出國報告(出國類別：考察)

100 年赴貝里斯、聖克里斯多福、聖露西亞進行「加勒比海資通訊應用提升計畫」考察報告

出差人員：　國際合作發展基金會人道援助處　顏銘宏組長
國際合作發展基金會人道援助處　林苡汶專案經理
遠通電收公司　李浩正總經理
私立淡江大學　梁德昭副教授
私立淡江大學　魏世杰副教授
私立朝陽科技大學　洪朝貴副教授

出國期間：　100 年 8 月 15 日至 9 月 9 日

目　　錄

摘要

本會自 2006 年起接受外交部委託辦理「加勒比海地區資通訊計畫」，期間以協助聖克里斯多福及尼維斯、聖露西亞、貝里斯進行電子化政府(E-Government)為主要合作計畫訴求，進行各國政府入口網站、行政電子化系統等開發及建置，其中最重要之工作係於各國建立國家資通訊中心(National ICT Center)。綜觀之，前述計畫係專注於公部門系統的開發，以系統建置與輔導上線為重點。考量我加勒比海友邦確具發展資通訊科技之需求與條件，為延續前述計畫之效益並提升計畫永續性，本會爰規劃辦理「加勒比海地區資通訊應用提升計畫」，承繼上一階段已有之發展成果，以整體規劃、系統整合之角度進行下一階段計畫之評估。為界定計畫項目與範疇，爰籌組考察團赴貝里斯、聖露西亞、聖克里斯多福及尼維斯進行評估，俾續擬定各國之明確計畫內容。

本次任務係透過事實調查方式，瞭解本計畫合作國家之資通訊發展策略、優先發展項目與關切事項，透過主要資通訊科技行為者之訪談，包含政府部門、民營資通訊服務業者、非政府組織等，界定本計畫之優先發展項目。本次考察所依循之策略思考原則為：一、尊重各國自發性之需求，並作為主要評估依據；二、考量區域性組織（CARRICOM）之整合性發展目標及方案，以節約推動計畫之成本，並擴大國際影響層面；三、建立系統性評估模式，依循「政策-建置-營運-轉移」之模式進行考察；四、客觀評估上一階段計畫之經驗值，去蕪存菁，有效連結，作為後續發展基礎。本次考察結論與建議摘述如下：

一、 現有之外交部委託 ICT 計畫應與本計畫有適切整合，善用既有之當地網絡與資源，以互補方式而非切割方式進行調整，延續計畫效益與永續性。

二、 我加勒比海友邦均為小型國家，問題複雜度與廣度有限，

可考慮依據各國之需求擬定一主軸計畫，進行全面且深入之推動，援助效果應會相當明顯。

三、 資通訊科技變化快速,未來推動計畫時應設計合適之架構，使計畫執行之資訊流動更加透明與即時，避免計畫執行過程出現偏差而無法及時調整與監控。

四、 本計畫倘定位為區域性計畫，仍應與區域性國際組織有所整合與連結，現階段似宜先以雙邊計畫為基礎，各國擇定一優先主軸進行深度發展，並同時與區域性國際組織對話互動，尋求合作推動區域性計畫之機會。

五、 本案可從 program 之角度建構本會在加勒比海地區推動資通訊計畫之整體規劃,program之主軸目標為應用提升，其下可以依據個別國家需求擬定一主要project。依據考察所蒐集資訊，可優先考慮項目為「貝里斯財政部賦稅系統提升」、「貝里斯 Corozal 自由貿易區保全系統提升」、「聖克里斯多福國安部警政系統強化」。

六、 治安問題已成為加勒比海地區國家之共同關切，此次考察國家亦盼能透過資通訊科技之應用，提升警政體系之運作效率，此亦為本會下一階段資訊計畫可著力之處。

七、 有關本次考察合作國家提出之小型合作需求，包含貝里斯國防部之內部聯網、聖克里斯多福工商總會之網站建置並結合 e-business platform 的概念、聖露西亞之資通訊科技應用意識提升並建立自由軟體資源中心，可考慮結合本會志工計畫或研習班協助政府和教育單位開發應用自由軟體方式進行。

八、 有關後續工作，建議儘速回應貝里斯與聖克里斯多福在警政保全議題上之急切需求，由國合會組織一結合我國中央

或地方警察機關、民間保全業者之考察團，赴貝國與克國瞭解對方明確需求以及現況，俾快速界定計畫範疇與所需資源，給予合作國家具體回應。

九、 本次考察發現，我駐聖克里斯多福大使館與駐聖露西亞大使館在合作國家曾推行電腦援贈計畫，對象為中小學學生，惟後續配套仍在規劃中，建議日後相關資訊設備援贈可搭配資通訊教育計畫，提升整體效益。

十、 未來四年計畫架構主軸方向當以前期外交部委辦計畫為基礎，以達到國家間資通訊發展永續性並結合區域安全議題、災害控管、人力資源提升及醫療。將資通訊發展成功國家經驗，以研習班或成果展的辦理方式，達到宣傳效果並同步複製到區域內其他國家。

第一章　考察概要

壹、緣起

本會自 2006 年起接受外交部委託辦理「加勒比海地區資通訊計畫」，期間以協助聖克里斯多福及尼維斯、聖露西亞、貝里斯進行電子化政府(E-Government)為主要合作計畫訴求，進行各國政府入口網站、行政電子化系統等開發及建置，其中最重要之工作係於各國建立國家資通訊中心(National ICT Center)。綜觀之，前述計畫係專注於公部門系統的開發，以系統建置與輔導上線為重點。考量我加勒比海友邦確具發展資通訊科技之需求與條件，為延續前述計畫之效益並提升計畫永續性，本會爰規劃辦理「加勒比海地區資通訊應用提升計畫」，承繼上一階段已有之發展成果，以整體規劃、系統整合之角度進行下一階段計畫之評估。為界定計畫項目與範疇，爰籌組考察團赴貝里斯、聖露西亞、聖克里斯多福及尼維斯進行評估，俾續擬定各國之明確計畫內容。

貳、目標

一、 依據資訊整備度問卷調查結果、駐館建議、現有 ICT 計畫執行經驗、專家建議等資訊，擬定各國優先考察項目，並據以赴貝里斯、聖克里斯多福及尼維斯、聖露西亞三國進行事實調查與計畫評估。

二、 與合作國家之資通訊相關單位進行洽談，包含相關政府部會、電信廠商、學校等，就資通訊發展概況與需求項目進行討論，並界定我方可參與之環節與合作步驟。

三、 與我駐館洽談，瞭解我國對合作國家之整體合作項目與政策，

以及合作國家相關政府部會之配合情形，俾界定本計畫之相關利害關係者。

四、 與外交部委託本會辦理之資通訊計畫駐地人員洽談，瞭解執行經驗與現階段計畫重點，避免本計畫之資源投入有所重疊，並以互補強化現有計畫之角度擬定本計畫內容。

參、執行人員

一、國際合作發展基金會人道援助處	顏銘宏組長
二、國際合作發展基金會人道援助處	林苡汶專案經理
三、遠通電收公司	李浩正總經理
四、私立淡江大學	梁德昭副教授
五、私立淡江大學	魏世杰副教授
六、私立朝陽科技大學	洪朝貴副教授

肆、工作範圍

一、貝里斯

(一) 拜會我駐貝里斯大使館，瞭解我國對貝國之整體合作項目與政策，以及拜會貝國相關政府部會電子化政府應用系統之配合情形，俾界定本計畫應強化之網通基礎建設面向和相關利害關係者。

(二) 協同貝國政府資通訊主政及相關單位(公眾服務部、財

政部Central Information Technology Office)界定分析應用提升之需求，並討論網路通訊普及化與建置無線網路設備 WiFi 之範疇，以及強化其網通基礎設備以協助 VOIP 語音服務產業之扶植構想。

(三) 評估現有 ICT 中心之營運現況與可提升應用之功能領域。

(四) 協同貝國核發 ISP 執照之政府部門，界定網路及資訊安全之需求。

(五) 與貝國電信主管單位及主要國營電信廠商BTL進行座談，瞭解貝國現有資通訊基礎建設、電信市場、資訊服務之供需現況，並界定資訊通信人力資源之建構需求。

(六) 與現有教學機構如University of Belize、St John’s College、 Galen University洽談，瞭解人力資源建構概況，並界定資訊通信人力資源之建構需求。

二、聖克里斯多福及尼維斯

(一) 拜會我駐聖克里斯多福及尼維斯大使館，瞭解我國對克國之整體合作項目與政策，以及克國相關政府部會之電子化政府應用系統之配合情形，俾界定本計畫應強化之網通基礎建設面向和相關利害關係者。

(二) 協同克國政府資通訊主政單位界定分析應用提升之需求，並確定克國政府在電子商務、警政聯繫網路、資訊安全以及資通訊人力資源建構之具體需求。

(三) 評估現有 ICT 中心之營運現況與可提升應用之功能領

域。

（四）評估國立醫院 Joseph N. France General Hospital 是否合適建置無線網路架構，分享台灣目前醫院無線網路結合醫療系統(HIS)之經驗，並就目前克國 JNF 院內 HIS 系統結合無線通訊之可行方案進行評估。

（五）與克國電信主管單位進行座談，瞭解克國現有資通訊基礎建設、電信市場、資訊服務之供需現況，並界定資訊通信人力資源之建構需求。

三、聖露西亞

（一）拜會我駐聖露西亞大使館，瞭解我國對露國之整體合作項目與政策，以及露國相關政府部會電子化政府應用系統之配合情形，俾界定本計畫之網通基礎建設面向和相關利害關係者。

（二）協同露國政府資通訊主政單位界定分析應用提升之需求，並確定露國政府在網路通訊基礎建設、資訊安全以及資通訊人力資源建構尤其在自由軟體應用方面之具體需求。

（三）評估現有 ICT 中心之營運現況與可提升應用之功能領域。

（四）協同露國教育部瞭解遠距教學與電子化教學發展現況，俾擬訂可行協助方案。

（五）與露國電信主管單位進行座談，瞭解露國現有資通訊基礎建設、電信市場、資訊服務之供需現況，並界定資訊

通信人力資源之建構需求，評估現有廠商是否有潛力成為未來專門提供 ISP 服務之業者。

伍、執行時程：本(100)年 8 月 17 日至 9 月 9 日，各國考察時間如下:

一、 貝里斯-8 月 18 日至 8 月 24 日

二、 聖克里斯多福及尼維斯-8 月 25 日至 8 月 31 日

三、 聖露西亞-8 月 31 日至 9 月 7 日

第二章　考察報告

本次任務係透過事實調查方式，瞭解本計畫合作國家之資通訊發展策略、優先發展項目與關切事項，透過主要資通訊科技行為者之訪談，包含政府部門、民營資通訊服務業者、非政府組織等，界定本計畫之優先發展項目。本次考察所依循之策略思考原則為：一、尊重各國自發性之需求，並作為主要評估依據；二、考量區域性組織（CARRICOM）之整合性發展目標及方案，以節約推動計畫之成本，並擴大國際影響層面；三、建立系統性評估模式，依循「政策-建置-營運-轉移」之模式進行考察；四、客觀評估上一階段計畫之經驗值，去蕪存菁，有效連結，作為後續發展基礎。

一、　事實調查

（一）貝里斯

1. 整體觀察

(1) 造成先前導入之若干 E-Government 系統成效不彰的原因，根本的問題不在於寬頻基礎建設之不足，應另有其他的因素。

(2) 貝國現有國營電信公司 BTL 肩負貝國通資訊基礎建設的任務，其成本及獲利考量不能以一般民營公司來看待。雖然我國或有能力以無線寬頻的建設提供貝國寬頻連網的另一選擇，但是仍然不建議直接涉入其寬頻基礎建設相關的項目，避免產生利益衝突。

(3) 我國協助建置之 ICT 中心已在電子化政府系統建置過程中，以 WiFi 無線寬頻的技術解決貝國首都 Belmopan 的政府單位間網路與通訊需求的經驗，所以在經驗與技術上的支援能力應有完全的把握，可滿足貝國國防部的內部聯網強化需求。

(4) Corozal 自由貿易區對於保全系統的需求是一個容易發揮的題目。首先對方有強烈需求，配合意願高；其次，該貿易區自成一格，需處理之問題相形單純。貿易區主席已允諾提送援助需求計畫書，俟收得後可立即評估其具體需求，並協助進行整體規劃，尤其是保全系統建置之前必須先建置完整的犯罪即時回應體系，利用類似快速打擊小組的方式與保全偵測系統連結，提供有效且即時的回應。

2. 連網通訊

(1) 經實地觀察，貝國在寬頻網路方面並未如出訪前之預期般地落後。其國內主要的通訊業者 BTL 在其國內主要地區皆能提供寬頻連網的服務。所以原因不在於寬頻服務可用性的問題，主要的問題在於費率過高。費率過高造成通訊費用居高不下，;在走訪貝國政府各部

門皆有同樣的反應。此外，BTL 公司為了維護其國內語音業務(市話、長途電話與行動電話)的利潤，在寬頻網路的服務中特別攔阻了語音封包的傳遞，這也是在寬頻費率過高的抱怨外，對於寬頻服務的不完整的普遍不滿。此行也和貝國其他通訊業者或有心發展通訊服務產業的民間人士晤談，表面上他們是針對通訊費率過高提供較合理費率的服務。跳過 BTL 或從瓜地馬拉，或從墨西哥界接 Internet。但就本質上，仍然有其在 BTL 偏高的費率之下有相當的獲利空間。

(2) 降低網路使用費率已有民間其他業者投入，如有足夠的獲利空間，不愁募集不到資金，因此在角色與定位上國合會似不宜涉入。

(3) 從貝國國內專家對該國的 ICT 政策的提議中可以看出，貝國政府部門有意以 WiFi 無線網路將各單位的網路接取服務匯集到 ICT 中心，再由 ICT 中心作為民眾接取電子化政府服務的閘口(gateway)。就技術面而言，本案沒有任何難度，只要確定原 ICT 中心的角色定位後，再據以增加有限的 WiFi 設備即可達成。

