訊安全認知與文化

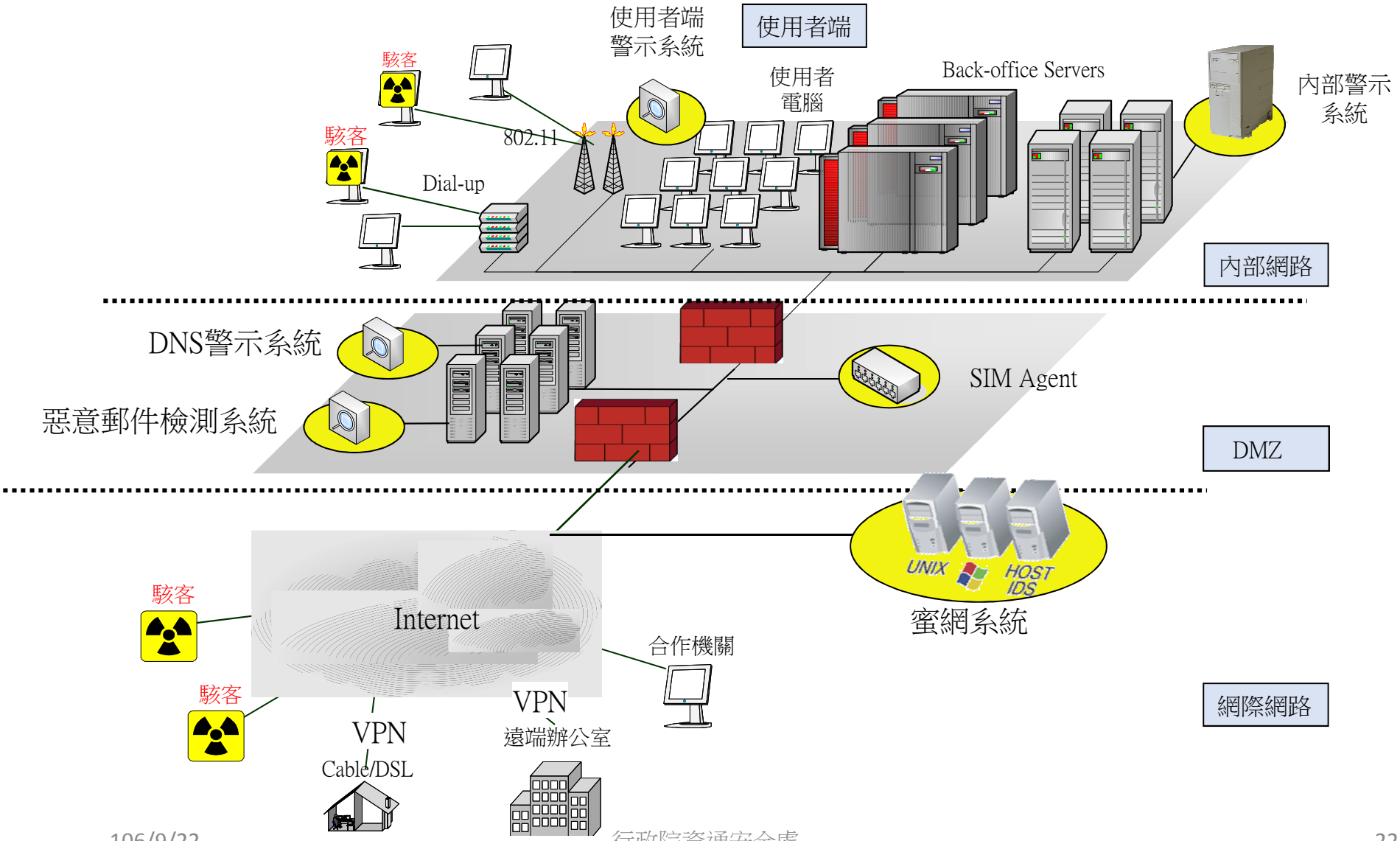
資安治理能力度與成熟度等級

- **能力度等級**：
  - 描繪組織流程於**特定**流程構面中的狀態
  - 以評審各流程構面之能力度
- **成熟度等級**：
  - 描繪組織的整體狀態
  - 用以評審組織之成熟度



