美國國防部資訊確保檢定與認證程序(DIACAP)初探

作者／資電作戰指揮部資電作戰組 邱述琛 中校

提要

隨著現代科技不斷發展，未來作戰場景必然是由多重維度—陸、海、空、星際、網際等多重網路組成，其資訊傳遞與運用將直接影響任務成敗，而在資訊科技發展迅速的今天，資訊化的普及與資訊安全的威脅也同步的成長，任何一項新資訊技術的採用，都伴隨著未知的資安風險。美國國防部已於 2007 年 11 月 28 日正式發佈了國防部命令(DoDI)8510.01[1]「美國國防部資訊確保檢定與認證程序(DIACAP)」，據以執行美國資訊系統檢定與認證程序，以取得上線運作許可的依據。其實美國與國軍面臨的挑戰是一樣的，其發展方向與重點也是一致的，而美軍對資訊確保的定位與重視、資訊確保執行面的規劃與落實、資訊確保與系統籌獲生命週期的整合及對資訊確保人員資格的要求等，值得國軍作為後續精進之借鏡與參考。

壹、 前言

美國國防部已於 2007 年 11 月 28 日由正式發佈了國防部命令(DoDI)8510.01「美國國防部資訊確保檢定與認證程序(DIACAP，以下簡稱資訊確保檢定與認證程序)」，並參酌美國「聯邦資訊安全管理法案[2](FISMA)」、國防部指令(DoDD)8500.01E[3]「資訊確保」、國防部指令(DoDD)8100.1[4]「全球網格架構政策」及國防部命令(DoDI)8500.2[5]「資訊確保施行」，作為美國資訊系統建立檢定與認證程序，並取得上線運作許可的依據。此命令用以管理資訊確保能力與服務之施行，並提供國防部資訊系統上線認證決定之可見度。(可信性)

在本命令中，明確宣告美國國防部以下的政策：

一、國防部須依照國防部命令(DoDI)8500.2「資訊確保施行」中訂定之資訊確保安控措施，透過「識別」、「施行」及「管理」資訊確保能力與服務，來檢

[1]美國國防部資訊確保檢定與認證程序：DoD I 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28,2007。

[2]美國聯邦資訊安全管理法案：Subchapter III of Chapter 35 of title 44, United States Code, Federal Information Security management Act (FISMA) of 2002。

[3]美國國防部指令 8500.01E 資訊確保：DoD Directive 8500.01E Information Assurance (IA), October 24, 2002。

[4]美國國防部指令 8100.1 全球網格架構政策：DoD Directive 8100.1 Global Information Grid(GIG) Overarching Policy, September 19, 2002。

[5]美國國防部命令 8500.2 資訊確保施行:DoD Instruction 8500.2 Information Assurance(IA) Implementation, February 6, 2003。

定與認證資訊系統。這些資訊確保安控措施須考量全球網格之架構與風險評鑑，並以全國防部之構型控制與管理程序予以管制。

二、資訊確保檢定與認證程序須支援國防部資訊系統傳移至全球網格標準與網路中心化環境，以確保達到資訊共享之目的。

三、所有擁有上線運作許可的國防部資訊系統必須每年進行檢視，以確保其資訊確保(資訊安全)維持在可接受的狀態。

四、用以施行資訊確保檢定與認證程序的資源，須在國防規劃、專案、預算與執行程序中明確律定。

五、本命令中涵括之系統、服務與專案之合約中，須述明符合資訊確保檢定與認證程序之要求；未述及此條文，亦不得作為不符本程序之辯證理由。

綜合以上的說明可以發現，美軍已明確宣告其資訊系統必須依其等級採取適當之資訊確保安控措施，並進行檢定與驗證程序，通過後每年亦須重覆檢視其資訊確保狀態，以確保其安全性。在今日資訊科技日新月益、資安威脅不斷翻新之際，美軍的作法勢必造成資源的投注，然美軍於作戰安全的考量下，仍以政策律定這些必要之作為，顯然可知，作不作，已不是決策重點，重點在於如何以最小的投資，換取最大的效益，才是問題的關鍵！

貳、 本文

美國國防部資訊確保檢定與認證程序(DIACAP)