（二）聖克里斯多福

1. 整體觀察

(4) 國家人口數少（約四萬六千人），幅員小，商業活動程度較低，相對而言，計畫執行範圍較易控制。

(5) ICT 政策與政府組織架構清楚(Department of IT)，主責人員(Mr. Christopher Herbert)專業與態度專注良好。配合區域計畫，按部就班提出國家政策方案，並新近與 EU 合作完成 ICT 環境評估計畫。

(6) 國安部與會主管思維明快，展現主導力，警政單位出席主管，沈穩專業。

(7) 基礎網路服務（電信及有線電視）產業競爭環境尚稱良好，與從業人員之專業素養與開放市場意識，表現達一定水平。

(8) 國合會在當地執行 ICT 中心移轉營運，進度順利，合作單位表現積極，駐地技師扮演關鍵角色。

(9) 教育環節較弱，正規 ICT 技職教育體系需藉外界資源提升發展能力，現有計畫新聘之專案推動人員表現靈活積極。

(10) 以 JNF 醫院為主要核心的公衛醫療體系，制度及運作

頗為完備，對出生人口資料(防疫)資料掌握程度高，惟仍以紙本記錄，亟待電腦化，可作為公民戶籍登錄之良好基礎。

(11) 工商總會提出E化需求，代表企業部門感受並願意試探網路商機的可能性。

(12) 駐館態度開放，政策推動延續性高。

2. 連網通訊

(1) 聖克里斯多福當地已有多家通訊業者提供電話及網路服務，其與 Internet 相連目前主要依賴衛星，未來可以有環東加海纜上岸。由於該國幅員有限，各家業者都能提供有線或無線的連線服務。在費率上也在合理的範圍。是以，並無任何以無線或有線的解決方式來提升該國的通資訊基礎建設的必要。

(2) 克國政府強烈期盼能有政府內部間的寬頻骨幹，惟依據考察團網通專家之觀察，由於該國已有能量與技術兼具的通訊業者，政府部門間的寬頻骨幹可直接從通訊業者租用虛擬電路的方式得到解決。研判克國政府應不知道如何規劃其所需之網路建設，或是囿於預算與經費的困難，使得克國政府仍然在對我方的彙報中

強調政府內部寬頻建設的需求。

(3) 考察團建議,倘欲協助克國規劃政府內部網路的建置,可藉由配合租用當地業者的專線及頻寬，來完成其政府部門間之內部網路(intranet)的基礎建設。如此，線路維護與服務可以有業者負責提供，為較能持久運作的做法。

(4) 如若不與當地業者配合而完全由我方協助構築其政府部門間的內部網路，在技術與能力上雖然不成問題，但是，不論是以光纖纜線或者是以 WiMax 配搭 WiFi 的方式來完成，其花費將遠大於前者。經費的來源是一個考量。其次，建置完成後的轉移與持續維運也是一個大問題。除非該國政府有意為其內部網路的維護與運作成立一專責部門，負責一切網路管理及器材維護與汰舊換新，否則難保持續正常運作，專責網管人才的培訓將會是不可或缺的配套措施。

(5) 克國 JNF 醫院提出之不同院區的連網需求，在技術上完全沒有困難，在其建築物間可以採用有線或無線的方式連接，其建築物內可以依範圍以若干無線基地台涵蓋。基地台間可以交換器配合電力線網路橋接器來

連接，如此，可以在幾乎不干擾正常醫療作業的情形下完成整個醫院的內部寬頻網路建設。硬體施工完畢後，尚須對院內各部門使用的 IP 位址作全面的規劃，使得各部門皆有其獨立的 IP 子網路，以保留後續發展各醫院資訊系統(HIS)各模組的空間。

(6) 總言之，克國所需之網路通訊需求在技術面上均可滿足需求，惟網路系統建置完成後，應培訓其自有資訊人員接手網路管理工作，否則隨著使用者增加與擴充，勢必將影響連網效率與穩定。

（三）聖露西亞

1. 整體觀察

(1) 拜旅遊產業之賜，商業活動相對活躍，且具一定規模，基礎建設較為完備。

(2) 國家資通訊政策主責單位(Ministry of Public Services & Human Resources)，同時擔負多重權責，計畫參與人員表現較為消極被動，ICT 中心移轉營運負責人年輕資淺，政府位階權威性，實際管理成效尚待瞭解。

(3) 刻正進行有關 ICT 國家政策計畫之相關產業調查與內

容草擬工作，詢問如申請國合會協助發展方案程序時間，允諾完成內部評估後提出。

(4) 基礎網路服務（電信及有線電視）產業具市場競爭型態，然未能有機會與產業對談。基礎建設及市場雖然尚稱健全活絡，然數據顯示，固網用戶遞減，行動電話用戶暴增但上網費率偏高，顯見 Affordability 仍為 ICT 應用提升的主要障礙。與會政府人員坦承，商業勢力主導發展，但同意可以小規模區域性之 WiFi 網路提供公共服務，作為政府平衡籌碼。

(5) 教育體系相對完整，國內唯一之專科教育學院 Sir Arthur Lewis Community College 計畫升格大學。市場對 ICT(電腦維修及資訊工程)人才有迫切需求，但學制及（師資、設備）規模不足應付。當地尚有境外大學（加藉）Monroe 學院，可作為發展技職及認證課程之選項。

(6) 露國消費性商業活動興盛,具一定國家教育文化水平，在區域內具備發展內容產業之潛力。

(7) 原外交部委辦計畫推動之犯罪管理系統(CMS)上線狀況良好，警政主管強勢落實推動，值得續行深化。

(8) 駐館引介之外籍教育事業業者Mr. Michael Walker之In-Time Project，透過電視頻道及自建教育訓練系統，在小學層級推動英語教育及師資培訓計畫，經驗豐富,握有900名教師資料庫及電子郵件通訊系統，借重平台及管道力量，可視為執行推廣小學ICT教育之最佳合作對象。但如計畫擴及其他範疇，以英語教材地域需求和即時性考量，進一步應用推廣恐需面對強大市場競爭考驗，且與本計畫推動主軸較不相關。

2. 連網通訊

(1) 聖露西亞寬頻上網主要依賴Cable&Wireless/LIME、Karib Cable、DigiCell三家ISP提供。島內已有光纖鋪設，由於對外光纖主供話務使用，能提供數據專用頻寬有限，故上網費用並不便宜，約為台灣3倍以上。另外，島內不同ISP間，並無本地封包交換機制，導致島內跨ISP封包也需經由島外交換，浪費頻寬。

(2) 露國政府NTRC(國家電信監督委員會)有意於都會區自行建置光纖網路以降低上網費用，對照台灣經驗，在都會區建設寬頻網路之主要障礙在挖路成本，解決方法係由政府投資建置共同管道，以經濟規模降低成

本，供業者租用佈設光纖網路方式，鋪設數千公里光纖，以降低線路成本，加快寬頻普及速度。倘露國政府若在都會區採用高架光纖，就無台灣挖路問題。 不管是成立專屬部門，或委託民間電信公司佈建，由於相對成本低，施工易，皆可快速達成自己擁有數據光纖網路之目標。此寬頻線路建成後可開放租用，對於降低政府及民間部門的數據線路費用有很大幫助。但是，除非政府自己也願意投資對外頻寬線路，目前上網費居高不下情況，恐怕短期仍內不易改善。

(3) 建議配合政府自有光纖之佈建，可先儘速促成近期所議本地封包交換中心之設置，以提升不同 ISP 間取用島內主機服務之速度及品質。再來可推廣政府各部門 VOIP 及電子化政府服務之使用。等整個島內 Intranet 應用發展起來，用戶變多，再考慮是否需要投資對外頻寬，以達到最終降低上網費用之目的。

(4) 另露國政府 NTRC 亦有意於偏遠地區建置寬頻網路，露國受限於環境多山，地勢不平，不利於使用直視(line of sight)微波作遠距寬頻骨幹。長期而言要佈建到偏遠地區，建議仍宜使用高架光纖。可視經費多寡，逐

步佈建，並參考台灣經驗，挑選具文化、農產、手工藝等特色之地區優先進行示範，以結合觀光資源， 發展文創產業，讓寬頻深入地方生活與生計當中。

肆、綜合考察建議

一、 現有之外交部委託 ICT 計畫應與本計畫有適切整合，善用既有之當地網絡與資源，以互補方式而非切割方式進行調整，延續計畫效益與永續性。

二、 我加勒比海友邦均為小型國家，問題複雜度與廣度有限，可考慮依據各國之需求擬定一主軸計畫，進行全面且深入之推動，援助效果應會相當明顯。

三、 資通訊科技變化快速，未來推動計畫時應設計合適之架構，使計畫執行之資訊流動更加透明與即時，避免計畫執行過程出現偏差而無法及時調整與監控。

四、 本計畫倘定位為區域性計畫，仍應與區域性國際組織有所整合與連結，現階段似宜先以雙邊計畫為基礎，各國擇定一優先主軸進行深度發展，並同時與區域性國際組織對話互動，尋求合作推動區域性計畫之機會。

五、 本案可從 program 之角度建構本會在加勒比海地區推動資通訊計畫之整體規劃，program 之主軸目標為應用提升，其下可以依據個別國家需求擬定一主要project。依據考察所蒐集資訊，可優先考慮項目為「貝里斯財政部賦稅系統提升」、「貝里斯 Corozal 自由貿易區保全系統提升」、「聖克里斯多福國安部警政系統強化」。

六、 治安問題已成為加勒比海地區國家之共同關切，此次考察國家亦盼能透過資通訊科技之應用，提升警政體系之運作效率，此亦為本會下一階段資訊計畫可著力之處。

七、 有關本次考察合作國家提出之小型合作需求，包含貝里斯國防部之內部聯網、聖克里斯多福工商總會之網站建置並結合

e-business platform 的概念、聖露西亞之資通訊科技應用意識提升並建立自由軟體資源中心，可考慮結合本會志工計畫或研習班協助政府和教育單位開發應用自由軟體方式進行。

八、 有關後續工作，建議儘速回應貝里斯與聖克里斯多福在警政保全議題上之急切需求，由國合會組織一結合我國中央或地方警察機關、民間保全業者之考察團，赴貝國與克國瞭解對方明確需求以及現況，俾快速界定計畫範疇與所需資源，給予合作國家具體回應。

九、 本次考察發現，我駐聖克里斯多福大使館與駐聖露西亞大使館在合作國家曾推行電腦援贈計畫，對象為中小學學生，惟後續配套仍在規劃中，建議日後相關資訊設備援贈可搭配資通訊教育計畫，提升整體效益。

十、 未來四年計畫架構主軸方向當以前期外交部委辦計畫為基礎，以達到國家間資通訊發展永續性並結合區域安全議題、災害控管、人力資源提升及醫療。將資通訊發展成功國家經驗，以研習班或成果展的辦理方式，達到宣傳效果並同步複製到區域內其他國家。

致謝

本次赴貝里斯、聖克里斯多福及聖露西亞進行計畫考察期間，承蒙駐貝里斯大使館、駐聖克里斯多福大使館及駐聖露西亞大使館協助規劃拜會行程，並洽商合作國家之重要機構與本考察團進行深度對話，駐館亦於考察期間提供各項寶貴意見，協助本次任務圓滿達成，在此謹表誠摯謝忱。

另本次考察期間，本考察團成員較多，幸獲駐貝里斯技術團、駐聖克里斯多福技術團及駐聖露西亞技術團之全力協助，妥善規畫交通、住宿等差旅事宜，讓本次考察行程得以順利進行，在此謹一併申謝。

2011

CFZ SECURITY ENHANCEMENT PROJECT

Kareem Young/David Akierman
Corozal Free Zone
Sunday, August 21, 2011

Project Identification

Project Name:	CFZ SECURITY ENHANCEMENT PROJECT
Agency:	CFZ
Contact:	Chairman CFZ - Mr. David Akierman
Date:	Sunday, August 21, 2011

Project Summary:

The Corozal Free Zone was established in 1994 at the Belize-Mexico border in the Corozal District of Belize. The main purpose of this initiative form the onset was to attract foreign investment into Belize by providing special incentives to investors. The climate of reduced taxation and operating costs provided by the free zone, has allowed it to grow and expand in the areas of wholesale and retail merchandise. These imports and exports now approach an annual value of approximately 150 million US dollars. In the process the zone has created significant impact in both the Corozal and Orange Walk districts and has contributed directly to poverty alleviation and income generating opportunities through the provision of considerable employment opportunities.

Currently, the Corozal Free Zone has approximately 276 registered companies, with approximately 25 of those being Asian companies. These 25 companies combine to produce revenues of approximately 50 million US dollars annually. The remainder of the annual revenue is generated from a diverse mix of investors from Belize and many other countries.

The retail and general merchandise business critical to the survival of the zone is directly driven by visitors to the free zone. These visitors primarily originate from Mexico and total over 1.5 million persons annually.

The economic contributions of the zone to the northern districts are far reaching and of specific importance. It is the biggest employer in the northern districts of Corozal and Orange Walk with 2,500 employees deriving direct benefit from its existence.
Therefore it is important that the zone continues to function and attract investments to drive its continued growth.

To facilitate and ensure the continued growth, the Corozal Free Zone must provide some basic infrastructure, which includes roads, utilities and security. However due to its size and distributed nature, security has been pushed into the forefront of concerns to be addressed. It has become very complicated to constantly monitor and control all areas within the perimeter of the zone thus, bringing into focus the issue of security. At the moment, there is no comprehensive or coordinated site surveillance system implemented at the Corozal Free Zone. Currently a Security Department exists with a structured security system consisting of 53 security officers and headed by a security chief. These officers are equipped with basic equipment which includes radios, flash lights and batons. It is imperative that issue of security be addressed to minimize and mitigate any threats to the physical assets of the direct stakeholders to provide a safe and secure environment in which they can operate.

Project Description

Security and controlled access to resources are key issues to be addressed in any organization. These concepts become a necessity when the theft and the illicit

movement or transfer of goods from the Corozal Free Zone into the country may affect the local economy.

The losses of revenues from theft of goods and damages to property have a severe impact on the companies and organizations that fall victim to such activities. Furthermore, the revenues lost by the movement of untaxed and uncustomed goods into the Belizean economy have far reaching detrimental effects.

A comprehensive site surveillance system is required by the Corozal Free Zone to increase security and mitigate the risks associated with illicit activities and theft.

After much discussions and deliberations about the placement of surveillance equipment, certain strategic locations were identified. Placement of monitoring equipment at these sites would provide real time, effective surveillance capabilities in these key areas of interest.