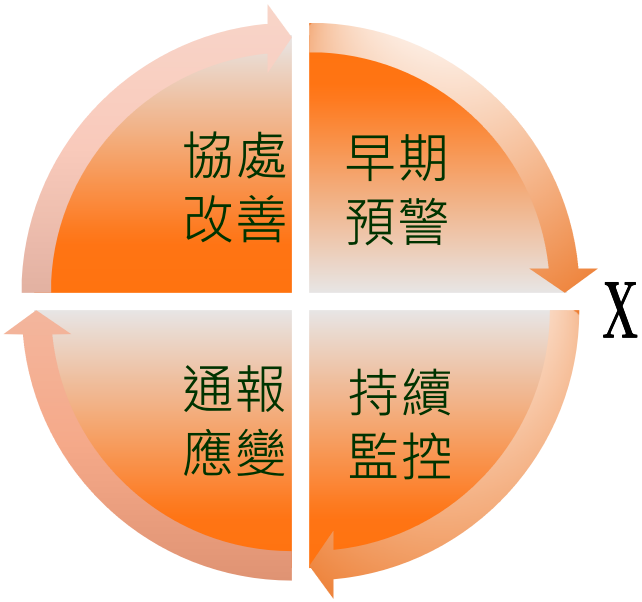
推動策略二：
建構國家資安聯防體系

縱深防禦


使用者端
警示系統
使用者端
駭客
駭客
802.11
Dial-up
使用者
電腦
Back-office Servers
內部警示
系統
內部網路
DNS警示系統
惡意郵件檢測系統
SIM Agent
DMZ
UNIX
HOST
IDS
蜜網系統
駭客
Internet
合作機關
駭客
VPN
VPN
遠端辦公室
Cable/DSL
網際網路