一、美國國防部資訊確保政策發展歷史

美國國防部資訊確保(Information Assurance, IA)政策自 1970 年代即開始發展，當時即有「自動資料處理系統安全需求(DoDD 5200.28)」及相關手冊；隨著資訊科技的進步，資訊安全的需求日益獲得重視，到了 1985 年，發展出了「可信賴電腦系統評估準則」，也就是資安界著名的「橘皮書」；在 2000 年美國防部訂定了「國防部全球網格資訊確保指引(DoD CIO G&PM 6-8510)」試行；2 年之後，也就是 2002 年，由國防部陸續簽署了資訊確保政策及建置系列文件(DoDD 8500 Series)。由此可知，美國國防部目前執行資訊確保工作以 8500 系列之命令作為主要依據。

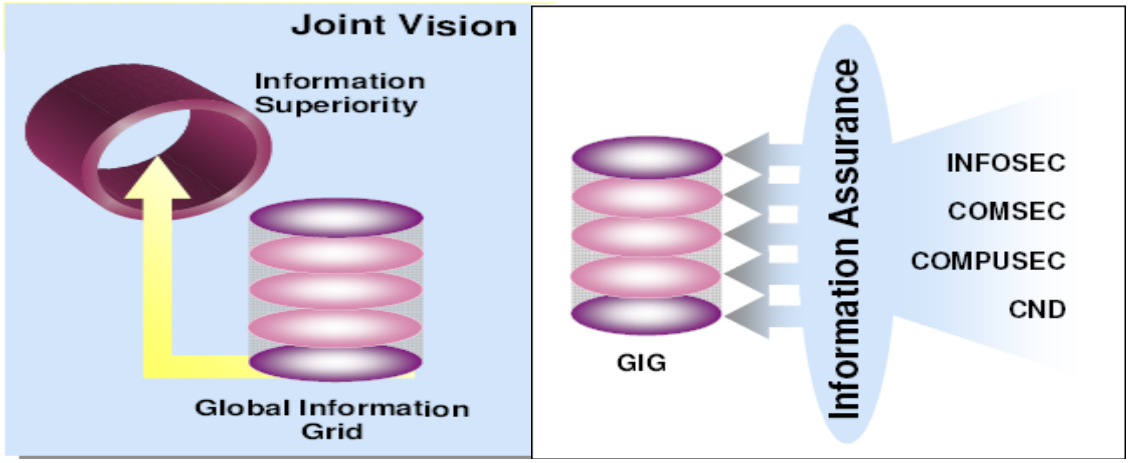
二、資訊優勢與資訊確保的相依性

美軍已將其 2010 之聯戰願景(Joint Vision)延至 2020 年，並以結合科技創新之「資訊優勢(Information Superiority)」作為基礎，爭取達到全方位主導(Full Spectrum Dominance)之目標；而全球資訊網格(GIG)已取代全球資訊基礎建設(GII)，成為爭取資訊優勢的基礎建設。美國已瞭解必須藉由全球性的相互連結，

有效聯結派駐世界各地終端的國防資訊能力，才有可能爭取到真正的資訊優勢，而由資訊安全(INFOSEC)、通訊安全(COMSEC)、電腦安全(COMPUSEC)及電腦網路防禦(CND)共同組成的資訊確保，則更是確保成功的關鍵成功要素。(聯戰願景如圖一、全球網格與資訊優勢關係如圖二)

Joint Vision:聯戰願景／Information Superiority:資訊優勢／Technology Innovation:科技創新
Dominant Maneuver:優勢機動／Precision Engagement:精準接戰／Focused Logistics:聚焦後勤
Full-Dimensional Protection:全維度防護／Full Spectrum Dominance:全方位優勢／
Joint Forces Coalition Partners: 聯戰部隊聯合夥伴

圖一 美國 2010~2020 年聯戰願景圖（資料來源：美國空軍 2003 年 BCOT 訓練教材）



Global Information Grid(GIG):全球網格／Information Assurance:資訊確保
INFOSEC:資訊安全／COMSEC:通訊安全／COMPSEC:電腦安全/ CND:電腦網路防禦

圖二 全球資訊網格與資訊優勢關係示意圖（資料來源：http://www.sstc-online.org/proceedings/2005/PDFFiles/CHL965.pdf.）

三、未來作戰場景

隨著現代科技不斷發展，未來作戰場景必然是由多重維度—陸、海、空、星際、網際等多重網路組成，其資訊傳遞與運用將直接影響任務成敗。資訊確保必須擔負起資訊傳遞之「一致性」、「完整性」、「可用性」、「確認性」、「不可否認性」、「正確性」、「時效性」等要求，扮演著足以影響成敗的地位。由此可知，因資訊優勢與資訊確保具有高度的相依性，在未來的戰場之中，如果無法作到足夠