For the proposed system to be successful and effective there is need for a division or unit that operates autonomously from but liaises and coordinates with the already established Security Department. This will allow the unit to effectively monitor and manage the equipment and applications to be implemented under this project. This unit will be executing critical activities utilizing the resources to be purchased thus need constant communication and feedback from the rest of the Security Department. It should be stressed that the already established Security Department will be reformed

and optimized to include and integrate the new capabilities offered by the new surveillance system. The personnel will be provided with the necessary skills and knowledge to facilitate this integration in order to continue ensuring the effective security of the Corozal Free Zone.

Specific Problem

The Corozal Free Zone is perhaps the only organized structure in the border area with the capacity to undertake any meaningful program that can have an impact on the many security threats that go far beyond the security of patrons, investors and assets. The problems of contraband of goods that seriously affect the national economy and the opening of channels for human and drug trafficking are specific issues that affect the CFZ. These issues are not directly under the mandate of the CFZ but due to our unique position they affect the CFZ directly and therefore have to be dealt with accordingly. The physical structure of the border zone and the free flow of visitors necessary for its functioning and commercial activities engender these issues and as such they become responsibility of the CFZ.

Currently there are limited, effective capabilities to secure the patrons and assets of the Corozal Free Zone. There is an acute need to implement a more robust and comprehensive surveillance system to monitor key areas and hotspots in order to prevent and/or minimize inappropriate or illegal activities and theft.

Objectives

General Objectives:

- To support economic growth of the Corozal Free Zone through the provision of adequate and secure infrastructure.
- To install a site surveillance system to monitor strategic problem areas within the confines and perimeter of the Corozal Free Zone.
- To assist the local authorities with complimentary resources that will deter the trafficking of humans and drugs.

Specific Objectives:

- To install and configure several surveillance cameras in the different areas depicted in annexes 1- 3.
- To implement a Wireless coverage system to provide connectivity to all surveillance sites (Depicted in annexes 2 - 3).
- To implement a centralized recording system to record and store the video feeds from the surveillance equipment.
- To establish a centralized control room with a special unit to monitor and control all surveillance capabilities.

Scope of Work

The work plan is divided as follows:

1. The installation of sites S1, S2, S3, S4, S5, F1, F2 and BG. (See Annex 1: Camera Positions). This phase is divided into two major components listed below.
    a. The installation of wireless infrastructure.
        i. This will include the installation of wireless equipment at all remote sites.
        ii. This will include the configuration of all wireless systems.
    b. The installation of surveillance infrastructure
        i. This shall include the installation of all cameras and video equipment.
        ii. The installation and configuration of an NVR (Networked Video Recorder). (This will include the acquisition of a server and NAS device to create the required NVR)
        iii. Configuration of monitoring capabilities in Security Operations Center. (This shall include the acquisition of a workstation adequate for the task described here.)
        iv. The configuration of all camera equipment.
    c. Installation of physical infrastructure
        i. Remodeling and preparation of control room.
        ii. Installation of posts and based of surveillance sites

iii. Installation of Masts and equipment enclosures

iv. Installation of required electrical connections and outlets at all sites

d. Training and capacity building

i. Developing of guidelines and polices of operation for new video surveillance and dispatch unit

ii. Training of members of new video surveillance and dispatch unit.

Main activities

1. Identification of locations with the qualities to establish the sites.
2. Preparation of sites for the installation of both camera and wireless equipment.
    a. Construction and installation of poles and/or braces and arms at individual remote sites for cameras and wireless equipment.
    b. Installation of power outlets/extensions at all sites.
3. Installation of power supplies and poles, brackets and braces at selected sites and main site.
4. Installation of camera hardware at selected sites.
5. Installation of wireless equipment at selected remote sites and main site.
    a. Installation of 10-12m tower at main site for installation of core wireless equipment.
6. Configuration of wireless system and devices.
7. Installation/Modification of corporate network infrastructure to integrate wireless LAN and accommodate NVR and operations center.

8. Construction and/or refurbishment of the control and operations center.
9. Installation and configuration of software and hardware in the operations center.
10. Development and implementation of guidelines and regulations for use of system and response to events.
11. Reorganization and reformation of security department to account for the integration of surveillance system.
12. Training of staff directly responsible for the control and operations center.

Estimated Results

1. Minimum eight (8) established remote video surveillance sites with the capability of centralized monitoring and control.
2. Establishment of a wireless network infrastructure inclusive of the eight (8) remote surveillance sites to transfer video feeds from remote sites to the central monitoring and operations center.
3. Modification and reorganization of corporate network to accommodate new surveillance systems.
4. Establishment of a dedicated operations center manned 24hrs by trained dedicated staff to monitor the live video feeds from all sites and coordinate appropriate responses in the case of emergencies and/or illegal activities.
5. Reformation of security department, including operational guidelines and procedures, to integrate the additional surveillance capabilities.
6. Training of Control Room Personnel to increase their competence in running the most critical part of the new system to be implemented.

Exclusions

- Negotiations for utilization of buildings or space at intended sites.
- Maintenance and support after completion of project.

Estimated Costs

The estimate costs for equipment and labor for the project is at a total of **$ 170,000.00 US**. The CFZ proposes to co-finance the project along with funding from the Taiwanese ICDF.

The CFZ recognizes the need to contribute tangibly to the project and proposes to enlist the assistance of all the direct stakeholders in the CFZ, along with its own financing, to provide the necessary funds as per its commitment to co-finance the project. The CFZ believes that by having a direct stake in the project it will ensure it ongoing support and ultimate success through a direct sense of ownership. This will ensure that the ultimate goals and objectives of the project are attained and that the returns on investments are maximized through its active participation in the project.

Table showing contribution amounts by both parties.

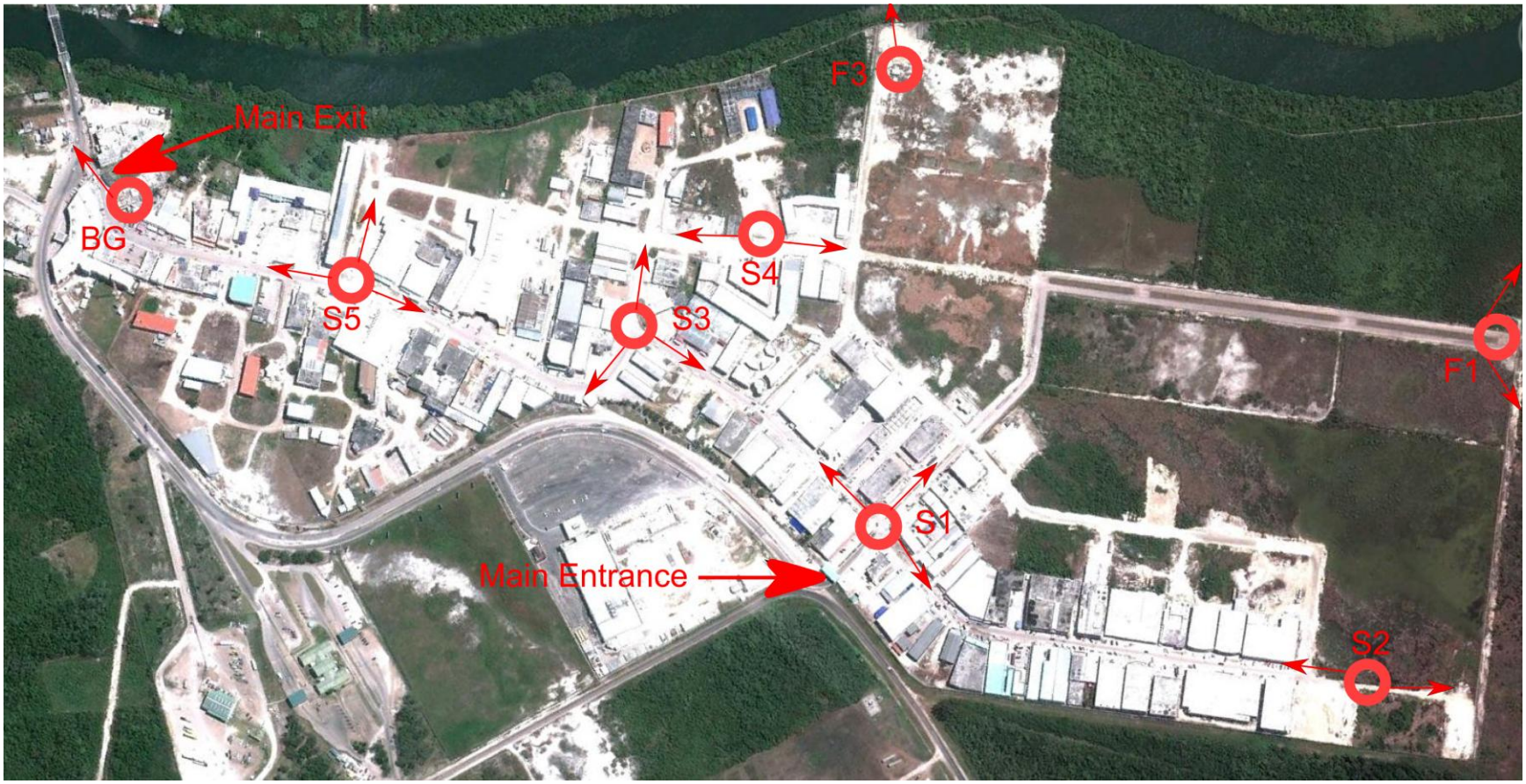
Total Taiwanese ICDF Contribution to Project (US)	**$140,000.00**
Total CFZ Contribution to Project (US)	**$30,000.00**
Grand Total (US)	**$170,000.00**

The contributions requested from the ICDF and those pledged by the CFZ are detailed in the tables below.

Taiwanese ICDF Contribution to Project			
Surveillance and Wireless Equipment			
Quantity	**Item Description**	**Unit Cost**	**Sub- Total**
3	Boxes of UTP Category 6 cable	$250.00	$750.00
8	NanoStation LOCO M5, MIMO CPE, AirMax Station (Ubiquiti)	$300.00	$2,400.00
2	Rocket5 MIMO, AirMax Basestation (Ubiquiti)	$250.00	$500.00
2	MIMO 120 degrees 5Ghz 16dbi AirMax Antenna (Ubiquiti)	$300.00	$600.00
8	Hybrid power supply for camera sites	$6,500.00	$52,000.00
8	IP Cameras PTZ Axis (with Bracket)	$6,250.00	$50,000.00
1	4TB NAS device (Lacie or Iomega)	$1,000.00	$1,000.00
8	Equipment Enclosures	$500.00	$4,000.00
2	Switches 24 ports 1000BaseT	$500.00	$1,000.00
8	Switches 8 to 16 ports with PoE capability	$250.00	$2,000.00
1	Network rack and patch panel (cat6)	$1,000.00	$1,000.00
1	Power Supply for NVR	$6,250.00	$6,250.00
1	Server (NVR)	$15,000.00	$15,000.00
1	Video Encoder (Axis) 4 ports	$1,000.00	$1,000.00
1	Video control joystick	$500.00	$500.00
1	Workstation	$2,000.00	$2,000.00
		Total (US)	**$140,000.00**

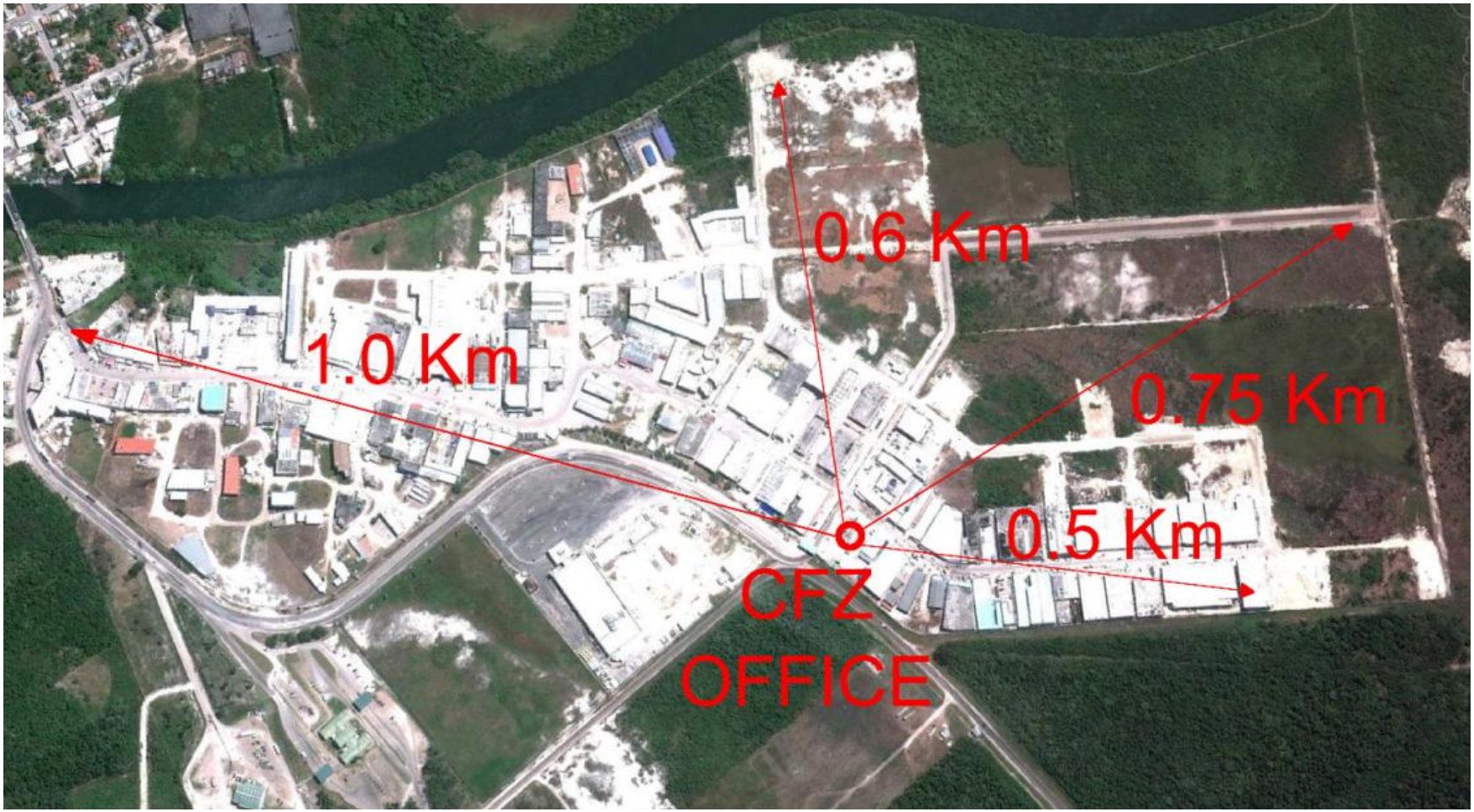
CFZ Contribution to Project			
Installation and Configuration			
Quantity	**Item Description**	**Unit Cost**	**Sub- Total**
1	Masts and Brackets	$2,000.00	$2,000.00
1	Clamps, conduit, wall plugs, screws, etc.	$500.00	$500.00
1	Connectors , jacks, wall boxes (Cat 6)	$500.00	$500.00
1	Shipping and handling	$1,500.00	$1,500.00
1	Labor (6 Weeks)	$10,000.00	$10,000.00
		Sub-total	**$14,500.00**
Construction of Stations			
Quantity	**Item Description**	**Unit Cost**	**Sub- Total**
8	20ft 4" Poles for stations	$500.00	$4,000.00
1	Labor	$1,500.00	$1,500.00
		Sub-total	**$5,500.00**
Refurbishment of New Control Room			
Quantity	**Item Description**	**Unit Cost**	**Sub- Total**
1	Materials for refurbishment of new control room	$5,000.00	$5,000.00
1	Labor	$2,000.00	$2,000.00
		Sub-total	**$7,000.00**
Training			
Quantity	**Item Description**	**Unit Cost**	**Sub- Total**
1	Training sessions of control room personnel	$2,500.00	$2,500.00
1	Materials for training sessions	$500.00	$500.00
		Sub-total	**$3,000.00**
		Total (US)	**$30,000.00**

