國家中山科學研究院
111年第58專案人力進用招考甄試簡章

壹、招考需求：

本院「資訊安全中心」需求全時聘雇研發類 1 員、技術生產類 7 員，合計 8 員，竭誠歡迎認同本院使命、定位、願景及核心價值之優秀夥伴踴躍報考，加入本院工作行列，依「招考需求表」辦理（如附表）。

貳、報名時間及方式：

一、甄試簡章及職缺需求刊登於本院全球資訊網，公告報名至 111 年 9 月 19 日止(網址：https://www.ncsist.org.tw)。

二、符合報考資格者，需至本院網路徵才系統(https://join.ncsist.org.tw)填寫個人資料及上傳履歷表、學歷、經歷、成績單、英文檢定證明、論文、期刊發表、證照、證書等相關資料後，選擇報考職缺並投遞履歷，各項資料依序彙整於同一檔案(PDF 檔)上傳，徵才系統履歷投遞步驟說明請參閱附件 1。

三、本院於徵才系統資料庫篩選符合報考資格者辦理初步選員(資格審查)。

四、報考人員經初步選員(資格審查)及書面審查合格者，以電話或電子郵件通知參加甄試，未獲選者不另行通知。

五、恕不接受紙本或現場報名甄試。

參、聯絡方式：

用人單位	郵件信箱	總機	聯絡人 及分機
資訊安全中心	amorfativiii@ncsist.org.tw	(03)4712201	簡小姐 354837

請將問題詳細描述並附上截圖寄至以上郵件信箱，並來電說明，將有專人協助處理。

肆、報名資格：

一、國籍：具中華民國國籍，並在臺灣、澎湖、金門、馬祖地區設有戶籍者。

二、學、經歷：教育部評鑑合格之各大學院校相關系所畢業(持國外學歷者須符合教育部頒「大學辦理國外學歷採認辦法」之資格)。

(一)學、經歷及科系專長須符合招考需求表之學、經歷條件者。

(二)報考人員若高於該職缺「學歷」，仍依本院相關規範薪資範圍核薪。

(三)同等學力不予運用。

三、依「從事及參與國防安全事務人員安全調查辦法」，為確保國防安全事務，本院得依安全調查事項協請保防安全單位及其他機關協助，就國(戶)籍、刑事案件與出入境等八款資訊辦理查詢。

四、限制條件：具有下列情形之一者，不得進用，並於甄試前簽具切結書；若於進用後，本院始查錄取人員有下列限制條件者，因自始即未符合報考資格，本院得取消錄取資格，不得提出異議：

(一)履歷內容填寫不實或於應徵過程中為虛偽意思表示及舞弊者。

(二)大陸地區、香港或澳門地區人士(包括現有或曾有前開地區之護照、居留證、身分證等，及其他經本院認定與前開地區有密切關聯之事實者)。

(三)無行為能力或限制行為能力。

(四)曾因違反毒品危害防制條例案件，受觀察勒戒、強制戒治及刑之宣告。

(五)犯內亂、外患、貪污罪及違反國家機密保護法，經判決有罪。但情節輕微且經緩刑宣告者，不在此限。

(六)曾犯前款以外之罪，經判處有期徒刑以上之刑，尚未執行或執行未完畢。但情節輕微且經緩刑宣告者，不在此限。

(七)因案被通緝或在羈押、管收中。

(八)依法停止任用。

(九)褫奪公權尚未復權。

(十)受監護宣告尚未撤銷。

(十一)於本院服務期間，因有損本院行為，遭解僱或以不勝任人員資遣。

(十二)本院各級主管之配偶及三親等以內血親、姻親，在其主管單位中應迴避任用。

(十三)因品德、操守或違反資安規定遭任職單位核予大過(含)以上之處分者。

伍、報名應檢附資料：

報名資料未繳交齊全或資料內容無法辨識者，視同資格不符。請參照附件2各項資料依序彙整於同一檔案(PDF檔)上傳，並請調整資料版面呈現方向(轉正)。

一、填具履歷表(履歷表填寫範例請參考附件 3，勿任意刪減欄位），並依誠信原則確實填寫，若未誠實填寫而錄取，本院則予不經預告終止契約解除聘僱。

二、主管核章之各類聘雇員工參加招考報名申請表掃描檔(如附件 4，僅本院員工需繳交)。

三、符合報考學歷之畢業證書掃描檔。

四、報考所需之個人相關掃描檔資料(如：工作經歷證明、證照、成績單或英文檢定成績等，請參考簡章招考需求表)。

五、檢附近 3 個月申請之警察刑事紀錄證明(俗稱良民證；證明期間為全部期間)。

六、提供工作經歷證明者，格式不限，但需由任職機構(單位)或雇主蓋章認可，內容需註明從事之工作內容(非職稱)及任職時間。

七、若有繳交非我國政府機構之工作經歷證明，需再檢附個人社會保險投保證明(如：勞保、公保、農保…等)，如未檢附，該工作經歷不予認可。

八、應屆畢業生報名甄試時尚未取得畢業證書者，僅需繳交學生證掃描檔查驗。前述人員錄取後，需於本院寄發錄取通知日起至報到日期間，繳驗畢業證書正本(如為學校因素無法如期繳交，須出具學校開立之佐證證明)，若無法繳驗，則取消錄取資格。