程度的資訊確保作為，可能會發生遭惡意程式攻擊、電磁輻射干擾、資訊格式不一致，影響作戰互通力、作戰網路遭到滲透、電磁頻譜管理不良等情況。每一種狀況，都將影響最終戰果。

四、系統籌獲政策與資訊確保的關係

美國系統籌獲政策以國家安全空間籌獲政策 03-01 為最高指導原則;國防資訊系統籌獲則以國防部命令(DoDI)5000 系統作為執行依據；而資訊確保相關作為則以國防部命令 8500 系列為基礎。綜上所述可以瞭解，資訊確保的行動必須與系統籌獲程序緊密的結合，除須在生命週期全程中，投入適當的經費外，在系統籌獲初期，更是要決定國防資訊系統任務確保類別及其對應的資訊確保安控措施，然後依律訂之評估程序驗證其效果後，才能獲得安全穩固的系統。

在美國系統籌獲政策最高指導之國家安全空間籌獲政策 03-01 中,已訂定了各階段資訊確保與專案防護應辦理之基本工作項目(如表一),提供作為各單位執行的依據。

表一　各階段資訊確保與專案防護辦理工作項目表(作者翻譯整理)

	關鍵決策點(KDP)前概念研究	A階段 概念發展	B階段 初步分析	C階段 完成設計	D階段 建造營運
資訊確保	分析作戰概念之資訊確保需求	進行IA策略規劃並開始系統安全授權協議、註冊系統	更新IA策略規劃及系統安全授權協議、發展IA需求及管理與執行計畫		支援IA測試、完成系統安全授權協議、提出系統營運許可請求
專案防護		系統弱點防護手段初步評估	更新專案防護規劃	更新專案防護規劃	

(資料來源：美國國家安全空間籌獲政策 03-01)

五、資訊確保檢定與認證程序

(一)發展原因：

1.符合法規要求：依聯邦資訊安全管理法案(FISMA)之要求，資訊系統應每年進行檢視。

2.支援網路化作戰及全球網格：作戰型態隨科技進步而改變，目前已朝網路化作戰及全球網格發展，考量其技術架構，並進行風險評估，藉以建立全國防部的構型管理程序。

3.單一系統移轉至系統整體運作：原本以單一資訊系統或服務為導向，隨著

系統整合、資訊分享而調整為整體作業環境之程序。

(二)重要術語說明：

1.指定核准授權機構(DAA)：從資訊安全風險觀點評估系統任務、業務情形及預算需求後，決定可接受的殘餘風險程度，下達核准系統上線運作決定的授權機構。

2.資訊確保經理(IAM)/檢定授權機構(CA)：管理驗證程序，進行技術與非技術驗證評估作業，並回報驗證狀況並提供認證結果之建議。

3.專案經理(PM)/系統經理(SM)：在生命週期全程中，實際負責系統權益的代表。

4.使用者代表(UR)：使用系統進行任務之代表，關切系統可用性、完整性及機密性。

5.驗證者(Validator)：測試系統是否符合資訊確保管控措施，以確保系統符合安全需求。

6.機密等級(CL)：用於決定可接受的存取因素，包括：個人安全聲明或背景調查的需求、存取的核准、因需要而知悉(Need-to-Know)的決定、管控措施與核准的連結、使用者可能存取系統可接收的方式。

表二　機密等級定義表(作者翻譯整理)

機密等級	定義
機密	系統處理機密資訊需要之高等級
敏感	系統處理敏感資訊需要之中等級
公開	系統處理公開資訊需要之一般等級

(資料來源：US DoDI 8500.2)

7.任務確保種類(MAC)：代表達成美國國防部目標與目的相關資訊的重要性，特別是戰士的作戰任務。一般用於定義系統可用性與完整性的需求，各任務確保種類需求等級及定義如表三。

表三　任務確保種類定義表(作者翻譯整理)

任務確保種類MAC	完整性需求等級	可用性需求等級
MAC I	高	高
定義：系統處理資訊在內容及時效，均對佈署及應變部隊之作戰準備或任務有效性，具有巨大的影響；喪失完整性或可用性是不能被接受的，可能造成任務有效性立即或持續的損害。		