關鍵基礎設施防護

使關鍵基礎設施<u>八大領域</u>均完成資安<u>四大面向</u>整備，建立情報驅動(Intelligence-based)之國家層級資安聯防架構



四大面向

X

八大領域

=

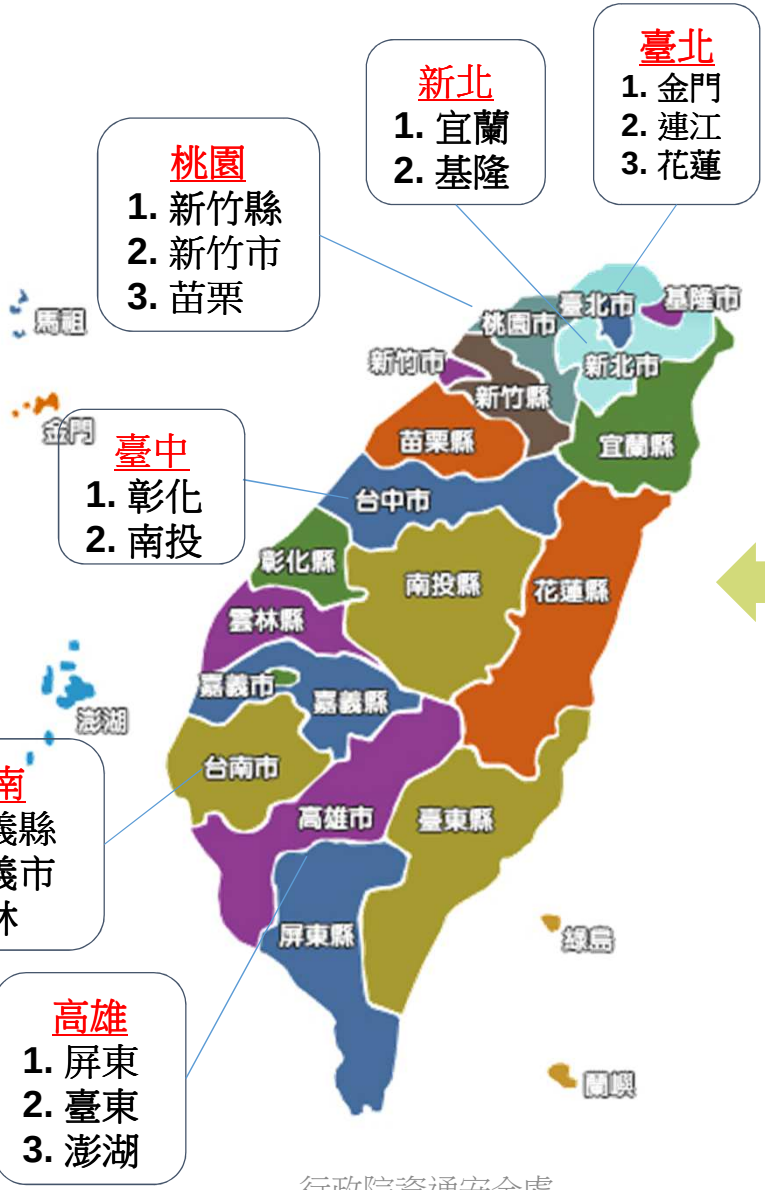
國家資安聯防架構

資安情報驅動三屬性

- 能見度(Visibility)
- 分析能量(Analysis)
- 快速行動(Action)