九、具身心障礙身分者，檢附身心障礙手冊(證明)正、反面掃描檔。

十、具原住民族身分者，檢附戶口名簿或戶籍謄本掃描檔，並標記族別。

十一、各項繳交資料正本於錄取報到時統一辦理繳驗，凡有偽造證件不實者，一律註銷錄取資格。

陸、甄試說明：

一、甄試時間：暫訂 111 年 10 月(實際甄試時間以甄試通知為準)。

二、甄試地點：暫訂本院新新院區(實際甄試地點以甄試通知為準)。

三、甄試方式：(科目及配分方式請參考招考需求表)

(一)書面審查。

(二)筆試。

(三)口試。

四、各項甄試作業(如：時間、地點…等)均以電話或電子郵件通知應考人員。請考生務必留意報考時提供之聯絡方式(履歷表與本院網路徵才系統所留電郵需一致)，若以電話或電子郵件通知無法聯繫，視為放棄報考不再另行通知。

五、甄試作業如遇天災、事變及突發事件等不可抗力之原因，需求單位得視情況調整甄試作業時間、地點及甄試方式。

柒、錄取標準：

一、單項(書面審查/筆試/口試)成績合格標準請參閱招考需求表，未達及格標準者不予錄取。

二、總成績合格標準為 70 分(滿分 100 分)。

三、如有其中一項甄試項目缺考者，不予計算總分，且不予錄取。

四、成績排序：

(一)以總成績高低依序錄取，總成績為各單項成績依比例計算後加總。

(二)總成績相同時，依序以筆試成績、口試平均成績、書面審查平均成績較高者為優先；遇所有成績均相同時，由單位決定錄取順序。

五、備取人數：

(一)完成各階段甄試合格，但未錄取之應徵者得為備取人員，並依成績排定備取順序依序備取，儲備期限自甄試結果奉權責長官核批次日起 4 個月內有效。

(二)人員錄取或遞補來院報到後，其他於本院應徵職缺之錄取或遞補皆視同自動放棄。

捌、錄取通知：

一、甄試結果暫訂於甄試後 1 個月內寄發通知單(或以電子郵件通知)，各職缺錄取情形公告於本院網路徵才系統。

二、錄取人員試用 3 個月，試用期間經考核為不適任人員，予以資遣並核予資遣費。

三、錄取人員若無特殊原因(需事先說明)，未於約定時間內完成報到者視同放棄錄取資格，逕由備取人員依序辦理遞補作業。

玖、注意事項：

一、薪資及福利待遇於任職後依本院相關規範辦理。

二、軍公教退伍(休)再任本院員工，依相關法令(規)所定規則辦理。

三、本院聘雇人員報名參加甄試，應具近六個月平時考核，且經單位主管同意。

四、歡迎具身心障礙身分或原住民族身分，且符合報考資格者報名參加甄試，並於本院資料庫登錄。

五、錄取人員如因職類及工作內容，將從事及參與「國家機密」事務，於入院乙個月內，均須依國防部「列管軍品廠商安全查核辦法」、「國防科技工業合作廠商安全調查執行作法」及本院「人員安全調查作業規定」等規範，填註從事及參與國防工業安全事務人員安全調查表(安全標準參考表如附件 5)，接受查核作業。

六、前開未通過國防部安全調查者，本院得予以資遣終止勞動契約。

七、奉核定從事及參與「國家機密」事務人員，依「入出國及移民法」、「臺灣地區與大陸地區人民關係條例」及「國家機密保護法」等法令暨本院「人員申請出國出境管理作業規定」辦理出境及赴大陸地區管制措施。

附表

國家中山科學研究院
111 年第 58 次專案人力進用招考需求表

工作編號	1	職類	研發類
工作地點	桃園龍潭	需求教育程度	碩士
薪資範圍	58,000-67,000	需求人數	1
主要工作項目	1.資安法規：各項資安法規及公務機關應辦事項推動作業、綜辦資安治理相關工作、辦理教育訓練相關事宜。 2.資安監控：研訂資通安全維護計畫、監控資安防護工作、依法規要求限時處理資安事件。 3.資安管理系統：資訊安全管理系統推動作業、綜辦 ISO 相關工作、辦理教育訓練相關事宜。 4.資安標準導入驗證：資通安全相關標準導入驗證推動作業、綜辦標準驗證相關工作、辦理教育訓練相關事宜。		
任職條件	1.工業工程/系統工程/應用數學/統計/電子/電機/機械/資訊/資科/電腦(計算機)/通訊/通信/電信/網路/軟體/光電/航太/土木/物理/海洋/水文/海下/地球科學/航海/軍事工程/化學/材料/資料科學/數據科學/應用科學理工系所畢業。 2.非上述之其他理工科系者，須具備以下兩項條件並經單位認定通過： (1)具主要工作項目任一相關經驗 1 年(含)以上。 (2)具備有效期限內之資通安全專業證照(須為行政院公布之資通安全專業證照清單內證照，如附件 6)。 3.非上述科系者，須具備以下兩項條件並經單位認定通過： (1)具主要工作項目任一相關經驗 1 年(含)以上。 (2)具備資安國際證照、國際重要資安競賽、資安特殊技能至少其中一項專長經歷(如附件 7)。 4.請檢附下列文件(缺件者視同資格不符)： (1)本院履歷表及自傳格式。 (2)大學(含)以上歷年成績單及畢業證書。 (3)近 3 個月申請之警察刑事紀錄證明(俗稱良民證；證明期間為全部期間)。 (4)多益 600 分(含)以上或同等英文檢定測驗(全民英檢、托福、雅思)之證明書。 (5)工作經歷證明或勞動部勞保局個人勞保投保明細表或人事命令(有工作經驗者)。 5.請檢附相關專題、論文、經驗等有助審查資料。 6.具下列條件尤佳，並納書面審查加分項目(請檢附相關證明)： (1)資安相關專業證照(如：CISSP、CEH、CompTIA Security+、CND、ECIH、ISO 27001…等)。 (2)其他可資佐證符合工作需求之專長(技能)或公、民營機構訓練證照(證明)。		
甄試方式	1.書面審查 20%（70 分合格）。 2.筆試 30%（70 分合格）。 3.口試 50%（70 分合格）。		
備註說明	1.筆試項目：資安管理系統規劃。(考題不以參考書目為限) 2.參考書目： (1)資通安全管理法(107 年 6 月 6 日華總一義字 10700060021 號)。 (2)CNS 27001：2014(資訊技術-安全技術-資訊安全管理系統-要求事項)。		