Annexes



Annex 1: Camera Positions

Annex 2: Wireless coverage Area



Annex 3: Distances to Sites

貝里斯 Corozal 自由貿易區保全系統需求

初步可行性評估

一、 **緣起**：本會重點工作計畫「加勒比海資通訊應用提升計畫」於本年 8 月間赴貝里斯、聖克里斯多福、聖露西亞進行可行性評估,在貝里斯評估期間由駐館安排至Corozal自由貿易區拜會，並由其主席主動提出保全系統提升需求，並指派專人至本會提送計畫提案。

二、 **貝方提案概要**：Corozal 自由貿易區位於貝里斯北部，佔地約一平方公里,區內現有約 200 間商家,貿易型態包含零售與批發，貿易對象以北邊鄰國墨西哥為主。由於貿易區內有大量現金交易，為防範犯罪事件發生，影響貿易區招商，爰貿易區理事主席 Mr. David Akierman 於本會考察團到訪時提出援助需求，並提送計畫書予本會。

貝方提案主要內容為：於貿易區左右兩側架設 8 支無線錄影監視器，並透過建置集中式監控管理中心，以 24 小時輪班方式監控。

貝方本案預算約為 17 萬美元,其中希望國合會協助監測設備及無線設備硬體部分，約 14 萬美元;自由貿易區自行負擔監控中心設備及人員訓練，約 3 萬美元。

三、 **諮詢外部專家**：新光保全許振煙副總經理、遠通電收李浩正總經理、台灣大哥大陳惠琪副處長。

四、 我方初步評估建議：

(一) **本案仍應請貝方明確說明期待為何**，避免對方期待得到之結果其實並非裝設監視器即可達成，故須向對方釐清建置保全系統所期待得到的結果。

(二) 「治安」係受到高度關注之議題，倘貝方欲與本會合作，**應鼓勵貝方從整體規劃面思考，避免不完整的保全系統根本無法有效遏止犯罪，反而讓本會代表之政府外交援助美意受到影響**，間接造成貝方人民不信任我方技術水準。本案單就貝方目前所提規模而言，仍是較為局部片念，恐怕無法有效抑止犯罪。

(三) 本案就整體規劃而言的確超過貝方預算，**計畫應以有效性為主要考量，預算可在與駐館或外交部商議進行資源配置之協調**。

(四) 經檢視貝方所提需求後，係期望透過監視錄影(camera monitor)降低犯罪事件，然監視錄影並無法保證犯罪事件可以得到抑制(無法派人24小時觀看監視螢幕)，僅能記錄事件過程以供事後調查，倘貝方之真正需求係犯罪事件發生當下即可有所反應，進而建立自由貿易區具備良好治安警衛機制之形象，**應在監視錄影之外加上感應系統(sensor)，一旦偵測到不正常動作即可主動警示，並即時處理犯罪事件**。

(五) 貝方目前所提計畫欲架設監視錄影器，考量監視器仍有監看範圍的限制，建議**應針對貿易區內之治安死角加上感應警示燈(alarm light)，一偵測到動作即直接開啟照明，達到嚇阻與警示效果**。

(六) 貝方目前規畫以無線方式架設錄影監視器，然無線方式容易受到干擾與遮蔽，加上貿易區面積規模較小，**宜考量改為鋪設實體線路方式較佳**。

(七) **建議貝方選擇犯罪熱點與重要區域設置緊急按鈕(emergency bottom)**，連結安全監控中心，使犯罪事件可以被主動舉發，提升犯罪防治的有效性。

(八) **貝方目前要求之監視錄影器需求，其實可以結合感應設備(sensor response)，發展智慧型影像系統(INTELLIGENT VIDEO SYSTEM, IVS)，將特定區域發展成為虛擬圍牆之功能**，亦即將幾支監視器的監視範圍框成一個區域，搭配感應設備的功能，一但有異常的人車進入該區域,即可主動示警,由勤務中心進行查看與反應。

(九) 貝方期待裝設之監視錄影器倘增加 I/O 功能，即可結合入侵偵測系統(Sensor)的功能，**將監視器與感應設備連動,用防線的概念將各項入侵動作以時間序列記錄下來，並進一步將相關資訊整合至勤務中心，以準確動員調派警衛進行處理**。此一功能亦能與貿易區現有之防火機制整合，形成整體的保全系統。

(十) 自由貿易區現有約 200 間商家，**可規劃導入付費機制**，由商家付費予貿易區管理中心提供保全服務，除各商家裝設封閉式保全系統外，亦由勤務中心負責警衛服務，**如此將可維持本計畫有收入來源而永續經營，並可成功將援助計畫提升為自給自足之產業**，倘貝方有意願朝此方向發展，有機會變成將援助計畫轉型為產業之成功案例。

(十一) 依據專家建議，自由貿易區現有面積與商家規模，警衛人力資源以「**1 輛車/3 名保全人員/24 小時輪班**」之規模即可因應區內保全需求。

(十二) 以建置時程而言，集中式勤務中心、監控管理系統、監視器等硬體安裝，再加上人員訓練工作(包含後端應用程式教育訓練)，約**1 個月時間即可完成**。

(十三) 總而言之，**本案需與貝方明確定義其期待為何，保全業者之硬體與服務已高度標準化，只要確定貝方期待到哪一個層次，就可以有相應的服務與硬體可以滿足其需求**。必需確定貝方清楚瞭解保全的意義在於「沒有發生的事件就要避免其發生，已經發生的事件就必需要清楚知道在哪裡發生，以及發生的是什麼問題」。

Government of St. Christopher (St. Kitts) and Nevis

MINISTRY OF NATIONAL SECURITY

INTEGRATED LAW ENFORCEMENT NETWORK

(LEF-NET)

PROJECT

PREPARED BY

CARIBBEAN CONSULTING & PROJECT MANAGEMENT LTD.

DATE: 27th July, 2011

BASSETERRE

ST. KITTS

tonu@ccpmlimited.com
joflaherty@ccpmlimited.com

FOR SUBMISSION TO THE REPUBLIC OF CHINA ON TAIWAN

1.1 Introduction

Impact of Crime in St. Kitts and Nevis

The Federation of St. Kitts and Nevis is characterized as an open economy, part of a global supply chain for markets all over the world. St. Kitts and Nevis

Saint Kitts and Nevis Federation's economy is characterized by its dominant tourism, agriculture and light manufacturing industries.

Agricultural (sans sugar), tourism, export-oriented manufacturing, and offshore-banking sectors are now taking larger roles in the country's economy and are being developed more rapidly. The growth of the tourism sector has become the main source of foreign exchange earnings for Saint Kitts and Nevis. In addition, the country has developed a successful apparel assembly industry and one of the largest electronics assembly industries in the Caribbean.

Economic restructuring, specifically diversification of the output base of the productive sectors, is a long-term development strategy of St. Kitts and Nevis and the cornerstone of its entire development programme.

The unprecedented and increasing levels of crime currently threaten the economic restructuring strategies by retarding local and foreign direct investment and threatening the largest sector, tourism, and the associated positive human capital spillovers associated with that industry, e.g job security, employment, income generation .

At the same time, the Federation is facing a high level of public sector debt and the associated debt servicing burden. The level of the country's public sector indebtedness is significantly above the 60% of GDP benchmark that is recommended by the Monetary Council of the Eastern Caribbean Central Bank (ECCB). At the end of 2009, the total public sector debt was 183% of GDP.

This impairs St. Kitts' ability to undertake short to medium-term critical investments in social and economic infrastructure, and underscores its commitment to Public/Private (PPP) initiatives. However the Government is committed to reforms that will address the issues of public safety to safe guard the very sectors that contribute to the Gross Domestic Product.

Part of the major policy focus of the Government in accordance to its Medium Range? Economic Strategy Paper 2009-2011, revolves around the following issues:

1. Strengthening of public finances to generate additional savings to finance infrastructure investment to reduce borrowing;

2. Improving government efficiency;

3. Introduction of cost cutting measures

4. Acceleration of the economic diversification program and

5. Enhancing prospects for sustained economic expansion.

The realitiy as it relates to crime is that

• Crime is networked, connected, and traceable

• Crime can be targeted from multiple angles and levels (activities, associations, funding,

modus operandi, etc.)

• Crime reduction requires multi-agency collaboration and cooperation

Therefore Crime can no longer be combated using purely traditional methods. Criminals have become more sophisticated and innovative in their use of technologies and new tools.

In this vein, the Government of St. Kitts and Nevis through the Ministry of National Security is committed to address National Security efficiency and effectiveness in Communication, Intelligence Gathering and Data Sharing. This effort can also facilitate government's drive towards adopting cost cutting measures which can potentially liberate resources to assist in mission critical infrastructural investments as the state of play changes.

National Security Context

Security threats, incidents and emergencies are essentially local in nature. The process of managing these and executing the activities necessary to respond to the situation begins with the National Security agency.

National Security recognizes the importance of interoperability amongst the security personnel in terms of communication and coordination, as well as the responsibilities of incident management in the twin island federation.

From day-to-day incidents to large-scale events, emergency responders are often disadvantaged by the inability to communicate or share critical voice and data information with other jurisdictions or disciplines. These events frequently expose the lack of communications interoperability capabilities and the inability of national security responders and leaders to manage response activities and perform essential functions on time. This inability to communicate threatens the safety and security of both national security responders and citizens.

The major challenge to the nation's security system has been the lack of **intelligence gathering infrastructure**. In all these situations, it is information that should drive the security solution.

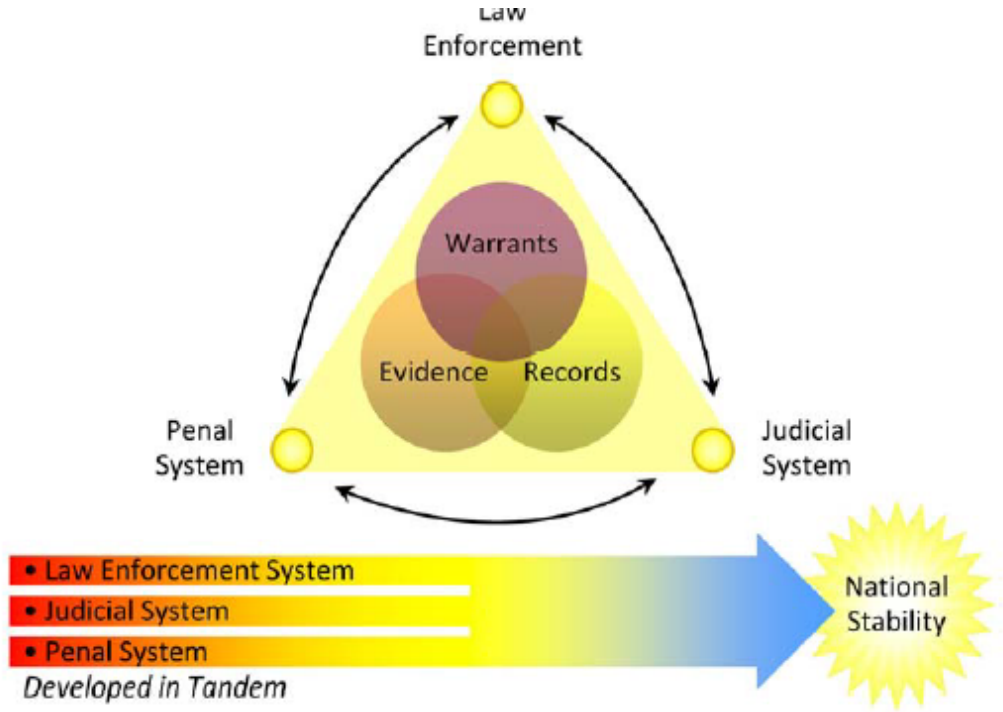
Infrastructure and specialized systems need to convert information and intelligence into actionable data that Law enforcement officials can use to counter criminal threats. Unified and integrated communications enables national security personnel to exchange information via data, voice, and video as authorized, to respond to situations. It enables personnel to have a significant "see, decide

and act" advantage over criminal networks, gangs and individuals. Many activities produce observable data that human and electronic sensors detect. The combination of trained and experienced analysts, coupled with open information sharing arrangements and advances in technology, allow departments to process and analyze a variety of collected observables from different, but complementary systems, and more rapidly produce actionable intelligence for decision makers.