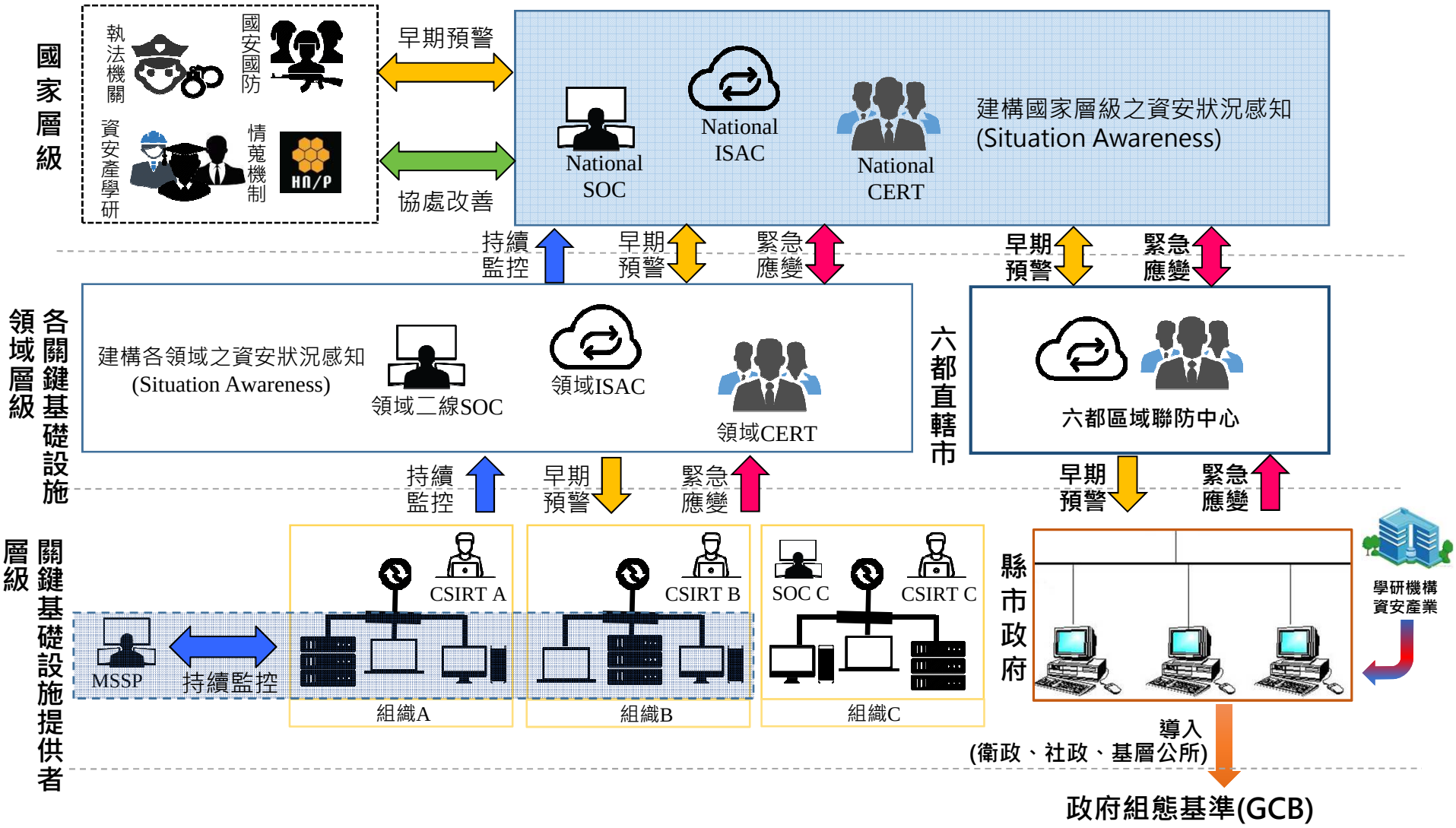
區域資安聯防

研究機構/
國內資安產業



大專院校

資安聯防整體架構


國家層級
執法機關
國安國防
資安產學研
情蒐機制
早期預警
協處改善
National SOC
National ISAC
National CERT
建構國家層級之資安狀況感知 (Situation Awareness)
持續監控
早期預警
緊急應變
早期預警
緊急應變
各關鍵基礎設施領域層級
建構各領域之資安狀況感知 (Situation Awareness)
領域二線SOC
領域ISAC
領域CERT
六都直轄市
六都區域聯防中心
持續監控
早期預警
緊急應變
早期預警
緊急應變
關鍵基礎設施提供者層級
MSSP
持續監控
CSIRT A
CSIRT B
SOC C
CSIRT C
組織A
組織B
組織C
縣市政府
學研機構
資安產業
導入
(衛政、社政、基層公所)
政府組態基準(GCB)

推動策略三：
推升資安產業自主能量

推升資安產業自主能量

資安產業推動策略作法

- 推動雲端運算技術，發展軍民通用資安產品
- 引進人工智慧(AI)，鼓勵資安產業升級轉型
- 鏈結產學研發能量，打造優質資安創新環境
- 培育資安專業人才，加強國際交流互動