國家中山科學研究院
111 年第 58 次專案人力進用招考需求表

工作編號	2	職類	技術生產類
工作地點	桃園龍潭	需求教育程度	學士
薪資範圍	39,000-46,000	需求人數	3
主要工作項目	1.執行供應商資安查核、評鑑作業。 2.執行資安法規應辦事項相關工作。 3.執行資安檢查及資安宣導相關作業。 4.執行資訊安全管理系統推動相關作業。		
任職條件	1.工業工程/系統工程/應用數學/統計/電子/電機/機械/資訊/資科/電腦(計算機)/通訊/通信/電信/網路/軟體/光電/航太/土木/物理/海洋/水文/海下/地球科學/航海/軍事工程/化學/材料/資料科學/數據科學/應用科學理工系所畢業。 2.非上述科系者，須具備以下兩項條件並經單位認定通過： (1)具主要工作項目任一相關經驗 1 年(含)以上。 (2)具備有效期限內之資通安全專業證照(須為行政院公布之資通安全專業證照清單內證照，如附件 6)。 3.請檢附下列文件(缺件者視同資格不符)： (1)本院履歷表及自傳格式。 (2)大學(含)以上歷年成績單及畢業證書。 (3)近 3 個月申請之警察刑事紀錄證明(俗稱良民證；證明期間為全部期間)。 (4)工作經歷證明或勞動部勞保局個人勞保投保明細表或人事命令(有工作經驗者)。 4.具下列條件尤佳，並納書面審查加分項目(請檢附相關證明)： (1)資安相關專業證照(如：CISSP、CEH、CompTIA Security+、CND、ECIH、ISO 27001…等)。 (2)其他可資佐證符合工作需求之專長(技能)或公、民營機構訓練證照(證明)。		
甄試方式	1.書面審查 20%（70 分合格)。 2.筆試 30%（70 分合格)。 3.口試 50%（70 分合格)。		
備註說明	1.筆試項目：資安管理實務。(考題不以參考書目為限) 2.參考書目： (1)資通安全管理法(107 年 6 月 6 日華總一義字 10700060021 號)。 (2)資訊安全概論與實務(第三版)，作者：潘天佑/出版社：碁峰資訊。		

國家中山科學研究院
111 年第 58 次專案人力進用招考需求表

工作編號	3	職類	技術生產類
工作地點	臺中西屯	需求教育程度	學士
薪資範圍	39,000-46,000	需求人數	1
主要工作項目	1.執行資安法規應辦事項相關工作。 2.執行資安評鑑、資安檢查及資安宣導相關作業。 3.執行資訊安全管理系統推動相關作業。 4.執行資通安全標準導入驗證相關作業。		
任職條件	1.工業工程/系統工程/應用數學/統計/電子/電機/機械/資訊/資科/電腦(計算機)/通訊/通信/電信/網路/軟體/光電/航太/土木/物理/海洋/水文/海下/地球科學/航海/軍事工程/化學/材料/資料科學/數據科學/應用科學理工系所畢業。 2.非上述科系者，須具備以下兩項條件並經單位認定通過： (1)具主要工作項目任一相關經驗 1 年(含)以上。 (2)具備有效期限內之資通安全專業證照(須為行政院公布之資通安全專業證照清單內證照，如附件 6)。 3.請檢附下列文件(缺件者視同資格不符)： (1)本院履歷表及自傳格式。 (2)大學(含)以上歷年成績單及畢業證書。 (3)近 3 個月申請之警察刑事紀錄證明(俗稱良民證；證明期間為全部期間)。 (4)工作經歷證明或勞動部勞保局個人勞保投保明細表或人事命令(有工作經驗者)。 4.具下列條件尤佳，並納書面審查加分項目(請檢附相關證明)： (1)資安相關專業證照(如：CISSP、CEH、CompTIA Security+、CND、ECIH、ISO 27001…等)。 (2)其他可資佐證符合工作需求之專長(技能)或公、民營機構訓練證照(證明)。		
甄試方式	1.書面審查 20%（70 分合格）。 2.筆試 30%（70 分合格）。 3.口試 50%（70 分合格）。		
備註說明	1.筆試項目：資安管理實務。(考題不以參考書目為限) 2.參考書目： (1)資通安全管理法(107 年 6 月 6 日華總一義字 10700060021 號)。 (2)資訊安全概論與實務(第三版)，作者：潘天佑/出版社：碁峰資訊。		