Interagency collaboration through liaison personnel is instrumental in bridging gaps and issues between organizations. Successful collaboration depends on the following factors among others:

- Establish strong relationship networks
- Build mutual trust and respect for colleagues
- Share a common vision
- Minimize territorial issues
- Encourage continuous communication
- Eliminate impediments to information sharing

All national security agencies must have seamless interoperable communications to manage their responses, establish command and coordination, maintain situational awareness and function within a common operating framework. This will lead to improved response capabilities and provide a more comprehensive approach to National Security, which will lead to increased safety for all citizens.



1.2 National Security Law Enforcement Network Project Proposal

Project Background & Rationale

National Security of St. Kitts and Nevis is made up of fourteen (14) police stations, ten (10) in St. Kitts and (3) in Nevis. The police force has approximately 500 personnel.

National Security also has the St Kitts Nevis Defense Force (SKNDF). It currently consists of an infantry unit (the St. Kitts Nevis Regiment) and a maritime unit (the St. Kitts Nevis Coast Guard). Both units having regular and reserve elements, all under the command of Force Headquarters (FHQ, SKNDF). The SKNDF has an active force of 300 personnel with a corps of 150 cadets.

Information is the lifeblood of effective day-to-day operations within the National Security community. In making countless pre-emptive, in-situ and reactive decisions every day, officials must have immediate access to timely, accurate, and complete information. It has become clear that effective decision making requires information that must often be shared across a broad landscape of systems, agencies, and jurisdictions.

Current Situation

General findings that relate to all departments

- Need for interdepartmental connectivity (intranet, email, radio communications , etc)
- Lack of information management systems
- Analog Radio Infrastructure and inadequate range

Telecoms

- Need for Training for dispatchers
- Absence of proper head quarters premises monitoring
- Inability to conduct talk groups
- Need for updated real-time voice call recording
- Lack of secure radio communications for covert units
- Lack digital storage
- High Cost of current communications operation

Offences – Criminal Investigative Division and Minor Offences

- Inability to pull run reports in an effective manner
- Need for capability to fast track deployment to a scene to commence reporting
- Procedures are manual

Immigration Department

- Require PC workstations and reliable network printing

Minor Offenses

- Require an Information Management System to enhance their capability to add to statistics that Local Intelligenco Office (LIO) does currently have.

Police Prosecution and Court Processes

- Require PC workstation and access to case files electronically
- Require reliable communications

Local Intelligence Office (LIO)

- Available statistical database needs upgrading
- Requires situational awareness database or information management system capabilities
- Requires a workflow system to facilitate the daily reports

Criminal Records Office (CRO)

- Records are currently all manual
- Requires a Records Registry and digitization of older records
- Upgrade of finger print comparison software
- More efficient file/information storage
- Needs efficient (digital) cataloguing of evidence collected at crime scenes
- Needs a Conviction database

Special Service Unit (SSU)

- Database specifically for gangs and gang activity
- Reliable communication during operations
- Lack of surveillance and intelligence gathering tools

Drug Unit

- Local drug database
- Reliable communications

Vision

From the high level assessment conducted by the project team, the following Vision has been articulated.

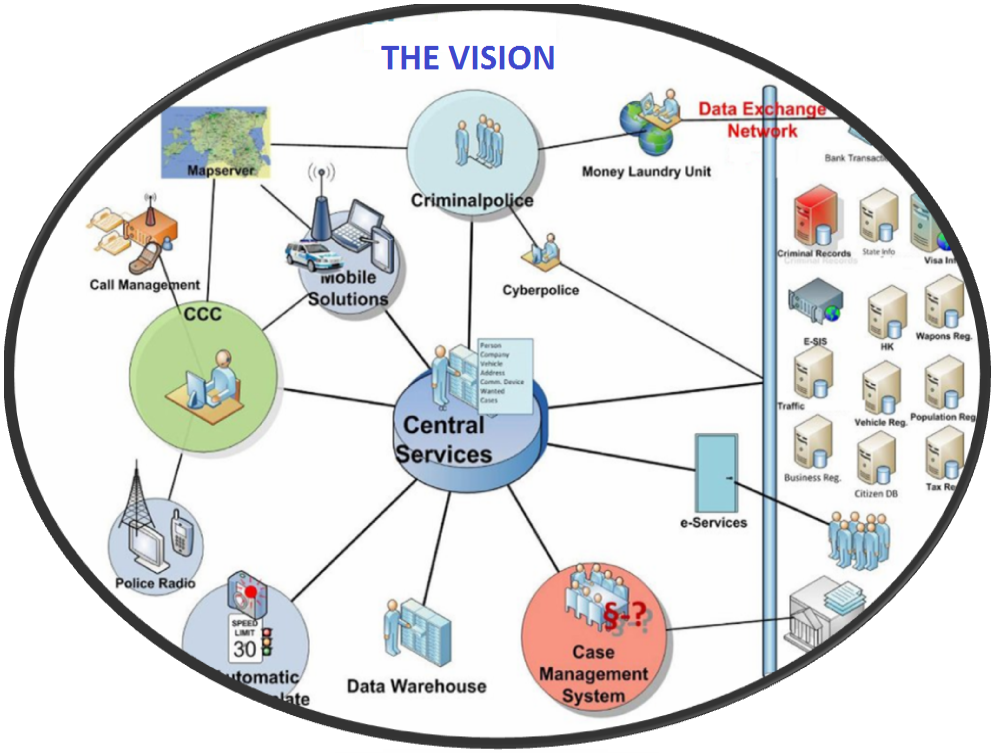
The Information and Communication Vision for National Security St. Kitts and Nevis

1. Modern State of the Art Scalable Internet Protocol Network, where this infrastructure would be leveraged as an effective integrated communication platform tool where many forms of electronic technologies and applications (audio/voice (radio, mobile, telephone), data (text, databases), and video)will be utilized in a seamless environment.

2. The ability to facilitate inter-agency collaboration in the processes of Law Enforcement, Civil and Emergency Management

3. To facilitate effective information management to foster proper intelligence and foster quick and responsive units

4. To Increase the efficiency and effectiveness of law enforcement and civil management



In order to achieve this objective, the following ten (10) goals will need to be realized.

1. Robust and Scalable Network Infrastructure Design and Development

2. Establishment of a National Security Network Operations and Control Centre (NSNOCC)

3. Re-Engineering 911 Emergency Communications, Inter Agency Collaboration, Management & Control

4. Establishing Effective Resource Management

5. Centralised Information Management and Intelligence System Design and Development

6. Inter-Agency Database Sharing and Collaboration for Key National Registers e.g Civil Registry, Business Registry

7. Case & Records Management System for Law Enforcement and the Judicial System

8. Establishment of Island Wide Close Circuit Television (CCTV), Vehicle License Plate Recognition and facial recognition

9. Extensive Sensitization and Training throughout the Entire Implementation Process

10. Establishment of a National Security Data Warehouse

Project Strategy

Caribbean Consulting and Project Management Ltd. (CCPM Ltd.) recognizes that there are unique challenges associated with implementing complex programs that are context-specific, relevant, and results-oriented. As a result, we work extensively through and areas of programming.

For the Police Communication Network And Information Management Project, CCPM's team of highly qualified and experienced practitioners bring technical experience, qualifications and competencies in Telecommunications, Information Communication Technology (ICT) Management, Electronic Governance, Knowledge Management and Training backed by more than 40 combined years of relevant professional experience in implementing complex projects.

Also critical to our success is a well-articulated strategy that fits with each local context (detailed in 2. Methodological Approach, below).

As part of this strategy, CCPM Ltd will adopt an implementation framework which will allow us to achieve the objectives of the Project. These are practical, tangible and designed to provide clear benchmarks that can be monitored over the course of the consultancy:

- A commitment to transparent operational and communication processes that focus on a team approach to program design, development, implementation, and monitoring and evaluation

- An established, on-the-ground presence of partners with regional expertise

- Efficient and effective resource planning

- Expertise in Knowledge Sharing Development and ICT Appropriation

We expect that the decision to employ one or a combination of capacity building techniques will be informed by a solid understanding of the relationship among stakeholders, the institutional environment and social and cultural factors.

CCPM Ltd. envisions using a number of design features to ensure the project is developed in a participatory manner to engage stakeholders from various levels in all aspects of the project. In addition, the project team is cognizant that the learning populations are adult learners seeking learning experiences that provide usable knowledge and skills.

As a contribution to the overall Information and communications vision for National Security, the following Project has been designed to address immediate information and communication needs while providing a solid framework to facilitate the realization of some of afore mentioned goals.

This Project envisions that National Security will adopt new management and response capabilities to assume more efficient preemptive and in-situ approaches. It will also reduce reactive approaches due to enhanced processes and tools that enable multi-agency and departmental communication and coordination and joint service operations. This will be achieved through the deployment of a security multimedia network for National Security, in order to address the challenge of inadequate intelligence infrastructure.

The network will not only provide National Security a platform to communicate outside the regular commercial network, it will also be equipped with surveillance cameras.

The project frames a scalable, responsive, dynamic, sustainable, and evidence-based platform and approach for those who contribute to the management of and response to national security events. The project framework also takes into account the changing nature of threats, vulnerabilities, and the varying contributions and capabilities related to these events in the Federation.

Project Overall Objectives:

- To empower National Security with an integrated communications network where officers can securely communicate, collaborate among themselves and with regional and international security authorities to better coordinate responses that lead to the quick resolution of a threat.

- To improve the effectiveness, responsiveness and management of national security resources.

- To enhance workforce efficiency and productivity

- To facilitate interoperability between first responders (Police, Defence Force, Fire Department, Emergency Medical Services, National Emergency Management Agency (NEMA))

Specific Objectives:

1. Robust and Scalable Network Infrastructure Design and Development
2. Establishment of a Video Surveillance Framework
3. Establishment of a National Security Network Operations and Control Centre (NSNOCC)
4. Re-Engineering 911 Emergency Communications, Inter Agency Collaboration, Management & Control
5. Establishing Effective Resource Management
6. Centralised Information Management and Intelligence System Design and Development
7. Communication and Information Management Awareness, Education and Training

Expected Results:

1. Police Headquarters Local Area Network and Wide Area Network
2. Police Meshed Network for Mobile Access and Video Surveillance
8. National Security Network Operations and Control Centre (NSNOCC)
3. Enhanced Digital 911 Emergency Communications
4. National Security Access and Control and Identity Management System
5. Improved Asset Management
6. Central Police Information Management and Intelligence System
7. Empowered Police Force and other law enforcement agencies

OUT OF SCOPE

For the purpose of this proposal the following services will be considered as out of scope of this proposal and would be executed in the project mode on an individual basis. Separate proposals would defined for these individual projects, this would be supplied at a later date and placed as contract addendums;

1. Criminal Hotline IVR and 24hr Call Centre Services
2. Case-Flow Management System - (Evaluation of the DPP Processes)
3. Prison Registry Database
4. Onsite Training after the project implementation Period
5. Financing for major upgrades will be provided by the Client and treated as a project outside the scope of this Agreement

Methodological Approach for Project Implementation – Core Components:

The Consultant's Project Implementation approach will consist of three (3) Core Components with three (3) main phases in the First Component and ongoing Project Management.

Fig 2 below shows a graphical figure of the approach. The implementation of some of the activities under the sub-components is interlinked.

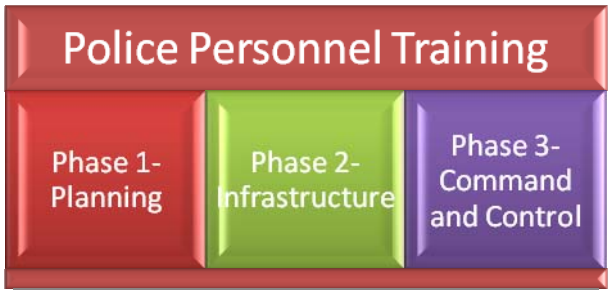


Fig. 2 – Consultant's Approach for Project Implementation Component 1- Three Phases

1.3 Detailed description of activities, inputs and outputs

1.3.1 Summary of specific activities

Main Activities for the Assignment. The assignment is scheduled to start by the beginning of September 2011 and last for a period of 13 months

CCPMs propose a Three-component approach and Three phases approach, outlined in the fig. 2, to achieve the project objectives and results.

List of Components and Activities, Inputs and Outputs are shown in the following tables:

• **MAIN COMPONENTS**	
• **COMPONENT 1**	❖ **POLICE COMMUNICATIONS AND INFORMATION NETWORK**
• **COMPONENT 2**	❖ **TRAINING AND CAPACITY BUILDING**
• **COMPONENT 3**	❖ **PROJECT MANAGEMENT & ADMINISTRATION**
• **ACTIVITIES IN RELATION TO THE OVERALL IMPLEMENTATION OF THE PROGRAMME**	
COMPONENT 1 : POLICE COMMUNICATIONS AND INFORMATION NETWORK	**PHASE 1**
	A 1.1 Development of National Security Information and Communication Architecture **o Site Surveys and Mapping** **o Technical, Process and Skill Audit**
	A 1.2 Development of Transition and Change Management & Training Plan o **Analysis** o **Design**
	A 1.3 Establishment of Project Steering
	A 1.4 Set up of Project Management Office & Project Management Platform
	A 1.5 Project Procurement of Equipment and Materials
	PHASE 2
	A 2.1 Design interior of Network Operations and Control Centre
	A 2.2 Construction and Installation of Finishing and Furnishing of Network Operations and Control Centre
	A 2. 3 Establish Back Up Network Operations and Control Centre and Satellite Centre

	A2. 3.1 A) Build and implementation of Police HQ Local Area Network (LAN)
	A2. 3.2 B) Build St. Kitts & Nevis Police Districts Wide Area Network (WAN) & VPN
	A2. 3.3 C) Wireless Mesh Network & Video Surveillance Hardware
	Sub Phase 1: Basseterre
	Sub Phase 2: Cayon, Sandy Point and Charlestown(Nevis)
	A2. 3. 4 D) Wireless WAN Redundancy
	A2.4 Digital Radio Conventional System Infrastructure & Radios
	A2.5 Process Mapping and Reengineering & Central Services Design - – Police Intelligence Information Management System
	PHASE 3
	A3.1 Unified VOIP Communications
	A3. 2 Computer Aided Dispatch & 911 Call Management Platform
	A.3.3 Locations Based Map Software & Server
	A.3. 4 911 SMS Software and Management
	A.3.5 Central Services Development & Implementation – Police Intelligence Information Management System & Applications
	A.3.6 Deployment of Mobile Terminals In Vehicles, Handhelds and Installation of PC Terminals
COMPONENT 2: TRAINING AND CAPACITY BUILDING	**A.4.1 Development and validation of the development action**
	A.4.2 Implementation
	A.4.3 Evaluation
COMPONENT 3: PROJECT MANAGEMENT	**A.5.1 Procurement Management**
	A.5.2 Administrative and logistic support during the whole duration of the project

	implementation
	A.5.3 Financial management of the services
	A.5.4 Management of the operational budget and cash flow projections
	A.5.5 Quality supervision
	A.5.5 Liaise and report to the contracting authority

1.3.1 COMPONENT 1: POLICE COMMUNICATIONS AND INFORMATION NETWORK

Project Activities

Each activity requires a careful preparation and implementation in order to achieve the envisaged results. The following describes the approach and methodology foreseen for each activity which is divided into three (3) Phases.

