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草案總說明

為配合一百零八年六月二十六日公布之電信管理法第八十七條第二項及第三項規定，並落實政府再造有關政府業務委外辦理之政策，復為確保受託對象辦理測試及驗證作業之品質與公信力，爰依前揭規定之授權，擬具「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」草案，共計十八條，其要點如下：

一、本辦法之訂定依據。(草案第一條)

二、本辦法之名詞定義。(草案第二條)

三、測試機構及其人員之資格條件、測試作業。(草案第三條)

四、測試機構之監督管理事項。(草案第四條)

五、驗證機構及其人員之資格條件。(草案第五條)

六、驗證機構申請程序。(草案第六條)

七、驗證機構實地評鑑。(草案第七條)

八、驗證機構之委託契約。(草案第八條)

九、驗證機構及其人員遵守事項。(草案第九條)

十、驗證機構受託辦理事項及抽驗機制。(草案第十條)

十一、 驗證機構之監督管理事項。(草案第十一條至第十五條)

十二、 驗證機構電子化系統建置。(草案第十六條)

十三、 驗證機構審驗費用相關要求。(草案第十七條)

十四、 本辦法之施行日期。(草案第十八條)

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草案

條　文	說　明
第一條　本辦法依電信管理法（以下簡稱本法)第八十七條第二項及第三項規定訂定之。	本辦法之訂定依據。
第二條　本辦法用詞定義如下： 一、關鍵電信基礎設施資通設備(以下簡稱資通設備)：主管機關依本法第四十二條第八項公告之技術規範規定之設備。 二、測試機構:指依前款技術規範辦理資通設備測試作業之機構。 三、驗證機構:指經主管機關委託辦理資通設備審驗作業之機構。 前項第三款資通設備委託審驗作業項目，由主管機關公告之。	本辦法之用詞定義。
第三條　測試機構應經財團法人全國認證基金會（以下簡稱認證組織）認證，具備執行主管機關公告之資通設備相關技術規範所列測試內容之能力。 測試機構應符合下列條件： 一、依法設立之本國法人、機構。 二、符合 CNS 17025 或 ISO/IEC 17025 標準。 三、未從事擬申請測試項目之資通設備輸入、設計、製造或販賣相關業務。 四、須設置三名以上之專業且專職之人員,包含測試主管一名及測試工程師二名。 前項第四款之人員,應符合下列條件： 一、測試主管： （一）為國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、資訊管理或相關科系畢業。 （二）具資通安全相關管理或測試評估實務工作經驗達五年以上,且瞭解相關法令與技術規範。	一、第一項及第二項明定申請擔任測試機構之資格與條件。 二、為確保測試機構之測試主管可依主管機關公告之相關技術規範研擬測試實施方案，督導測試工程師正確、有效執行測試，並對測試報告負責，爰於第三項要求測試機構人員之資格。 三、第四項明定認證組織認證測試機構符合第一項至第三項要求後，應檢具測試機構認證證書，報請主管機關備查。 四、第五項明定測試機構應設置必要之測試設備，並依主管機關公告之相關技術規範執行測試作業。 五、為確保測試機構核發檢驗報告之有效性及適時釐清測試機構實際辦理測試作業之執行情形，主管機關向測試機構調閱相關測試數據及實地查證仍有其必要性，爰第六項規定主管機關請測試機構提供相關資料等，測試機構應予以協助。

（三）取得 CNS 17025 或 ISO/IEC 17025 訓練合格證書。 二、測試工程師： （一）為國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、資訊管理或相關科系畢業。 （二）具資通安全相關測試評估實務工作經驗達二年以上。 （三）具備 ISO/IEC 15408 測試評估專業訓練時數至少四十小時以上之證明。 （四）取得道德駭客認證（Certified Ethical Hacker，CEH）或國際網路資安認證（CompTIA Security+）有效之資訊安全相關專業證照。 （五）具備下列有效之資訊安全相關專業證照之一： 1. 資訊系統安全專家證照（$(ISC)^2$ Certified Information Systems Security Professional，CISSP） 2. 資安分析專家證照（EC-Council Certified Security Analyst，ECSA） 3. 資安鑑識調查專家證照（EC-Council Computer Hacking Forensic Investigator，CHFI） 4. 滲透測試專家證照（GIAC Penetration Tester，GPEN） 5. 資安專業人員證照（$(ISC)^2$ Systems Security Certified Practitioner，SSCP） 認證組織認證測試機構符合前三項規定後，應檢具測試機構認證證書，報請主管機關備查。 測試機構為執行主管機關公告之資通設備相關技術規範，應設置必要之測試設備以辦理測試作業。 主管機關得向測試機構調閱及查核相關文件，並得派員至測試機構實地查證，測試機構無正當理由不得規避、	