國家中山科學研究院
111 年第 58 次專案人力進用招考需求表

工作編號	4	職類	技術生產類
工作地點	桃園龍潭	需求教育程度	學士
薪資範圍	39,000-46,000	需求人數	2
主要工作項目	1.執行資安防護設備(如：IPS、WAF…等)或系統(防毒軟體、EDR 軟體等)維管工作。 2.執行資安監控中心事件通報、追蹤及研析作業。 3.執行本院作業環境滲透測試及弱點驗證。 4.執行資安事件鑑識及研析工作。 5.執行本院資訊設備之資安檢測工作。		
任職條件	1.工業工程/系統工程/應用數學/統計/電子/電機/機械/資訊/資科/電腦(計算機)/通訊/通信/電信/網路/軟體/航太/土木/物理/海洋/水文/海下/地球科學/航海/軍事工程/化學/材料/資料科學/數據科學/應用科學理工系所畢業。 2.非上述科系者，須具備以下兩項條件並經單位認定通過： (1)具主要工作項目任一相關經驗 1 年(含)以上。 (2)具備有效期限內之資通安全專業證照(發證機構須為(ISC)^2、CompTIA、CREST、EC-Council、GIAC、ISACA、Offensive Security、鑒真數位及中華民國網路封包分析協會等)。 3.請檢附下列文件(缺件者視同資格不符)： (1)本院履歷表及自傳格式。 (2)大學(含)以上歷年成績單及畢業證書。 (3)近 3 個月申請之警察刑事紀錄證明(俗稱良民證；證明期間為全部期間)。 (4)工作經歷證明或勞動部勞保局個人勞保投保明細表或人事命令(有工作經驗者)。 4.具下列條件尤佳，並納書面審查加分項目(請檢附相關證明)： (1)資安相關專業證照。 (2)其他可資佐證符合工作需求之專長(技能)或公、民營機構訓練證照(證明)。		
甄試方式	1.書面審查 20%（70 分合格）。 2.筆試 30%（70 分合格）。 3.口試 50%（70 分合格）。		
備註說明	1.筆試項目：資安防護實務。(考題不以參考書目為限) 2.參考書目： (1)資通安全管理法(107 年 6 月 6 日華總一義字 10700060021 號)。 (2)資訊安全概論與實務(第三版)，作者：潘天佑，出版社：碁峰資訊。		

國家中山科學研究院
111 年第 58 次專案人力進用招考需求表

工作編號	5	職類	技術生產類
工作地點	桃園龍潭	需求教育程度	學士
薪資範圍	39,000-46,000	需求人數	1
主要工作項目	1.日常資安事件監控。 2.資安預警通報發佈。 3.資安事件報表製作。 4.其他臨時交辦事項。 5.需排班輪值。		
任職條件	1.工業工程/系統工程/應用數學/統計/電子/電機/機械/資訊/資科/電腦(計算機)/通訊/通信/電信/網路/軟體/航太/土木/物理/海洋/水文/海下/地球科學/航海/軍事工程/化學/材料/資料科學/數據科學/應用科學理工系所畢業。 2.請檢附下列文件(缺件者視同資格不符)： (1)本院履歷表及自傳格式。 (2)大學(含)以上歷年成績單及畢業證書。 (3)近 3 個月申請之警察刑事紀錄證明(俗稱良民證；證明期間為全部期間)。 (4)工作經歷證明或勞動部勞保局個人勞保投保明細表或人事命令(有工作經驗者)。 3.具下列條件尤佳，並納書面審查加分項目(請檢附相關證明)： (1)資安相關專業證照。 (2)其他可資佐證符合工作需求之專長(技能)或公、民營機構訓練證照(證明)。 4.此職缺需排班輪值，可接受者再投遞。		
甄試方式	1.書面審查 20%（70 分合格）。 2.筆試 30%（70 分合格）。 3.口試 50%（70 分合格）。		
備註說明	1.筆試項目：資安防護實務。(考題不以參考書目為限) 2.參考書目： (1)資通安全管理法(107 年 6 月 6 日華總一義字 10700060021 號)。 (2)資訊安全概論與實務(第三版)，作者：潘天佑，出版社：碁峰資訊。		