MAC II	高	中
定義：系統處理資訊對佈署及應變部隊是重要的；喪失完整性是不能被接受的；喪失可用性僅能容許極短的時間		
MAC III	基本	基本
定義：系統處理資訊對每日營運是必需的，但在短時間內對佈署及應變部隊不會造成實質影響；對作戰準備或任務有效性不會造成巨大影響。		

(資料來源：US DoDI 8500.2)

(三)資訊確保管控措施(IA Control)：每個美國國防部的資訊系統都要指定其任務確保種類(MAC)及機密等級(CL)，並由此兩者共同決定資訊確保管控措施；資訊確保管控措施是資訊確保驗證與認證的基準，其主題領域與管控措施數目如表四：

表四　資訊確保管控措施主題領域與管控措施數目表(作者翻譯整理)

縮寫	主題領域名稱	管控措施數量
DC	安全設計與構型	31
IA	辨別與確認	9
EC	系統範圍與運算環境	48
EB	系統範圍邊界防禦	8
PE	實體與環境	27
PR	人員	7
CO	持續性	24
VI	弱點與意外管理	3

(資料來源：US DoDI 8500.2)

(四)活動循環：包括「啟動與規劃」、「建置與驗證選定的資訊確保管控措施」、「下達驗證的判定並核發認證的決定」、「維護上線許可並執行重新檢視」及「汰除」等 5 個活動，各活動中執行工作簡單說明如后：

1.啟動與規劃：其活動內容包括向美國防部相關部門資訊確保專案註冊系統、選定資訊確保管控措施、組成資訊確保驗證與認證程序工作團隊、啟動資訊確保驗證與認證程序建置計畫。

2.建置與驗證選定的資訊確保管控措施：其活動內容包括執行資訊確保驗證與認證程序建置計畫、執行驗證的行動、準備修正行動與里程碑計畫(Program of Action & Milestone, POA&M)、匯集驗證的結果並登錄於資訊確保檢定與認證程

序計分表(Scorecard)。

3.下達驗證的判定並核發認證的決定：其活動內容包括下達驗證的判定、核發認證的決定。

4.維護上線許可(Authorization to Operate, ATO)並執行重新檢視：其活動內容包括維護狀況覺知(Situation Awareness)、維護資訊確保狀態—至少每年重新檢視資訊確保狀態、重新認證。

5.汰除：系統汰除。

(五)各活動工作：資訊確保檢定與認證程序工作流程中，可分為 5 個活動，共計包括 18 項工作(如表五之一～七)，各項工作之內容、具體產出及主要負責人說明如后：

1.啟動與規劃資訊確保檢定與認證程序：

表五之一(作者翻譯整理)

順　序	1	2	3	4
工　作	啟動工作流程：註冊系統及組成團隊	選定資訊確保管控措施及其它需求	進行系統生命週期狀態及組態分析(或啟動 DIP)	同意 DIP
產　出	系統識別概況(SIP)	資訊確保管控措施使用清單	DIP	
負責人	(主)PM	(主)PM	(主)PM	(主)PM

(資料來源：美國國防部資訊確保檢定與認證程序工作流程)

DIP(DIACAP Implementation Plan)：資訊確保檢定與認證程序執行計畫／PM(Program Manager)：專案經理／SIP：系統識別剖繪(System Identification Profile)

2.執行資訊確保驗證與認證程序建置計畫(DIP)：

表五之二(作者翻譯整理)

順　序	5	6	7
工　作	驗證資訊確保管控措施	對驗證行動中獲得結果與預期結果進行分析與比較	發展 POA&M
產　出	驗證結果	POA&M(如需要)	POA&M
負責人	(主)PM 及驗證者	(主)驗證者	(主)PM 與使用者代表

(資料來源：美國國防部資訊確保檢定與認證程序工作流程)

POA&M(Program of Action & Milestone)：修正行動與里程碑計畫

表五之三(作者翻譯整理)

順　序	8	9
工　作	匯集驗證結果	PM 綜整及檢視全部的資訊確保檢定與認證程序工作
產　出	資訊確保檢定與認證程序計分卡	資訊確保檢定與認證程序工作狀況及風險評鑑
負責人	(主)驗證者	(主)PM

(資料來源：美國國防部資訊確保檢定與認證程序工作流程)

3.驗證判定與認證決定：

表五之四(作者翻譯整理)

順　序	10	11	12
工　作	進行初步的驗證檢視	進行驗證判定	核發認證決定
產　出	驗證建議(簽署信)	驗證判定	認證決定(ATO、IATO、IATT、DATO)
負責人	(主)CA	(主)CA	(主)DAA