我國資安產業發展現況

- 2016年產值：新臺幣351.7億元
- 廠商家數/從業人數：約100家/約4,000人

身分辨識與加解密

• 2016年產值：新臺幣17.8億元

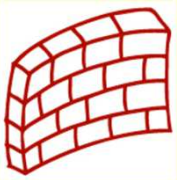

身份識別
存取控制

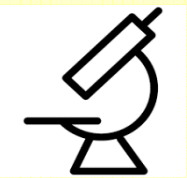

惡意程式
植入後門

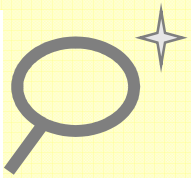

盜取資訊
破壞系統

威脅管理

• 2016年產值：新臺幣135億元


入侵偵測
防禦


威脅監控
分析


系統弱點
掃瞄

系統整合與顧問服務

• 2016年產值：新臺幣83.2億元

- 日誌倉儲
- 事件通報應變
- 資安事件管理
- 每日更新情報
- 快速聯防，阻止事件擴散

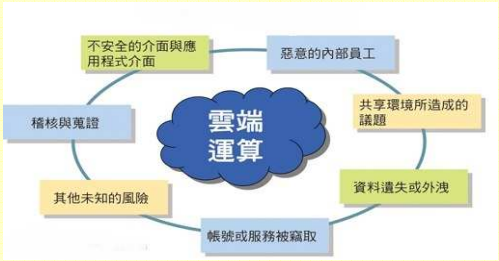
其他產品

• 2016年產值：新臺幣13.1億元

裝置辨識、交易偽冒
資料傳輸安全

專業與其他服務

• 2016年產值：新臺幣18.7億元



共享環境資安議題

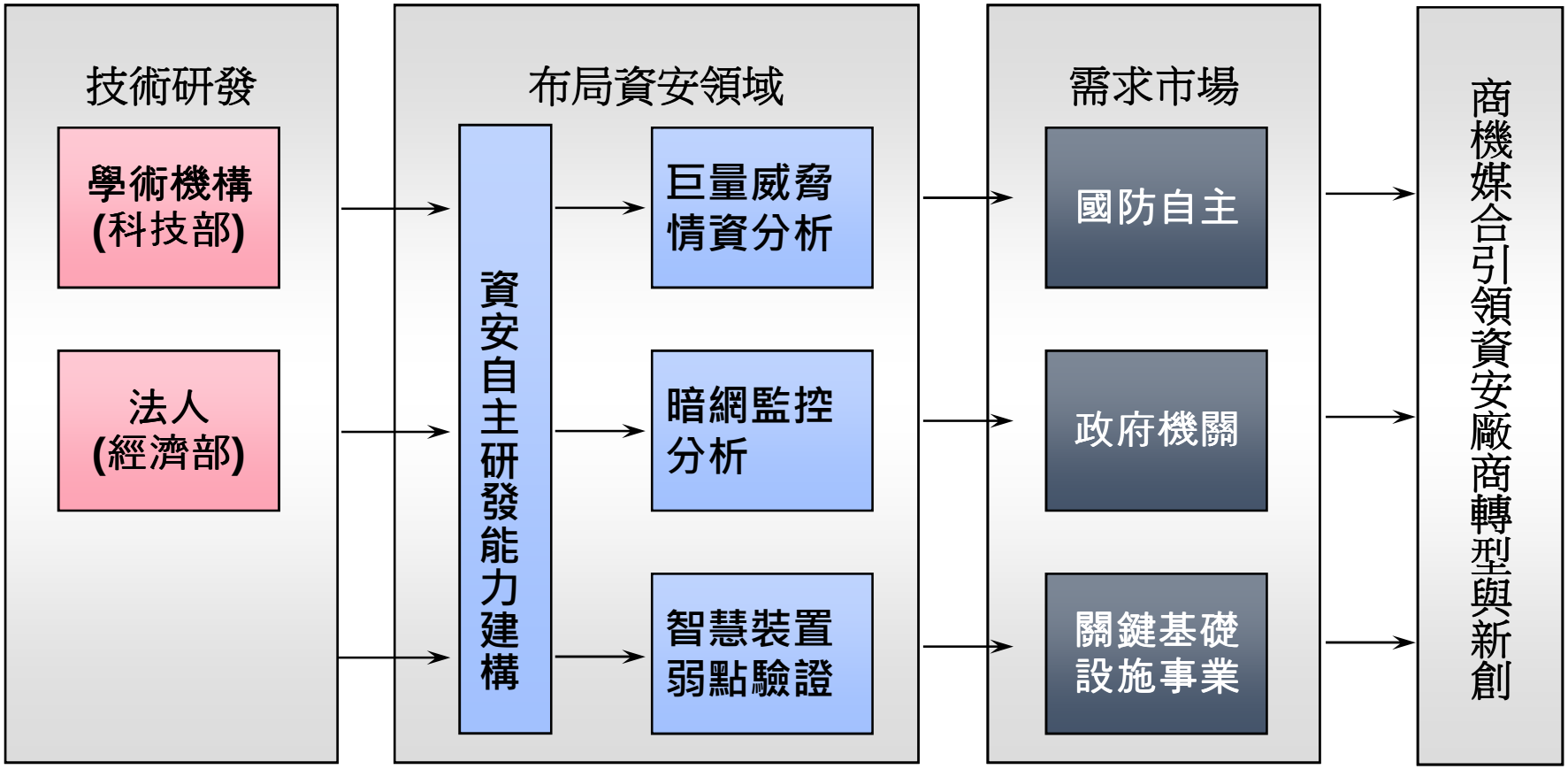
內容防護與資料安全