附件 1

國家中山科學研究院徵才系統履歷投遞步驟說明

◆ 請至本院網路徵才系統 https://join.ncsist.org.tw，完成下述步驟。

步驟 1：點選頁面右上角【註冊】，完成註冊後，【建立個人資料及個人履歷】。

步驟 2：點選【搜索職缺】(尋找欲投遞職缺)→【投遞履歷】→【填寫自我推薦信】→【確認送出】。

◆ 報名應檢附資料：依據「附表-招考需求表」各項次所列學、經歷條件規定繳交(資料未繳交齊全或內容無法辨識，視同資格不符)。

(一)檔案格式：各項資料依序彙整於同一檔案，以 PDF 格式上傳。

(二)檔名規則：請以「姓名」為檔名。

(三)資料項目與順序：報考資料請依順序排列，自行增減。

上傳書審資料

職缺查詢及報名方式

附件 2

依進用招考需求表學歷、經歷條件需求資料，依序自行增修並調整資料版面之呈現方向(轉正)，以利閱讀

一、履歷表：

(一)Word 檔請至本院徵才系統-個人資料管理-表單下載：制式履歷表，請勿刪減欄位並貼妥照片。

(二)自述視需要可自行增加延伸。

二、學歷文件(本項視學歷、經歷條件需求)：

(一)畢業證書(符合報考職缺學歷要求以上(含)之畢業證書)(請貼上畢業證書圖檔，如未檢附視同資格不符)。

(二)成績單(符合報考職缺學歷要求以上(含)之歷年成績單)(請貼上之成績單圖檔，如未檢附視同資格不符)。

三、碩士論文摘要(本項視學歷、經歷條件需求)。

四、英文能力證明文件(本項視學歷、經歷條件需求)(請貼上證明文件圖檔)。

五、相關專業工作經歷證明，需再檢附個人社會保險投保證明(如：勞保、公保、農保等)，如未檢附，該工作經歷不予認可。(本項視學歷、經歷條件需求，需公司開出之證明文件)(請貼上工作經歷證明及個人社會保險投保證明圖檔，如未檢附視同資格不符)。

六、具各公、民營機構相關技能訓練證照或證明(請檢附訓練時數 300 小時以上相關證明)或其它相關證照(本項視學歷、經歷條件需求)。

七、檢附近 3 個月申請之警察刑事紀錄證明(俗稱良民證；證明期間為全部期間)(請貼上警察刑事紀錄證明掃描圖檔，如未檢附視同資格不符)。

八、其它補充資料(本項視學歷、經歷條件需求，或補充自身相關專業之專題、論文、獲獎文件…等資料)。

附件 3

履　　歷　　表

姓　名		英文姓名 (同護照名)		身分證號　碼		正面上半身清晰照片 (非生活照)
出生地		出生日期		民國　年　月　日		
國　籍	□具中華民國國籍(始具報考資格) □其他：_____、_____(雙<多>重國籍者請填寫國家名稱) □曾(或現)具陸、港、澳地區人士身分					
兵役狀況	□役畢 □免役 □未役 □服役中(退役時間：　　)					
電子郵件						

通訊處	通訊地址		行動電話	
	戶籍地址		連絡電話	
	緊急聯絡人		連絡電話	

學歷	學校名稱	院系科別	學位	起迄時間
	註：依所獲學位，由高至低順序填寫(例：按博士－＞碩士－＞學士順序)。			

經歷	服務機關名稱	職稱(工作內容)	起迄時間

家庭狀況	稱謂	姓名	出生地	國籍	目前職業(服務機關)	曾擔任之外國或陸港澳地區職業(服務機關)

一、二親等親屬	稱謂	姓名	出生地	國籍	目前職業(服務機關)	曾擔任之外國或陸港澳地區職業(服務機關)

註：1. 家庭狀況欄請填載配偶、子女及其他同住之二親等親屬。
2. 其他非同住之二親等親屬請填載於一、二親等親屬欄。
3. 一、二親等親屬欄請填載如：父母、祖父母、配偶之父母、配偶之祖父母、子女、孫子女、兄弟姐妹及其配偶等親屬；無則免填。
4. 配偶或二親等親屬具雙重以上國籍或其他地區居留權者，均應全數詳實填載於國籍欄位內。

在中科院任職三親等親屬	稱謂	姓名	單位	職類（或職稱）
	註：無則免填。			

以上履歷表欄位均詳實填寫。

婚　姻：□已婚　□未婚	身高：　公分	體重：　公斤	血型：　型
原住民：□山地　□平地；族別：　族			
身心障礙：等級：　度；類別　障(類)			

自述(請以1頁說明)

自述內容應包含事項：
一、家庭狀況(含二親等補述說明及其身分背景)、成長背景等。
二、工作經歷(專長)。
三、因求學、就醫、工作或其他原因，長期停留或頻繁往返之境外歷程。
四、是否曾任職公務機關經歷，有無特殊功過獎懲。
五、其他(考生視需要自填)。
六、請依本履歷規定格式撰寫(含履歷表、自述及報考項次之學歷、經歷條件需求資料)。
七、視需要可自行增加延伸，整份履歷表必須彙整為一個PDF檔案上。

請勿自行刪除本表欄位項目

填寫範例

履　歷　表

姓　名	李 小 明	英文姓名（同護照名）	Li Hsiao-Ming	身分證號碼	H123456789	正面上半身清晰照片（非生活照）
出生地	桃園市	出生日期	民國 80 年 1 月 1 日			
國　籍	■具中華民國國籍(始具報考資格) □其他：＿＿＿＿、＿＿＿＿（雙<多>重國籍者請填寫國家名稱） □曾(或現)具陸、港、澳地區人士身分					
兵役狀況	■役畢 □免役 □未役 □服役中（退役時間：　　）					
電子郵件	A123aa@gmail.com					
通訊處	通訊地址	桃園市龍潭區中正路1號		行動電話	0911-111111	
	戶籍地址	桃園市龍潭區中正路1號		連絡電話	03-455-5555	
	緊急聯絡人	李大明		連絡電話	03-477-2222	