(資料來源：美國國防部資訊確保檢定與認證程序工作流程)

IATO(Interim Authorization to Operate)：暫時上線許可／IATT(Interim Authorization to Test)：暫時測試許可／DATO(Deny Authorization to Operate)：否決上線許可

表五之五(作者翻譯整理)

順　序	13			
工　作	ATO-系統上線許可	IATO-執行POA&M(如需要)	IATT-在特定時間進行實際測試(如需要)	NTO-修正DIP(如需要)
負責人		(主)PM 與驗證者	(主)PM 與驗證者	(主)PM 與驗證者

(資料來源：美國國防部資訊確保檢定與認證程序工作流程)

4.維護上線許可(Authorization to Operate, ATO)並定期檢視：

表五之六(作者翻譯整理)

順　序	14	15	16
工　作	維護資訊確保狀態	年度檢視	重新認證(每 3 年)
產　出		IA 管控措施檢視報告	認證決定
負責人	(主) PM 與驗證者	(主) PM 與驗證者	(主) PM

(資料來源：美國國防部資訊確保檢定與認證程序工作流程)

5.汰除：

表五之七(作者翻譯整理)

順　序	17	18
工　作	決定是否汰除	汰除

(資料來源：美國國防部資訊確保檢定與認證程序工作流程)

六、檢定與認證程序的移轉方式

美軍驗證與認證(C&A)程序在資訊確保檢定與認證程序(DIACAP)公佈前，係使用國防資訊科技安全檢定與認證程序(DITSCAP)執行單一系統之資訊安全檢定與認證，因應資訊科技的進步、資訊分享及系統整合日益增加的需求，精進調整。惟任何軍用資訊系統籌獲時間都很長的，在兩個不同的程序間，美軍也訂定了 6 項移轉規則，以作為各單位進行程序移轉時作為執行依據。移轉規則說明如后：

(一)新開始或營運中的美國國防部資訊系統(尚未展開 DITSCAP 活動)等未認證系統—立即啟動資訊確保檢定與認證程序。

(二)美國國防部擁有 DITSCAP 上線許可的資訊系統，運作已超過 3 年—立即啟動資訊確保檢定與認證程序。

(三)美國國防部資訊系統已開始 DITSCAP 程序，但尚未獲得第 1 階段系統安全授權協議(SSAA)之簽署—立即移轉至資訊確保檢定與認證程序。

(四)美國國防部資訊系統已開始 DITSCAP 程序，且已獲得第 1 階段系統安全授權協議(SSAA)簽署—在 2007 年 1 月 6 日前，修正 SSAA，強調重新認證的需求；並描述系統移轉制資訊確保檢定與認證程序之策略及期程，移轉期程不可超過系統重新認證的時間(3 年)限制；年度的檢視以符合 FISMA 的回報需求。

(五)美國國防部資訊系統已開始 DITSCAP 程序，已獲得第 1 階段系統安全授權協議(SSAA)簽署，並已開始第 2、3 階段作業(尚未得到認證決定)，SSAA 需求追溯矩陣表(RTM)國防部命令 8500.2 列舉之 IA 管控措施不完全符合—持續 DITSCAP 程序，在 2007 年 1 月 6 日前修正 DITSCAP 之 RTM，符合國防部命令 8500.2 列舉之 IA 管控措施，並發展執行計畫，DITSCAP 認證決定不需要符合所有的 IA 管控措施，但系統須提供其符合程度之可見性及達到完全符合之可行計畫。此外，修正系統安全授權協議，強調重新認證的需求；並描述系統移轉制資訊確保檢定與認證程序之策略及期程，移轉期程不可超過系統重新認證的時間(3 年)限制。

(六)美國國防部擁有 DITSCAP 上線許可的資訊系統，運作在 3 年內—在 2007

年1月6日前建立系統移轉制資訊確保檢定與認證程序之策略及期程，DITSCAP之RTM不完全符合國防部命令8500.2列舉之IA管控措施，資訊系統應提供授權認證授權機構其一致性評估；如上線許可是暫時性，則持續DITSCAP程序以獲得正式許可。