• 2016年產值：新臺幣83.9億元


防止外部入侵

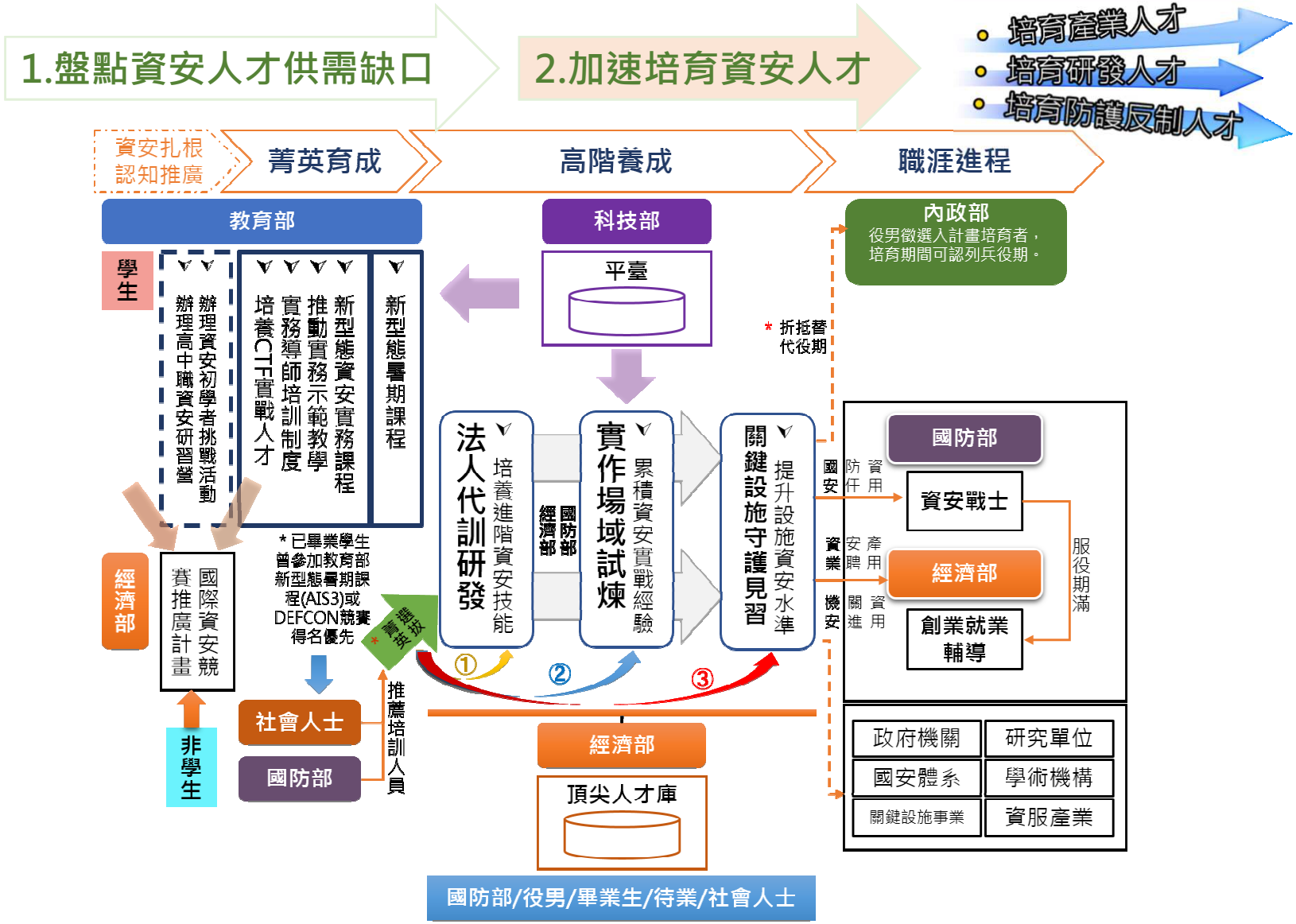

防止內部竊取

結合技術與內需市場之資安產業布局



推動策略四：
孕育資安菁英人才

孕育資安菁英人才


1.盤點資安人才供需缺口
2.加速培育資安人才
培育產業人才
培育研發人才
培育防護反制人才
資安扎根
認知推廣
菁英育成
高階養成
職涯進程
教育部
科技部
內政部
役男徵選入計畫培育者，
培育期間可認列兵役期。
學生
辦理資安初學者挑戰活動
辦理高中職資安研習營
培養CTF實戰人才
實務導師培訓制度
推動實務示範教學
新型態資安實務課程
新型態暑期課程
平臺
* 折抵替代役期
法人代訓研發
培養進階資安技能
實作場域試煉
累積資安實戰經驗
關鍵設施守護見習
提升設施資安水準
國防部
經濟部
國安人才
資安戰士
資業人才
經濟部
創業就業輔導
服役期滿
國防部
資訊戰菁英
* 已畢業學生曾參加教育部新型態暑期課程(AIS3)或DEFCON競賽得名優先
經濟部
國際資安競賽推廣計畫
非學生
社會人士
國防部
推薦培訓人員
①
②
③
經濟部
頂尖人才庫
政府機關
研究單位
國安體系
學術機構
關鍵設施事業
資服產業
國防部/役男/畢業生/待業/社會人士