學歷：依畢業證書填寫（由高至低）

學歷	學校名稱	院系科別	學位	起迄時間
	○立清華大學	電子工程所	碩士	102/9至104/6
	○立成功大學	電子工程系	學士	98/9至102/6
	註：依所獲學位，由高至低順序填寫(例：按博士－>碩士－>學士順序)。			

經歷：服務機關名稱、職稱及起迄時間應依個人勞保投保明細表填寫。

經歷	服務機關名稱	職稱（工作內容）	起迄時間
	大風股份有限公司	工程師（電子元件開發）	106/10-111/2
	○○○○○○	助理工程師（電路設計）	104/10-106/8

家庭狀況	稱謂	姓名	出生地	國籍	目前職業（服務機關）	曾擔任之外國或陸港澳地區職業（服務機關）
	妻	王 美 美	台灣	中華民國	教師(石門國小)	無
	子	李 文	台灣	中華民國	無	無

一、二親等親屬	稱謂	姓名	出生地	國籍	目前職業（服務機關）	曾擔任之外國或陸港澳地區職業（服務機關）
	父	李 大 明	台灣	中華民國	中科院	無
	母	林 小 文	台灣	中華民國	無	無
	兄	李 明 明	台灣	中華民國	中科院	無

註：1.家庭狀況欄請填載配偶、子女及其他同住之二親等親屬。
2.其他非同住之二親等親屬請填載於一、二親等親屬欄。
3.一、二親等親屬欄請填載如：父母、祖父母、配偶之父母、配偶之祖父母、子女、孫子女、兄弟姐妹及其配偶等親屬；無則免填。
4.配偶或二親等親屬具雙重以上國籍或其他地區居留權者，均應全數詳實填載於國籍欄位內。

在中科院任職	三親等親屬	稱謂	姓名	單位	職類（或職稱）
		父	李大明	資通所	工程師
		註：無則免填。			

以上履歷表欄位均詳實填寫。

婚姻：■已婚 □未婚	身高：180 公分	體重：70 公斤	血型：…AB…型
原住民：□山地 □平地；族別： 族			
身心障礙：等級：……度；類別 障(類)			

附件 4

國家中山科學研究院
各類聘雇員工參加招考報名申請表

<table>
<tr><td>現職單位
(至二級)</td><td>姓名
(身分證號碼)</td><td>職類及級職</td><td>最高學歷
(含科/系/所)</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">工作內容及經歷(請簡述)</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">擬參加甄選單位職缺</td></tr>
<tr><td colspan="2">報考單位</td><td>職類</td><td>工作編號</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td>本人簽章</td><td>二級單位</td><td colspan="2">一級單位主管批示</td></tr>
<tr><td rowspan="3">電話：</td><td></td><td colspan="2" rowspan="3"></td></tr>
<tr><td>一級人事單位</td></tr>
<tr><td></td></tr>
</table>

備註：

1. 非本院現職員工免填，申請人應具近六個月平時考核紀錄。
2. 本申請表經單位一級主管同意後始得報名參加甄試，並依簡章及招考需求表所列資格條件與需求實施條件初審，後續由用人單位實施嚴格審查。

附件 5

從事及參與國防工業安全調查事務人員安全標準參考表	
項次	安全標準
1	涉及破壞、敵諜、叛國、恐怖主義、煽動等行為，或陰謀、預備、協助、教唆他人犯以上各罪。
2	涉嫌建立、參與不法組織（活動），列管有案或偵（調）查中者
3	主張或使用暴（武）力推翻國家或咨意變更國體者。
4	曾犯洩密罪經判刑確定，或通緝有案尚未結案者，或違反保密規定，受懲戒處分、記過以上行政懲罰者。
5	同時具有中華民國國籍及外國國籍；或在外國居住，刻正尋求或取得外國公民之資格。
6	犯有內亂外患罪、違反「槍砲彈藥刀械管制條例」、涉有「妨害性自主」案、殺人、搶奪、竊盜、洩密、毒品危害防制條例、組織犯罪條例與兒童及少年性交易防制條例等前科判決確定者。
7	自填安全調查表內容不符事實，經審查誠實性、可靠性及可信賴度具重大缺失，足以影響安全調查結論判斷。
8	本人、配偶、同居人、三親等內血親，曾在外國、大陸地區（含香港、澳門）擔任其黨務、軍事、行政或具政治性機關（構）、團體之職務；或一親等內血親曾在大陸地區或香港、澳門連續停留 1 年以上者。
9	曾酗酒滋事、藥物成癮或其他精神疾病，有具體事證者。
10	超額負債致發生財務困難。
11	非法使用、持有、運送、販賣危險藥品。
備註：參照美國國防部人員安全計畫安全標準適用性制訂。	

附件6

資通安全專業證照清單

日期：111 年 3 月 15 日修正

序	發證機構(單位)	管理類(18)	技術類(92)
1.	已簽署國際認證論壇(International Accreditation Forum, IAF)多邊相互承認協議(ISO/IEC 27006 範圍)之認證機構所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構[1]	1. ISO/IEC 27001:2013 Information Security Management System(ISMS) Auditor/ Lead Auditor 2. ISO 22301 Business Continuity Management System(BCMS) Auditor/Lead Auditor 3. ISO/IEC 29100 Lead Privacy Implementer Information technology — Security techniques — Privacy framework (111 年 3 月 15 日停止認定) 4. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor Lead Auditor 相關證照應具有效性，除提出證照外，尚須提供當年度至少有 2 次實際參與該證照內容有關之稽核經驗證明。	
2.	$(ISC)^2$ 國際資訊系統安全核准聯盟[0]		1. Certified Information Systems Security Professional(CISSP) 2. Systems Security Certified Practitioner(SSCP) 3. Certified Cloud Security Professional(CCSP) 4. Certified Authorization Professional(CAP) 5. Certified Secure Software Lifecycle Professional(CSSLP)