美國國防部已訂定了明確的時間限制與移轉規則，供各單位在執行移轉工作時執行，也讓審定及稽核工作之執行有所依循。

參、 結論與建議

一、 結論

(一)美軍明確律定系統籌獲及資訊確保執行基準

美軍系統籌獲及資訊確保執行係依據國防部命令 5000 及 8500 系列的政策、技術文件作為指導及依據，在部隊組織中絕大多數人並非資訊專業人才的實際環境中，相關基準文件對於任務執行具有絕對的幫助。然而面對如此龐大的文件架構，勢必需要足夠的技術人力來支撐、維護，並隨時跟著最新技術的發展，研擬出應該採行的標準及移轉的程序，這也是美國國防資訊系統局(DISA)所扮演的重要角色。

(二)系統上線許可(ATO)與年度檢視

美國國防部所有的資訊系統都必須指定任務確保種類與機密等級，並據以選用相關的資訊確保管控措施，在經過驗證與認證程序後，必須獲得指定的核准授權機構(DAA)的上線許可(Authorization to Operation, ATO)後，系統才能上線運作。獲得上線許可後，系統每年還要進行資訊確保的檢視，針對最新威脅及弱點的發展，評估是否需要進行新的驗證與認證作業，另每 3 年系統都必須重新進行認證程序，以確保系統的安全性。美軍即是面對目前資訊科技發展迅速及威脅日增的實際環境下，因應作戰任務的需要，採取必要的作為。

(三)系統籌獲風險評估方式

美軍在系統籌獲時會執行相關的風險評估，其認為完全避免風險幾乎是不可能或是不符作戰需求或投資效益，故其採取的方式是參酌系統任務、架構、運作環境與系統安全目標後，承受可接受的風險程度。其採取的步驟說明如后：

1.定義系統：就任務及架構考量，必須進行防護的能力。

2.資產的辨識與量化：評估資產在機密性、完整性及可用性受到影響時所造成的衝擊。

3.辨識威脅：辨識人為、機械、天然、蓄意、非蓄意等。

4.辨識管控措施：辨識那些實體、行政管理與技術的管控措施必須執行。

5.辨識殘存的弱點：辨識那些弱點尚未/或不能被減低。

6.建立目前風險權重：評估威脅利用殘餘弱點可能造成的風險。

7.決定/調整建議的額外的對應作法。

(四)明確訂定系統資訊確保管控措施基準

依美軍 DoDI 8500.2 之規定，按任務確保種類與機密等級不同，其應採取的資訊確保管控措施統計如表六。自最低的 75 項，到最高的 115 項，訂定的十分明確，每一個系統依據其分類，可以依此標準選定適用之資訊確保管控措施，而後續的驗證與認證程序，亦以此作為基準。美軍作法可提供國軍對後續系統資訊確保管控機制選用及檢、認證之參考。

表六 美軍系統資訊確保管控措施基準統計表(作者翻譯整理)

MAC \ CL / Control		機密等級(CL)		
		高(45)	中(37)	基本(11)
MAC 任務確保種類	MAC I(70) 高完整性／高可用性	115	107	81
	MAC II(70) 高完整性／中可用性	115	107	81
	MACIII(64) 基本完整性／基本可用性	109	101	75

(資料來源：US DoDI 8500.2)