妨礙或拒絕。	
第四條　測試機構有下列情形之一者，主管機關得令其限期改善並暫停辦理測試作業，經主管機關確認改善完成，始得辦理測試作業： 一、不符合第三條第二項各款條件。 二、未依主管機關公告之資通設備相關技術規範辦理測試作業。 三、拒不提供相關文件或無正當理由拒絕主管機關派員實地查證。 四、經主管機關或認證組織認定違反CNS17025 或 ISO/IEC 17025 標準。 前項測試機構暫停辦理測試作業之期間至少三個月，主管機關並得視情節輕重予以延長至一年。	一、第一項明定測試機構違反第三條測試機構之資格條件及應遵守之事項時，主管機關得令其改善並暫停辦理測試作業，並於主管機關確認其改善完成後，始恢復辦理測試作業。 二、第二項明定主管機關暫停測試機構辦理測試工作之最短效期。
第五條　申請擔任驗證機構者（以下簡稱申請人），應符合下列條件： 一、依法設立之本國法人、機構。 二、未從事擬申請驗證項目之資通設備輸入、設計、製造或販賣相關業務。 三、符合CNS 17065 或 ISO/IEC 17065 標準。 四、須設置二名以上專職之驗證人員。 前項第四款之驗證人員，應符合下列條件： 一、為國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、資訊管理或相關科系畢業。 二、具資通安全相關管理或測試評估實務工作經驗達五年以上，且瞭解相關法令與技術規範。 三、取得CNS 17065 或 ISO/IEC 17065 訓練合格證書。 四、具備下列有效之資訊安全相關專業證照之一： （一）資訊系統安全專家證照（$(ISC)^2$ Certified Information Systems Security Professional，CISSP） （二）資安分析專家證照(EC-Council Certified Security Analyst，	一、第一項明定申請擔任驗證機構之資格與條件。 二、為確保驗證機構之驗證人員具評估測試方法、結果之合理性，及是否符合技術規範要求之能力，爰於第二項明定驗證人員資格。 三、為確保驗證機構執行審驗作業之公正性及獨立性，爰於第二項第五款明定驗證人員不得兼任第三條第二項第四款之測試主管或測試工程師。

ECSA） （三）資安鑑識調查專家證照（EC-Council Computer Hacking Forensic Investigator，CHFI） （四）滲透測試專家證照（GIAC Penetration Tester，GPEN） （五）資安專業人員證照（(ISC)^2 Systems Security Certified Practitioner，SSCP） 五、不得兼任第三條第二項第四款之人員。	
第六條　申請人應檢具下列文件，向主管機關提出申請： 一、資通設備驗證機構申請書(如附件一)。 二、設立證明文件影本。 三、申請人取得之 CNS 17065 或 ISO/IEC 17065 證書影本。 四、驗證人員符合前條第二項資格之基本資料。 五、驗證部門組織架構圖與功能說明表。 六、驗證部門品質手冊。 七、驗證部門品質文件一覽表。 八、擬申請驗證之資通設備審驗作業程序。 九、其他經主管機關指定之資料。 前項申請文件有不全或記載不完備者，經主管機關通知限期補正，屆期未補正或補正不完備者，駁回其申請。 前項補正期間最長不得逾一個月。	一、第一項明定申請人所需檢具之文件；其中第二款至第五款之文件，係審查申請人是否符合前條之資格；第六款至第八款係進行實地評鑑時所需資料。 二、第二項明定申請人屆期未補正或補正不完備者，駁回其申請。 三、為使申請程序迅速明確，爰於第三項明定補正期間限制。
第七條　申請人依前條規定檢附之文件，經主管機關審查合格者，由主管機關進行實地評鑑。 主管機關應依下列各款規定辦理實地評鑑，並提出評鑑報告： 一、CNS 17065 或 ISO/IEC 17065 標準。 二、主管機關公告之資通設備相關技術規範或國家標準之規定。 三、其他經主管機關指定與實地評鑑相關之事項。 經實地評鑑有不符合前項各款規定者，主管機關應列舉不符合事項，並	一、為使申請人具備擔任驗證機構之相當技術能力及日後從事驗證作業流程符合相關標準，爰於第一項明定申請人依第六條規定檢附之文件之經主管機關審查合格者，由主管機關進行實地評鑑。 二、為使實地評鑑之實施合於公正、公開之原則，爰於第二項明定實地評鑑標準，並於完成實地評鑑後，撰寫評鑑報告。 三、第三項明定實地評鑑不合格者之後續改善行為，並於第四項明定改善