A.1 PHASE ONE : PREPARATION, PLANNING AND ANALYSIS

A 1.1 Development of National Security Communication Architecture

The architecture starts with the preparation of the project and will occur to support the data gathering needs of the project. i.e site survey, process mapping .

Interviews and meetings as well as a comprehensive basis for data collection and information survey will be available. All gathered information needs to be analysed, validated, clustered and brought together in a systematic approach which will serve to recognize and achieve the key information. Some figures or given information might be verified through additional research. Further relevant information will be added by desk research. The final results will be filtered to get all key information concerning the stakeholder identification and to support the development of the designs and workplans.

- **Site Surveys and Process Mapping**
- **Technical, Process and Skill Audit**
- **Stakeholder Consultations**

A.1.2 Development of Transition and Change Management & Training & Capacity Building Plan –

In order to address the holistic change management process, a Training and capacity building programme would have to be developed and implemented throughout all the phases of the project. The Training Process will be adopt the ADDIE Instructional Design Model. See Fig. 3 below.

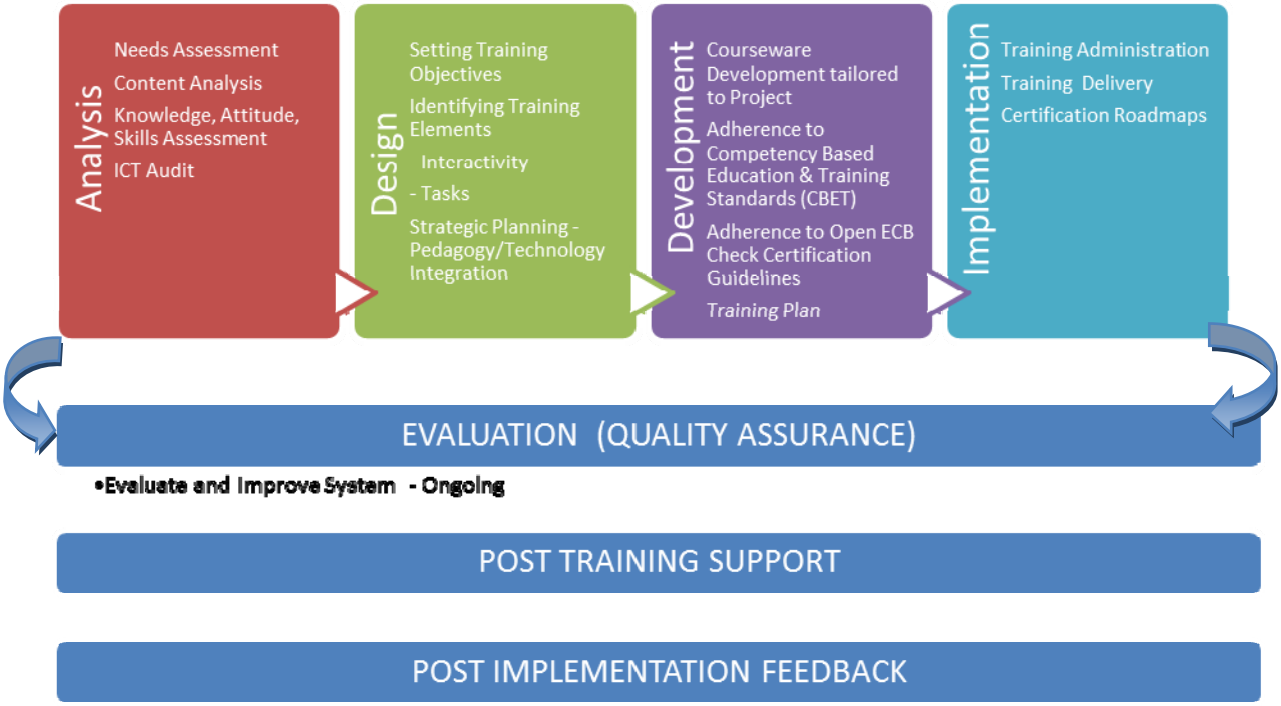


Figure 3: The Consultant's Instructional Design Model

Below is a summary of the training programme which will comprise core Communications Training and systems training. Training programmes will be designed, in close consultation with the beneficiary and other stakeholders through the process of a training needs analysis, in order to meet the needs identified by the capacity and training needs analyses undertaken. This participatory approach makes the three types of workshop (consultative, informative, and training) efficient and effective and is fully in line with the "backbone strategy".

Training tool kits (slide show, CD, manual) are to be drawn up and implemented in accordance.
CCPM Ltd. will utilize a competency-based (CBET) approach for the design and delivery of all its education and training consultancies. This approach focuses on the attainment of standards and the honing of competencies that are matched against of the identified training needs. Participants are deemed to be competent when they can perform to the agreed outcomes. This is the approach recommended globally for training assessment and certification for workforce enterprise development.

POLICE PERSONNEL TRAINING

Soft Skills

- Interpersonal Communication
- Effective Listening
- Conflict Resolution
- Negotiation
- Dispatch Communications and Logistics
- Technical Writing
- Effective Interviewing
- Effective Reporting

Technical Skills

Dispatch Systems Training

Police Information Systems Training

Digital Communications Training

Server Management

A.1.3 Establishment of Project Steering

The Project will facilitate the setting up of a Project Steering Committee comprising mainly of the key decision makers of the Ministry of National Security which will serve to provide Project Oversight.

A.1.4 Set up of Project Management Office and Project Management Platform

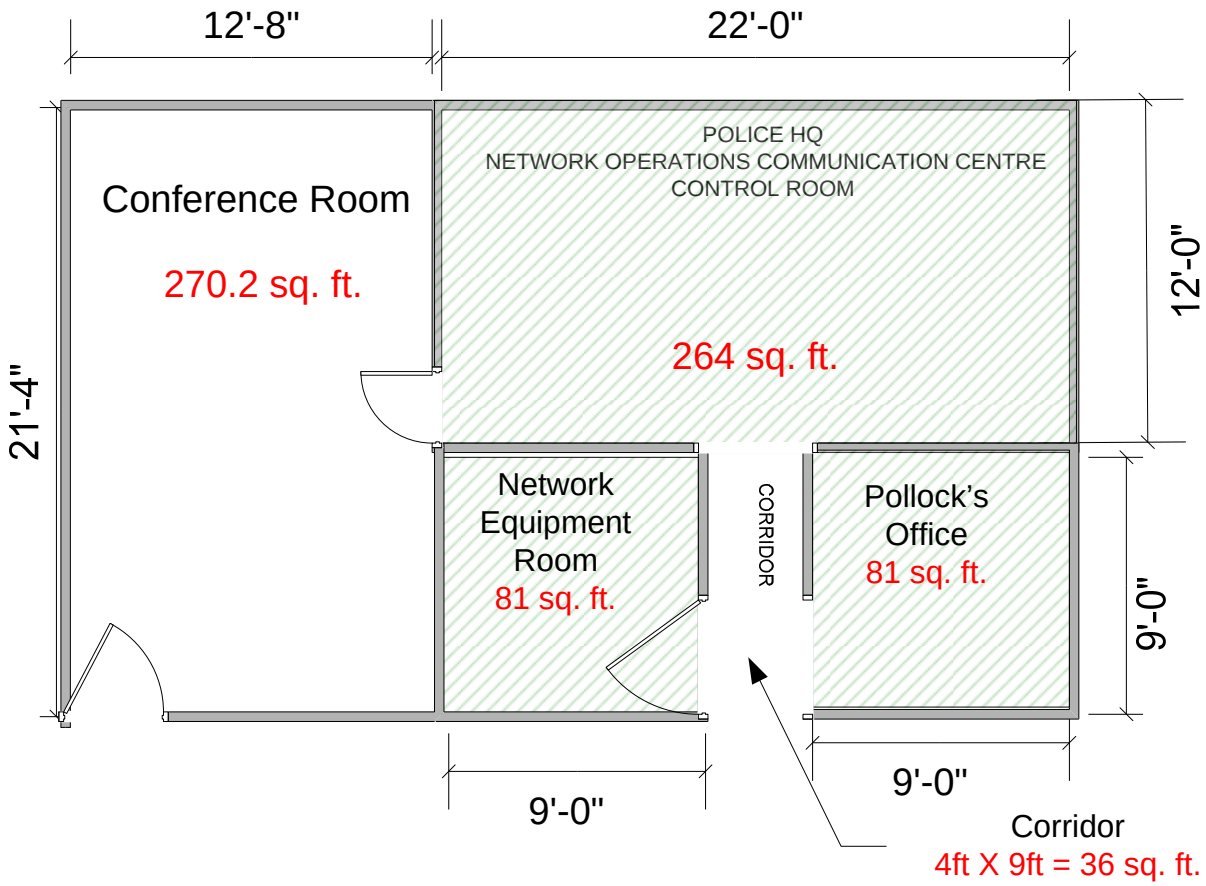
The Project Management Office will be set up to facilitate coordination of the Project. Project Reporting and Communication with the Project Steering Committee will be supported by a Project Management Platform which will serve as an intranet where documents will be stored and communications will be delivered and will facilitate project monitoring and project scheduling.

A.1.5 Project Procurement of Equipment and Materials

The Project will procure essential equipment to support the implementation of the project. A list of potential items to be procured is annexed to this document.

A.2 PHASE TWO : INFRASTRUCTURE DESIGN, DEVELOPMENT & ESTABLISHMENT OF THE NATIONAL SECURITY NETWORK OPERATIONS AND CONTROL CENTRE (NSNOCC)

A.2.1 Design interior of Network Operations and Control Centre

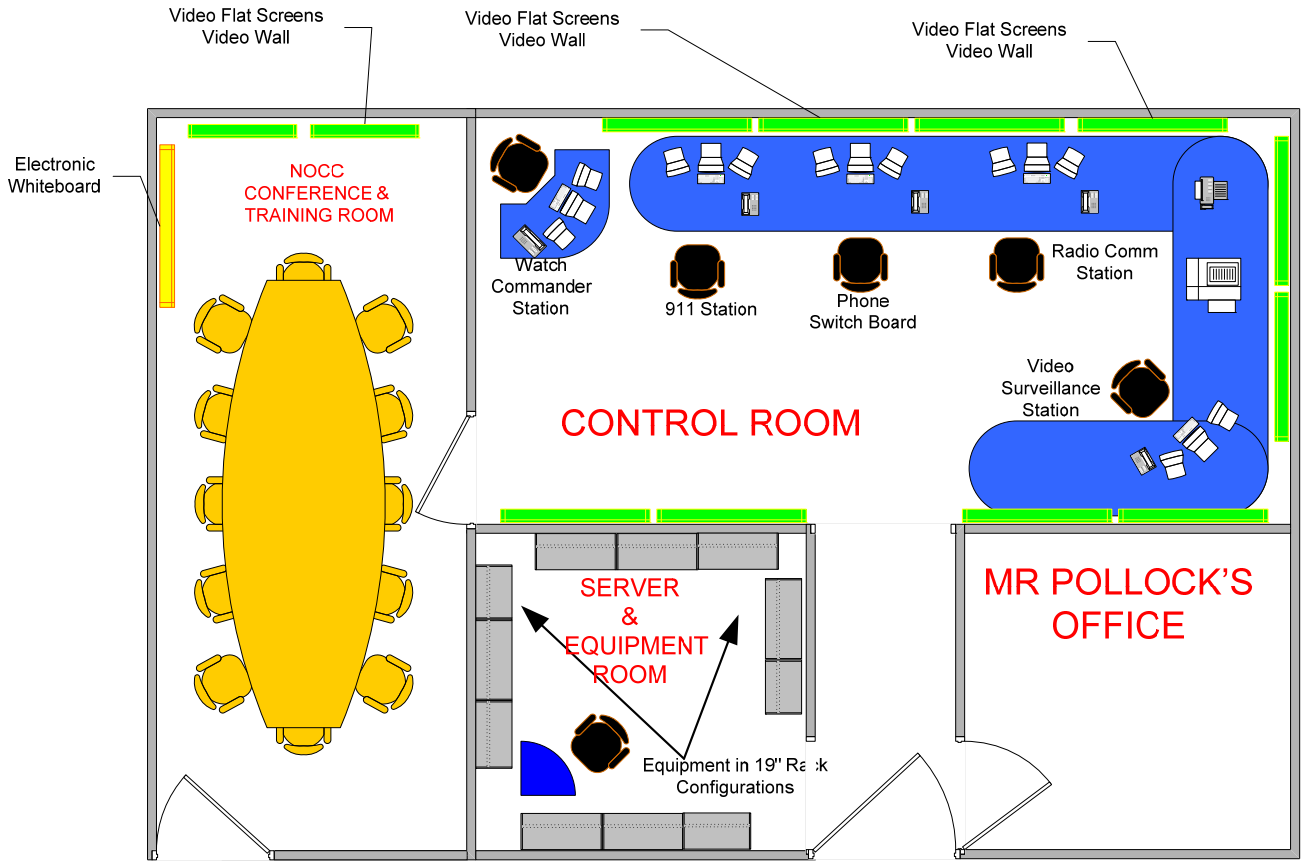


POLICE HEAD QUARTERS
NETWORK OPERATIONS COMMUNICATION CENTRE, (NOCC)
FLOOR PLAN DIMENSIONS

The proposed plan calls for the implementation of a Local Area Network (LAN), at the Basseterre HQ building. The Network Operations Communication Centre (NOCC) will be housed on the fourth floor of the HQ building.