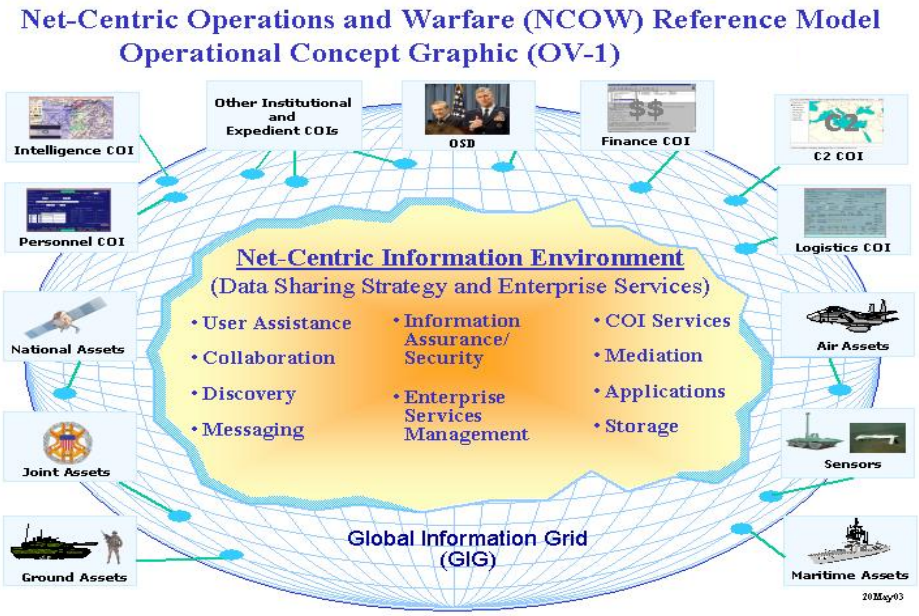
(五)結合商用資源，運用最新科技

資訊科技發展訊速，美軍從最早自行發展所有的軍規標準，已轉變為大量評估引用最新資訊科技的商規標準，除了樽節國防資源外，另外也是顧及資訊科技的重要特性—互通性，也就是在不同的標準間，使用相同的通訊協定、資料型式，以進行相互整合。在網路化作戰及全球網格的作業型態中，互通性更是重點中的重點，必須讓需求單位在適當的時間、地點，存取到所需的資訊。美軍在這方面大量的運用商用資源，將一些不具機敏性，技術面或程序面的發展，委託或運用成熟的商用標準，是一項值得參考的作法。

二、建議

(一)參考美軍網狀化戰爭參考模型—NCOWRM 作戰觀點(OV-1)示意圖(如圖3)可以明確的瞭解，資訊確保擔負所有資訊系統支援任務執行的重要關鍵，提供作戰指揮官系統的可用性，並可以信任系統傳遞資訊之完整性及保密性。所以美軍才會律定在任何資訊系統上線前，都要執行驗證與認證程序，並獲得正式的上線許可後，才可運作。而獲得上線許可後，每年還要進行安全檢視，每 3

年要重新進行認證，以確認系統可因應最新的威脅，並將風險降至可接受的程度。這項作業勢必耗費大量的人、物力資源，但在實際的作戰環境中及考量未來網狀化作戰中，資料共享的需求，若無法確保聯結系統間之資訊確保狀態，作戰指揮官將無法下達同意系統整合的決心，因為資訊確保必須支持作戰安全。國軍近期正導入網路化作戰概念並籌建指管通資情監偵(C4ISR)系統，在後續系統整合規劃時，務須將「資訊確保」列入考量，以免影響任務遂行。美軍累積多年實戰經驗之作法，值得國軍參考。



Net-Centric Information Environment:網狀中心化資訊環境／User Assistance:用戶協助

Data Sharing Strategy and Enterprise Services:資料共享策略與企業服務／Collaboration:合作

Discovery:資料搜尋／Messaging:訊息傳遞／Information Assurance(Security):資訊確保(安全)

Enterprise Services Management:企業服務管理／COI Services:利害共同體管理

Mediation:衝突斡旋／Application:應用程式/Storage:資料存儲

圖三 網路化作戰與戰爭參考模型 OV-1 示意圖（資料來源：http://www.aiaa.org/Participate/Uploads/JZ@AIAA%20NCOPC%20May%2005.ppt）

(二)資訊系統資訊確保作為是系統籌獲生命週期中一項不可缺少的環節，在系統籌獲階段中，資訊確保應執行的工作包括了：決定與檢視資訊確保籌獲策略、選用任務確保種類、選定機密等級、執行驗證與認證作業、執行與驗證資訊確保管控措施、決定驗證結果、發佈認證結果等。絕對不是將資訊確保獨立於系統之外，單獨建置一些防火牆、入侵偵測、防毒系統及保密器就完成的，而是與系統功能需求整合後進行週詳的評估，才是正確的作法。資訊系統籌獲程序如可結合資訊確保之需求，將可收事半功倍之效。更進一步說，資訊確保的需

求在系統開始規劃時，就應該進行考量，並與作戰需求、系統功能需求一同進行功能分析，並整體評估並權衡資訊確保管控措施與其它功能之衝突，才能獲得成功的系統。美軍之作法，值得國軍參考。相關作業示意圖如圖七；而資訊確保能力更應在啟始能力文件(ICD)，以前之任務需求聲明中就加以訂定，以作為後續執行之依據，資訊確保能力與系統籌獲重要文件關係示意圖如圖八。