序	發證機構(單位)	管理類(18)	技術類(92)
			6. HealthCare Information Security and Privacy Practitioner(HCISPP) 7. Information Systems Security Architecture Professional(CISSP - ISSAP) 8. Information Systems Security Engineering Professional(CISSP - ISSEP) 9. Information Systems Security Management Professional(CISSP - ISSMP)
3.	The Computing Technology Industry Association (CompTIA)[3]		1. CompTIA Security (CompTIA Security+) 2. CompTIA Cybersecurity Analyst (CySA+) 3. CompTIA Advanced Security Practitioner (CASP+) 4. CompTIA PenTest (CompTIA PenTest+)
4.	CREST[4]		1. Penetration Testing (1) The CREST Practitioner Security Analyst (CPSA) (2) The CREST Certified Wireless Specialist (CCWS) 2. Simulated Target Attack & Response/CBEST (1) The CREST Certified Simulated Attack Specialist (CCSAS) (2) The CREST Certified Simulated Attack Manager (CCSAM) (3) The CREST Registered Threat Intelligence Analyst (CRTIA) (4) The CREST Certified Threat Intelligence Manager (CCTIM)

序	發證機構(單位)	管理類(18)	技術類(92)
			3. Incident Response (1) The CREST Practitioner Intrusion Analyst (CPIA) (2) The CREST Registered Intrusion Analyst (CRIA) (3) The Certified Network Intrusion Analyst (CCNIA) (4) The CREST Certified Host Intrusion Analyst (CCHIA) (5) The CREST Certified Malware Reverse Engineer (CCMRE) (6) The CREST Certified Incident Manager 4. Security Architecture (1) The CREST Registered Technical Security Architect Examination (CRTSA)
5.	EC-Council[5]	1. Certified Chief Information Security Officer (CCISO) 2. EC-Council Information Security Management(EISM)	1. Certified Network Defender Course (CND) 2. Certified Ethical Hacker(CEH) 3. EC-Council Certified Security Analyst(ECSA) 4. Computer Hacking Forensic Investigator(CHFI) 5. EC-Council Certified Incident Handler(ECIH) 6. EC-Council Disaster Recovery Professional(EDRP) 7. Certified Threat Intelligence Analyst (CTIA) 8. Certified Application Security Engineer (CASE)NET、JAVA 9. Certified Penetration Tester (CPENT)

序	發證機構(單位)	管理類(18)	技術類(92)
			10. Licensed Penetration Testing (LPT) 11. Certified SOC Analyst(CSA) 12. CEH (Master)
6.	Global Information Assurance Certification (GIAC)[6]	Management, Audit, Legal (1) GIAC Security Leadership(GSLC) (2) GIAC Systems and Network Auditor(GSNA) (3) GIAC Law of Data Security & Investigations(GLEG) (4) GIAC Strategic Planning, Policy, and Leadership(GSTRT) (5) GIAC Information Security Professional (GISP) (6) GIAC Critical Controls Certification (GCCC)	1. Cloud Security (1) GIAC Cloud Security Essentials (GCLD) (2) GIAC Certified Web Application Defender (GWEB) (3) GIAC Cloud Security Automation (GCSA) (4) GIAC Public Cloud Security (GPCS) 2. Cyber Defense (1) GIAC Open Source Intelligence (GOSI) (2) GIAC Certified Intrusion Analyst (GCIA) (3) GIAC Certified Windows Security Administrator (GCWN) (4) GIAC Continuous Monitoring Certification (GMON) (5) GIAC Defensible Security Architecture (GDSA) (6) GIAC Certified Detection Analyst (GCDA) (7) GIAC Security Operations Certified (GSOC) (8) GIAC Information Security Fundamentals (GISF) (9) GIAC Security Essentials (GSEC) (10) GIAC Certified Enterprise Defender (GCED)

序	發證機構(單位)	管理類(18)	技術類(92)
			(11) GIAC Certified Incident Handler (GCIH) (12) GIAC Foundational Cybersecurity Technologies Certification (GFACT) (13) GIAC Defending Advanced Threats (GDAT) (14) GIAC Certified Perimeter Protection Analyst(GPPA)(111 年 3 月 15 日停止認定) (15) GIAC Certified UNIX Security Administrator(GCUX) (111 年 3 月 15 日停止認定) 3. Offensive Operations (1) GIAC Enterprise Vulnerability Assessor (GEVA) (2) GIAC Penetration Tester (GPEN) (3) GIAC Web Application Penetration Tester (GWAPT) (4) GIAC Python Coder (GPYC) (5) GIAC Mobile Device Security Analyst (GMOB) (6) GIAC Cloud Penetration Tester (GCPN) (7) GIAC Assessing and Auditing Wireless Networks (GAWN) (8) GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) (9) GIAC Secure Software Programmer-Java(GSSP-