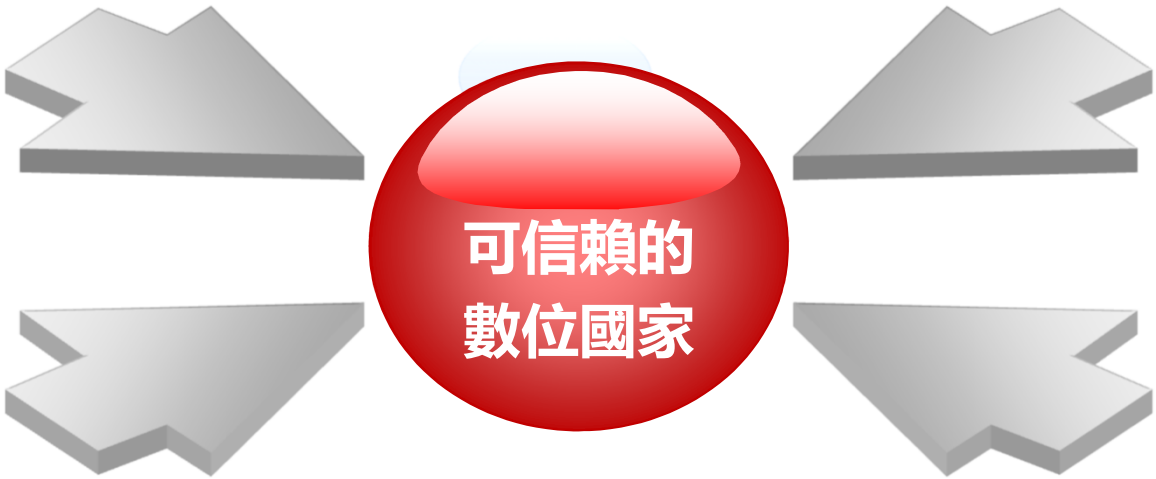
預期效益

預期效益 (1/2)

建構安全可信賴的網際生態體系

研發前瞻AI資安分析能力

推動學研成果產業化



引進國外先進技術

培植國內新創公司

培植政府資安人力

提升治理成熟度

預期效益 (2/2)

建構安全可信賴的網際生態系

- 保障寬頻應用安全及穩定的環境
- 建立IoT檢測標準、環境及機制
- 強化行動應用APP安全檢測機制，確保行動通訊安全
- 建構無人載具安全標準及驗證機制

引進國外先進技術，培植國內新創公司

- 以政府機關需求為基礎，提供國內業者研發誘因
- 協助國外業者技術轉移，提升國內產業量能
- 提升政府機關採購國內自主產品達50%
- 培育產業資安人才2,000人
- 輔導1家資安產業領導廠商於國際露出

民眾

產業

研發前瞻AI資安分析能力

推動學研成果產業化

- 導入AI分析資安大數據，強化自主偵測能力
- 推動前瞻研究，如後量子密碼、DDoS攻擊等
- 建構研究成果產業化環境與機制

學研

政府

培植政府資安人力，提升治理成熟度

- 保障寬頻應用安全及穩定的環境
- 建立IoT檢測標準、環境及機制
- 強化行動應用APP安全檢測機制，確保行動通訊安全
- 建構無人載具安全標準及驗證機制

謝謝聆聽
敬請指教