(三)資訊確保工作具有高技術性之特質，參考美軍對其資訊人員之資格訂有明確的要求，除了電腦環境技術及管理人員可由無經驗之新進人力擔任外，餘網路及資訊系統環境之技術、管理人員均需 3 至 10 年不等之工作實務經驗，方可擔任相關職務。美軍資訊人員工作經驗需求表如下。此外，美軍亦對各等級人員應取得之認證資格訂有明確規範(如表七)，觀察其要求之認證類別，絕大多數的認證均為國際資訊安全組織或機構所採用之標準，像是國際資訊系統安全標準聯盟(ISC2)的認證資訊系統安全專業人員(CISSP)、資訊安全認證從業人員(SSCP)；系統管理與網路安全組織(SANS)的國際資訊確保資訊安全基礎(GISF)、國際資訊確保認證安全基本認證(GSEC)、國際資訊確保認證安全領導認證(GSLC)、國際資訊確保認證安全專家(GSE)；資訊系統稽核與管控協會(ISACA)的認證資訊安全稽核員(CISA)及認證資訊安全管理者(CISM)。科技的管控措施需要的是國際組織的認證標準，這些認證，代表著執行能力客觀的證明，若是在軍事制度中建立這些認證標準，要隨著最新科技的進步隨時調整課程內容、培養師資，是不符合經濟效益及實際需求的。其實就使用者的角度而言，選用適當的認證標準是最經濟的方式，所以美軍的作法是建立比照制度及任用基準。國軍的任職條例中，仍是以軍事學資作為主要標準，在專業的領域中，建議可以參考美軍的作法，考量實務面的作業需求及優先順序，訂定比照制度及任用基準，以完成任務。

表七 美軍資訊確保人員工作經驗需求表(作者翻譯整理)

	技術	管理
等級 1(電腦環境)	0~4 年經驗	0~5 年經驗
等級 2(網路環境)	3~7 年經驗	5 年以上經驗
等級 3(資訊系統範圍)	7 年以上經驗	10 年以上經驗

(資料來源：US DoD 8570.01-M)

(四)美國國防部按任務確保種類與機密等級之不同，明確訂定其應採取之資訊確保管控措施基準，並以「DoDI 8500.2 資訊確保履行」頒佈執行。而每一項資訊確保管控措施均經國防部之評估，並賦予其衝擊代碼(Impact Code)。其目的在明確的告知使用單位此管控措施可能造成之衝擊，並據以作為後續系統是否通

過檢定與認證之參據。此規定律定之資訊確保管控措施基準，為美國防部評估殘存風險後可接受之最低標準。美軍此類由上而下自政策面發起，具體律定執行方式之作法，深值國軍後續籌建軍用系統之參考。

(五)國軍系統正進行大幅資訊化及整合，其面臨的資安威脅亦不斷改變，必須藉定期檢視，才能確保系統安全。美軍的作法提醒了國軍，資訊確保的工作，在系統生命週期中是不斷在執行，隨時檢視、認證，如此才能真正作到「資訊確保」。

(六)檢視美軍之作法與國軍目前推動的資訊安全管理系統(ISMS)精神是一致的，都是以資產為核心，惟美軍於資訊系統籌獲生命週期中，即已融入此觀念，國軍目前仍以推動通過 ISMS 認證為重點，若是能將風險評估的動作結合到系統籌獲程序並加上定期的檢視，相信將能獲致更大的效益。

肆、 預期成果

在資訊科技發展迅速的今天，美軍與國軍面臨的挑戰是一樣的，其發展方向也是一致的。美軍對資訊確保的定位與重視、資訊確保執行面的規劃與落實、資訊確保與系統籌獲生命週期的整合及對資訊確保人員資格的要求等，都值得國軍精進之借鏡。

參考資料

一、 美國國防部資訊確保檢定與認證程序工作流程，http://isae.disa.mil/ditscap/diacap-workflow.pdf。

二、 系統管理、稽核與網路安全 2007 年會 DIACAP 授課教材：SANS 2007 DIACAP Training Material。

三、 美國空軍 2003 通資參謀軍官班授課教材：USAF BCOT Training Material, 2003。

四、 系統與軟體科技會議(System & Software Technology Conference, STC)之資訊確保、籌獲與全球網格(IA, Acquaistion & GIG)，http://www.sstc-online.org/proceedings/2005/PDFFiles/CHL965.pdf。

五、 MORS IA OperationsWorkshop 之「資訊確保於美國國防部系統籌獲與測試」：資料來源 http://www.mors.org/meetings/2007_tia_pres/christensen.pdf。

六、 超越科技互通與指管通資情監偵之網路中心化與網路備便(Net-Centricity & Net-Ready-Beyond Technical Interoperability & C4ISR)，http://www. aiaa.org/Participate/Uploads/JZ@AIAA%20NCOPC%20May%2005.ppt。