This component will deal with the proper design of the NOCC.

A.2.2 Construction and Installation of Finishing and Furnishing of Network Operations and Control Centre



POLICE HEAD QUARTERS
NETWORK OPERATIONS COMMUNICATION CENTRE, (NOCC)
OFFICE LAYOUT

The creation of the NOCC will serve as the seat of Command and Control for communications assets and will serve as the hub for the Law Enforcement Network for the Ministry of National Security and the Police Department.

The NOCC will include an in-line uninterruptible power system with back-up diesel generator, back up power through UPS and Solar. The NOCC will host multiple redundant Internet service providers to ensure network availability.

A.2.3 Establish Back Up Network Operations and Control Centre and Satellite Centre

A backup NOCC will be essential to serve as a substitute Command and Control centre in the event of failure. This backup NOCC will be implement at the NEMA headquarters. A smaller Satellite Centre for the NOCC will be located in Nevis in order to facilitate a seamless communication between the two islands.

A.2.4 A) Build and implementation of Police HQ Local Area Network (LAN)

As stated above the Police Head Quarters in Basseterre will be the primary central hub of the proposed National Security Law Enforcement Network.

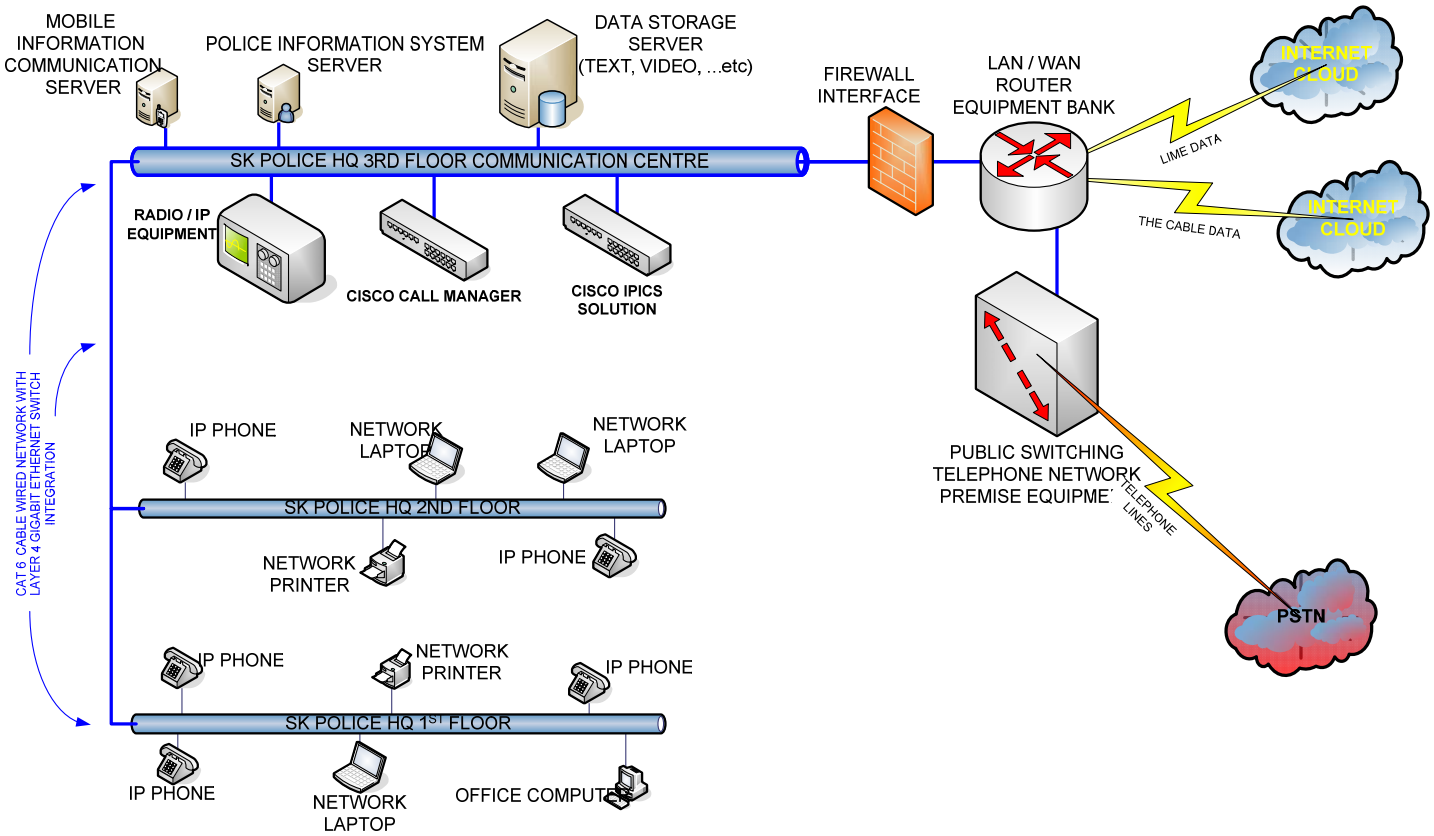


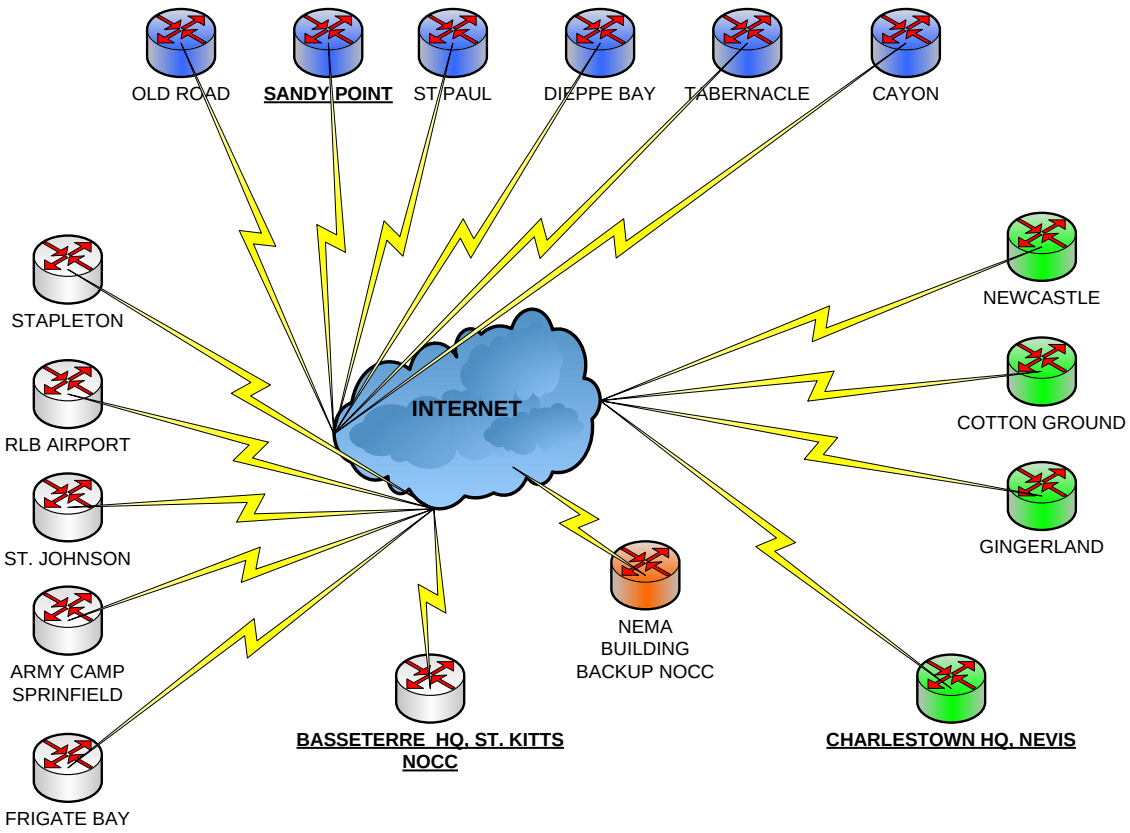
Figure 1 Basseterre Police Head Quarters Network - (LAN)

A.2.4 B) Build St. Kitts & Nevis Police Districts Wide Area Network (WAN) & VPN

The diagram below is an illustration of the proposed WAN for the Ministry of National Security. The Police HQ in Basseterre will house the main network center with a possible backup network center in the NEMA building

There are about 14 Police Stations spread out across the two islands of St. Kitts and Nevis, with additional sites at the Army Camp and the Airport.

- **10 Stations – St. Kitts - 68sq miles**
- **4 Stations Nevis - 36sq miles**



POLICE STATION WIDE AREA NETWORK (IP NETWORK)

There are three Police Command Sectors separated into Districts A, B, C

- District A, illustrated in GRAY, shows the Basseterre St. Kitts –Capitol Town area Police stations.
- District B, illustrated in **BLUE** , shows the St. Kitts rural area Police stations
- District C, illustrated in **GREEN**, shows the Nevis island area Police stations

A.2.4 C) Wireless Police Wide Area Network

a. Wireless Mesh Network Establishment & Video Surveillance Hardware Placement on Mesh.

The approach is to implement a wireless meshed network which will serve multiple purposes to support law enforcement mobile units.

This will support the video surveillance initiatives by providing a scalable infrastructure to facilitate “hot spot” deployments of video surveillance cameras which are connected to the LEFNET . Also other cameras such as traffic cameras, automated Vehicle License Plate recognition and Facial recognition cameras can be supported.

A.2.4. D) Wireless WAN redundancy

The project will then explore other wireless redundancy possibilities with wireless service providers in order to ensure that the network still functions in an event of a failure at any one point. This redundancy option will be evaluated.

A.2.5 Digital Radio Conventional System Infrastructure

There will be three possibly four main sites where Radio Repeaters will be located. There will be two sites in St. Kitts at Brimstone Hill-Sandy Point and in Basseterre. The other site is on the island of Nevis at the Brownhill location. A possible site might be Dieppe Bay.

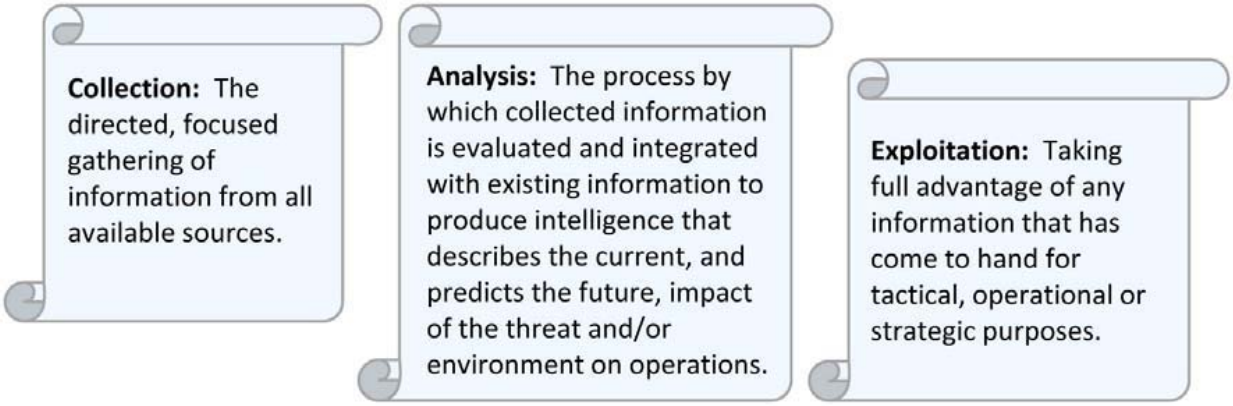
The conventional digital radio communications system will facilitate the extension of the existing radio infrastructure as well as to provide a state of the art conventional radio system which will address a number of issues associated with trunked radio systems. Some of these are;

- Reduction of dependence on the building facilities where the controller is located. Non-trunked systems can be made diverse by locating comparators and other common equipment at multiple locations, so as not to be dependent on a single building.
- Loss of Communication due to Isolation of central controller from remote radio sites-The proposed conventional radio system will be built typically using a compartmentalized approach so as not to be dependent on a single building or facility.
- Reduction of Push to Talk delays

- Ability to facilitate an infinite number of simultaneous conversations
- Low audio latency
- Non dependency on proprietary software, which allows maintenance reduction – no recurring license fees, as well as allowing for various brands of radios and radio systems to communicate seamlessly.
- Competitive Pricing, costs three to five times less than and options for Maintenance
- Incremental replacement of infrastructure equipment is possible
- Very easy and low cost to expand coverage or to make changes
- Has a much longer life cycle than trunked radio – 15-20 years if not longer

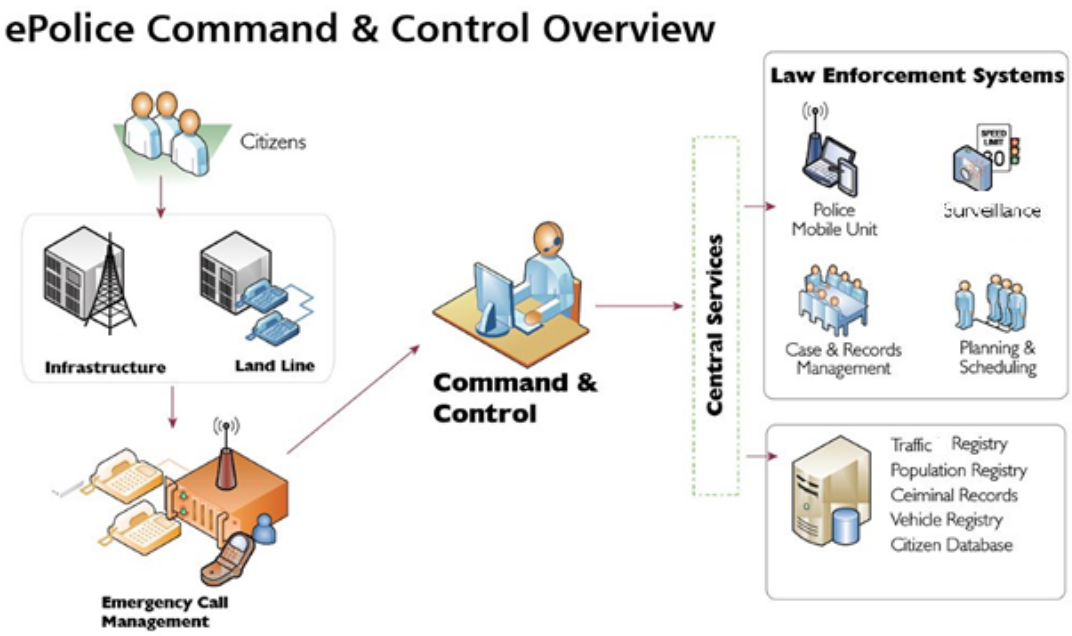
The system will comprise Infrastructure, radios and GPS microphones.