序	發證機構(單位)	管理類(18)	技術類(92)
			JAVA)(111 年 3 月 15 日停止認定) (10) GIAC Secure Software Programmer- .NET(GSSP-.NET)(111 年 3 月 15 日停止認定) 4. Digital Forensics and Incident Response (1) GIAC Battlefield Forensics & Acquisition (GBFA) (2) GIAC Certified Forensic Examiner (GCFE) (3) GIAC Advanced Smartphone Forensic (GASF) (4) GIAC Certified Forensic Analyst (GCFA) (5) GIAC Network Forensic Analyst (GNFA) (6) GIAC Cyber Threat Intelligence (GCTI) (7) GIAC Reverse Engineering Malware (GREM) 5. Industrial Control Systems (1) GIAC Global Industrial Cyber Security Professional (GICSP) (2) GIAC Response and Industrial Defense (GRID) (3) GIAC Critical Infrastructure Protection (GCIP) 6. GSE (1) GIAC Security Expert(GSE)
7.	Information Systems Audit and Control Association (ISACA)[7]	1. Certified Information Security Manager(CISM) 2. Certified in the Governance of Enterprise IT (CGEIT)	

序	發證機構(單位)	管理類(18)	技術類(92)
		3. Certified Information Systems Auditor (CISA) 4. Certified in Risk and Information Systems Control (CRISC)	
8.	The International Society of Forensic Computer Examiners (ISFCE)[8]		Certified Computer Examiner (CCE)
9.	Offensive Security[9]		1. Offensive Security Certified Professional(OSCP) 2. Offensive Security Certified Expert(OSCE) 3. Offensive Security Wireless Professional(OSWP) 4. Offensive Security Exploitation Expert(OSEE) 5. Offensive Security Web Expert(OSWE) 6. Offensive Security Exploit Developer (OSED) 7. Offensive Security Experienced Penetration Tester(OSEP)
10.	Cisco[10]		1. CCNA 200-301 Implementing and Administering Cisco Solutions 2. CBROPS 200-201 Cisco Certified CyberOps Associate certification
11.	經濟部[11]		iPAS 資訊安全工程師中級能力鑑定
12.	ISA[12]	1. ISA/IEC 62443 Cybersecurity Fundamentals Specialist	1. ISA/IEC 62443 Cybersecurity Design Specialist

序	發證機構(單位)	管理類(18)	技術類(92)
		2. ISA/IEC 62443 Cybersecurity Risk Assessment Specialist	2. ISA/IEC 62443 Cybersecurity Maintenance Specialist 3. ISA/IEC 62443 Cybersecurity Expert

備註：

1. 針對目前已停止核發、規劃停止核發或刪除之證照，於資通安全專業證照清單公告停止認定，以證照效期內且不逾公告停止認定日一年內認定為有效，惟公告停止認定日證照剩餘效期小於 1 年者，以公告停止認定日 1 年內認定為有效。
2. 本證照清單定期更新，各機關如有新增資通安全專業證照建議，請依資通安全專業證照認可審查作業流程辦理。
3. 本清單於資通安全會報網站定期更新，機關如有任何疑問歡迎來電行政院資安處(02-33568068)反映。

參考資料：

1. TAF：https://www.taftw.org.tw/
   IAF：
   https://www.iafcertsearch.org/search/certification-bodies?standards_id=4cb16367-3cd5-5a6c-a382-1f524564b9d9&standards_name=ISO%2027001
2. $(ISC)^2$ ：https://www.isc2.org/
3. CompTIA：https://certification.comptia.org/
4. CREST：https://www.crest-approved.org
5. EC-council：https://www.eccouncil.org/
6. GIAC：https://www.giac.org/
7. ISACA：https://www.isaca.org/
8. ISFCE：https://www.isfce.com/
9. Offensive Security：https://www.offensive-security.com
10. Cisco：https://www.cisco.com
11. iPAS：https://www.ipas.org.tw/ise
12. ISA：https://www.isa.org/

附件 7

特殊領域	限制條件	內容	採計審認
資訊安全	資安國際證照(本項適用對象須具備右列證照至少一項且證照有效期必須未過召募報名截止日期)	(1).ISO 27001 之資訊安全管理系統主導稽核員認證 (2).ECSA 資安分析專家認證 (3).EDRP 資安災害復原專家認證 (4).CCISO 資安長/EISM 資安經理人認證 (5).CISSP 資訊安全系統專家認證 (6).CSSLP 資訊安全軟體開發專家認證 (7).CCIE Security 認證 (8).RHCA Red Hat Linux 系統安全調校認證 (9).LPT 滲透測試專家認證 (10). Guidance EnCase 國際專業鑑識認證 (11). CHFI 資安鑑識調查專家(數位鑑識)	由本院認定審認。
	國際重要資安競賽(本項適用對象須具備右列 2 年內國際資安競賽獲得前 10 名(含)至少一項)	(1).Defcon CTF Qualifier (2).Plaid CTF (3).Boston Key Party CTF (BKPCTF) (4).HITCON CTF (5).Hack.lu CTF (6).RuCTFe	
	資安特殊技能	1.對資訊安全領域有重要成就或傑出表現(如挖掘重要資訊系統弱點，經正常管道提報，避免重大損害)。 2.曾於 Defcon、BlackHat 國際重大論壇發表論著。 3.曾挖掘零時差弱點於 HITCON ZERODAY 或 Vulreport 經審認發表。	