通知其限期改善。申請人應於通知期限內完成改善，並提出改善報告，屆期未完成者，駁回其申請。 前項改善期間最長不得逾三個月。	期間之限制，以確保實地評鑑程序迅速明確。
第八條　申請人經主管機關評鑑合格，與主管機關簽訂資通設備委託審驗契約（以下簡稱委託審驗契約），並經主管機關核發資通設備驗證機構認證證書（以下簡稱認證證書，如附件二），始得辦理資通設備審驗工作。	配合第二條第一項驗證機構之定義，爰於本條明定申請人經評鑑合格後，仍應完備相關作業，始得辦理資通設備之審驗工作。
第九條　驗證機構對於申請資通設備審驗案件(以下簡稱審驗案件)，無正當理由，不得拒絕或為差別待遇。 驗證機構及其驗證人員不得從事輔導廠商或改變資通設備功能之相關工作。 驗證機構辦理審驗案件時，應以驗證機構之名義為之。 前項審驗案件之測試報告應由經認證組織認證之測試機構出具。	一、依行政程序法第二條第三項規定，驗證機構受託從事資通設備審驗時視為行政機關，爰於第一項明定驗證機構從事審驗工作時，應遵守事項及平等原則，禁止為差別待遇。 二、第二項明定驗證機構及其驗證人員應迴避之情形。 三、為避免驗證機構以非主管機關委託辦理審驗業務之名義辦理審驗證明之核發、換發、撤銷或廢止等事項，影響行政處分之效力，並確保外界正確判斷受理審驗之對象，爰第三項規定驗證機構辦理審驗案件時，應以驗證機構之名義為之。 四、第四項明定審驗案件之測試報告應由符合第三條規定之測試機構出具。
第十條　驗證機構應依關鍵電信基礎設施資通設備資通安全檢測技術規範等規定，辦理資通設備審驗證明（以下簡稱審驗證明）之核發、補發、換發、撤銷或廢止、審驗申請之駁回或同意經審驗合格之資通設備其外觀變更等事項。 驗證機構受理審驗案件之完整資料，應自完成之日起十日內，依主管機關指定方式報請備查。 主管機關於必要時，得指示驗證機構抽驗關鍵電信基礎設施設置者之資通設備。抽驗之每一案件應於抽驗之日起二個月內將抽驗結果報請主管機關備查。 前項抽驗之資通設備由關鍵電信基礎設施設置者提供。	一、第一項及第二項明定驗證機構依規定辦理申請審驗案件後，應於規定期限內，將審驗案件完整資料報請主管機關備查。 二、為確保資通設備之品質及符合相關技術規範，爰於第三項及第四項明定抽驗機制。
第十一條　驗證機構申請增列資通設備	一、增列申請驗證項目者，應重新申請，

之驗證項目者，應依第六條規定申請，並辦理認證證書之換發；換發之認證證書有效期間與原認證證書同。 主管機關受理前項申請得依第七條規定辦理實地評鑑。 認證證書記載事項異動時，除第一項增列驗證項目外，應自異動發生日起十五日內，檢附認證證書向主管機關申請換發。經換發之認證證書，其有效期間與原認證證書同。 驗證機構有驗證人員出缺、增加之異動，應於異動發生之日起十五日內，檢附異動人員資料報請主管機關備查。 驗證人員出缺未補實致不符合第五條第一項第四款規定時，主管機關得令該驗證機構暫停辦理有關之審驗工作；驗證機構應於驗證人員補實後，檢附驗證人員基本資料，報請主管機關准予恢復辦理審驗工作。	爰於第一項明定新申請案之申請程序及認證證書之換發。 二、經審查文件合於規定後，視實地評鑑結果以決定是否同意其增列，爰於第二項明定辦理實地評鑑。 三、因認證證書係表彰驗證機構其技術能力符合標準且已受主管機關委託實施審驗，爰於第三項明定證書記載事項異動時換發認證證書之相關規定。 四、第五條第一項驗證機構之資格與條件中，對於驗證人員設有員額之最低限制，爰於第四項明定驗證人員有增減之異動時，應報請主管機關備查。 五、第五項明定驗證人員出缺未補之管理事項。
第十二條　主管機關得派員至驗證機構進行不定期查核，驗證機構不得拒絕之。	為確保驗證機構之服務品質，爰明定主管機關得派員至驗證機構進行不定期查核。
第十三條　委託審驗契約之期間為三年。 委託審驗契約期間屆滿前三個月起之二個月內，驗證機構得申請辦理續約，主管機關得視需要依第六條及第七條規定辦理審查及評鑑。 主管機關應於委託審驗契約期間屆滿前一個月通知驗證機構不得再受理審驗案件。驗證機構應於通知之日起一個月內完成已受理之審驗案件。	一、第一項明定委託審驗契約之期間。 二、第二項明定驗證機構於契約期滿，如欲繼續擔任審驗工作時，申請續約之程序及主管機關保留審查及評鑑之權利。 三、為使驗證機構於委託審驗契約期間屆滿前一個月受理之審驗案件能於期間屆滿前完成審驗工作，保障驗證機構之權益，爰於第三項明定主管機關之通知義務。
第十四條　驗證機構有下列情形之一者，主管機關得終止委託審驗契約，並令其繳回認證證書及註銷其認證證書： 一、不符合第五條第一項各款條件。 二、違反第九條第二項、第十條、第十一條或第十六條規定。 三、逾越委託審驗契約授權範圍或怠於辦理審驗案件工作。 四、無正當理由拒絕主管機關不定期查核。 五、違反本法、行政程序法、關鍵電信基礎設施資通安全檢測技術規範	一、第一項明定終止委託審驗契約之事由。 二、因終止契約之各種事由情節輕重不一，對於申請審驗案件影響較輕微之終止契約事由，給予改善期限，爰於第二項明定之。

或本辦法等法令規定。 六、受理申請審驗案件，有無正當理由之拒絕或差別待遇之情事。 七、核發之審驗證明有虛偽不實之情事者。 前項第一款至第四款情形，主管機關得令驗證機構限期改善，屆期未改善者，依前項規定辦理。	
第十五條　委託審驗契約經依前條規定終止時，驗證機構應將未完成之審驗案件交由主管機關指定之驗證機構辦理。 驗證機構應於委託審驗契約關係消滅後七日內將所有審驗案件相關之完整資料移交主管機關。 經依前條規定終止委託審驗契約之驗證機構，於委託審驗契約終止日起一年內，不得重新申請擔任驗證機構。	一、為確保申請審驗案件者之權益，爰於第一項明定委託審驗契約經依前條規定終止時，對於驗證機構已受理而尚未完成之審驗案件之辦理方式。 二、第二項明定審驗案件相關資料應移交主管機關。 三、第三項明定委託審驗契約終止後，重新申請擔任驗證機構之期間限制。
第十六條　驗證機構應於取得第八條認證證書之日起一年內建置網路申辦系統，受理資通設備審驗之申請。	為建置政府行政電子化環境，以縮減申辦時間，明定驗證機構應建置網路申辦系統，以落實電子化政府政策。
第十七條　驗證機構受理審驗案件時，應依主管機關所定收費標準向申請審驗案件者收取審驗費，並於收訖之次日悉數解繳國庫；主管機關另依委託審驗契約議定標準核支其委託費用。	驗證機構審驗費之收取、核支及訂定依據。
第十八條　本辦法自中華民國○年○月○日施行。	本辦法施行日期。

附件一

關鍵電信基礎設施資通設備驗證機構申請書

一、申請人名稱：

二、申請人地址：□□□

三、代表人：

四、聯絡人：　電話：　　傳真：

五、申請驗證項目：

檢附資料（一式一份）

□1、設立證明文件影本。

□2、申請人取得之 CNS 17065 或 ISO/IEC 17065 證書影本。

□3、驗證人員名冊、其資格資料及相關證明文件。

□4、申請人所屬驗證部門組織架構圖與功能說明表。

□5、申請人所屬驗證部門品質手冊。

□6、申請人所屬驗證部門品質文件一覽表。

□7、依驗證項目之資通設備之審驗作業程序。

□8、其他經主管機關指定之資料。

以上提供資料若有不足，本機構願配合實地評鑑作業隨時提供必要的資料，全力支持實地評鑑過程。

申請人（蓋章）：

代表人（蓋章）：　　申請日期：　年　月　日

承辦人員簽章：　　申請日期：　年　月　日

附件二

關鍵電信基礎設施資通設備驗證機構認證證書

證書號碼：

一、驗證機構名稱：

二、代表人：

三、驗證機構地址：□□□

四、有效期間：自　　年　　月　　日至　　年　　月　　日止

五、驗證項目：

（以下空白）

蓋印

中華民國 ○○○年○○月○○日