A2.5 Process Mapping, Reengineering & Central Services Design – Police Intelligence Information Management System



The nature of National security and specifically the police force is based on intelligence gathering which must be firmly embedded into the operations process. While each operation and environment differs in design and circumstances, all operations follow the planning, preparation, execution and assessment cycle inherent in the operations process. Understanding this process is essential in designing and developing a Police Intelligence and Information Management System. This will be the precursor to the actual development or finalization of this system which is central and core to the functioning of the organization and National Security on a whole.

Phase 3: National Security Command and Control and Platform

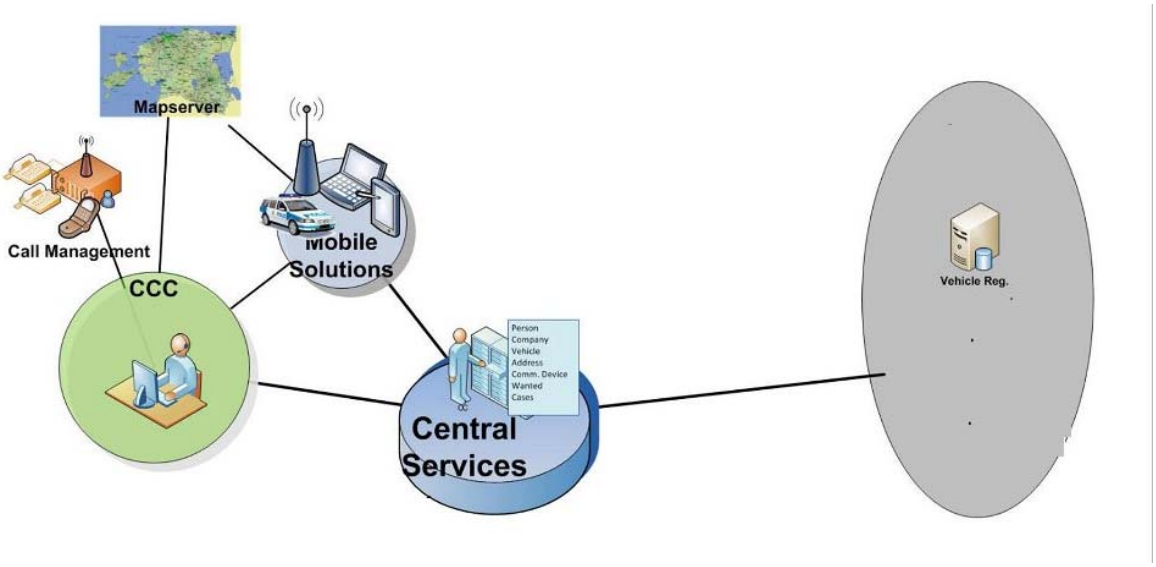


Citizens depend on domestic emergency service to effectively react to situations that threaten their lives and property. This requires real-time secure collaboration between all National Security Departments other Government Agencies to accurately exchange information.

Effective emergency management is crucial and organizations need to be able to respond as quickly as possible to an incident and be prepared for a wide range of threats. Whenever emergency calls come in, time is critical. With the Command and Control Platform, Civil and Emergency Management can save lives by ensuring that the right resources are quickly dispatched to the scene.

Therefore it is important for the establishment of a National Security Command and Control Infrastructure and Platform .

The National Security Command and Control Platform is a flexible solution for the operations centre that can integrate the existing analog communications infrastructure.



The Platform comprises the following software applications and hardware complements;

- **Unified VOIP Communications**

- **Computer Aided Dispatch & 911 Call Management Platform**

A single call to the 911 Centre or to any police extension will facilitate Dispatch unit to ensure that resources are contacted, and deployed all at the same time. With other tools such as GIS mapping and Tracking, dispatch can file incident reports that are necessary to deploy teams.

- **Locations Based Services with Location Map Software & Server**

Geographical Information Systems (GIS) and mapping are essential components of national security solutions. The LEF-NET will include integrated support for GIS services and mapping services. It will also provide for asset tracking.

- **911 SMS Software and Management**

911-SMS is an extension to traditional 911 communications, which would allow customers to send a free text to the 911 Centre. The proposed solution will facilitate two-way texting and the dispatcher sending out an undetected call to the mobile device to enable ALI (automatic location information) .

Alternatively, the 911 centre can be proactive and launch a campaign to pre-register persons on a 911 hotline with the use of IVR to retrieve the ALI (automatic location information).

- **Central Services – Police Intelligence Information Management System & Applications**

  As mentioned before, this application is central and core to the entire operations of the Police Force and as such will have a number of features. Some of these are highlighted below.

  - **Security Knowledge Management System**

Security

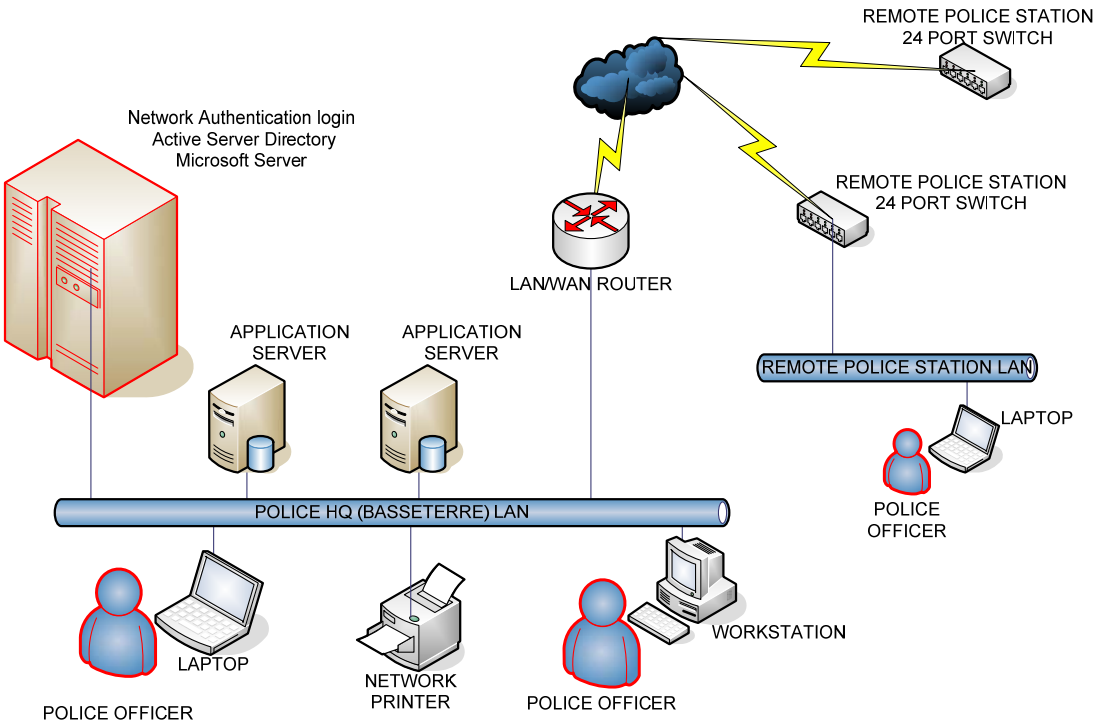
The LEF-NET will be a unique offering with advanced security features. All applications will be engineered to meet International best practices for central intelligence agencies which underscore the requirement of physical security standards for hosting classified data in a sensitive compartmented information facility . These protections will allow LEF-NET to meet and exceed the protections necessary for hosting sensitive, unclassified information for our customers. In addition, biometric controls can be used to improve access and control.

The project foresees the registration of all Human Resources and the issuance of contactless proximity cards, locking mechanisms, for facility control and access as well as the issuance of digital signatures for auditable electronic logs.

Information Sharing

A key requirement for information sharing between the LEF-NET and other Government applications is federated identity management. LEF-NET will support the Global Federated Identity and Privilege Management (GFIPM) framework that provides a standards-based approach for implementing federated identity.

This allows users of LEF-NET applications to identify and authenticate with other government systems participating in the federation.



POLICE NETWORK USER AUTHENTICATION

- **Asset Management**

- **Intranet**

LEF-NET applications will include capabilities in information and document management through the creation of an Intranet system which will be optimized for national security missions. This will include an integrated, searchable document repository (database) with workflow approval and expiration date mechanisms and the ability to apply metadata and tags to all content.

It will include the capability for non-technical users to create custom forms using a Web 2.0 drag-and-drop user interface. Rich, dynamic forms can be created with integrated workflow and business rules.

The Intranet will include but not be limited to the following;

- **Document & Knowledge Management**
- **Email Management**
- **Reporting Management**
- **Surveillance Management**
- **Incident Management**
- **Gang Management**
- **Case Management within the Police Force**
- **Web Communications**
- **Intelligence Databases**
  - **Weapons Register**
  - **Linkage to Civil Register**
  - **Drug Possession Register**
  - **Offenses Register**

Computer Terminals

It is forseen that some more Computer Terminals may need to be deployed at the various stations. Clarification on the numbers can be given during the Technical Audit.

Mobile Accessibility –

One of the essential tenets of having a network such as the proposed LEF-NET is the ability to access information via a web browser or mobile device. The project forsees the deployment of Tablets in Vehicles, Handhelds for specific departments such as Traffic, CID, CRO, SSU and Drug Squad.

The LEF-NET will be made accessibile to all forms of mobile units via the intranet or internet browsers.

The following mobile units will be deployed;

- **Laptops, Tablets, Smart Phones and Tablets with wifi connections for police car with data terminals,**

National Security Command and Control Platform Summary

Software	Hardware
- Computer Aided Dispatch & 911 Call Management **- Radio Management**	**Video Switches ((CISCO VSM) – Virtual Matrix)** **CFT Flat Screens and Consoles** **PSTN Switches** **Servers**
Voice Over IP Software, **Soft Phone Client**	**Servers/Switches** **150 amount VOIP PBX phones and extensions**
Location Based Software	**Map Servers** **100 GPS Microphone for Mobile and Portable Radios**
911 SMS Software	**Services**
Development and Testing (Central Services Intranet and database application) **Police Intelligence and Information Management System** - **Workforce Registration** - **Access and Control** - **Asset Management** - **Identity Management** - **Video Surveillance Management** - **Surveillance Management** - **Incident Management** - **Gang Management** - **Intelligence Databases** o **Weapons Register** o **Linkage to Civil Register** o **Offenses Register** o **Drug Possession Register**	• **Servers** • **Servers/Switches, Cisco VSM** • **Video Storage Servers** • **Video Wall Consoles** • **Contact Less Cards** • **Key Pad/Access & Control Hardware** • **Biometric Readers** • **Identity Management terminals** • **GPS Tracking Hardware**

1.1.4 COMPONENT 2: TRAINING AND CAPACITY BUILDING

A.2.1 Development & validation of the development

The Consultant's approach to the development of the training programme will be in a modular format to allow for flexibility with reference to supporting the delivery of a non-prescriptive approach as different departments would have different needs. Through the development of necessary training modules, more targeted training can be delivered while adding to the knowledge base of the Communication Network for future employees. Also new capacity development needs are likely to surface during project implementation.

A.2.2 Implementation

This component's activity is interlinked with the Training and Capacity Building Component and focuses on the Training Plan which will include the amendments to training material and the monitoring.

The capacity building should result in an actual transfer of technology: after the completion of the tasks, the Trainees should be able to apply the acquired knowledge to use the new systems and processes and enforce adherence to the Quality Assurance Metrics and Standards defined. This capacity building should foster adoption.

All trainers will apply multiple methods to create a state-of-the-art learning environment for the adult learner. A constant change between plenary sessions, such as presentations, facilitated discussion, the pinboard technique and working in groups will be implemented, with cases and critical incidents, and group presentations being a central tool. More individual advice will also be given during the online coaching.

The consultant will focus on the implementation and assessment of this programme. The Training programmes will be implemented using a training schedule articulated by the training plan and will be programmed at times and locations that would be most convenient and accessible to the participants.

All trainings will be run as 'blended trainings': i.e. combining the advantages of classic presence trainings and the opportunities provided by the internet via web-based trainings. All training materials will be SCROM compliant and will be posted on a virtual learning environment (VLE) consisting of a Learning Content Management System (LCMS) which will be defined and deployed,

The trainees will get access to this section. Apart from online coaching, there will be tasks and testing for the trainees.

The Consultant will deploy Training Teams comprising of a Capacity Building Expert, IT Expert and Administrator, who will be responsible for the organisation of and delivery of simultenous training cycles and complementary training material.

The training team will also provide an additional e-learning module for Info Points to support the knowledge transfer to ensure sustainability as they attend the face to face training workshops in order.

A.2.3 Evaluation

This Component will establish adequate mechanisms to provide feedback. These feed-back mechanisms should help answer questions at various levels:

- What is the standard and level of the training and consulting offered, and did this correspond to the needs and specific requirements which had been identified?
- Are all processes, from promotion of trainings to selection of trainees and all training measures delivered, to be considered as successful?
- How satisfied were the participants with the training measures?
- What is the participants' situation after the training?
- To what extent has the training, consultancy and other assistance provided been relevant for the target groups?

- ## 1.1.5 COMPONENT 3: PROJECT MANAGEMENT

A.6.1 Administrative and logistic support to key experts during the duration of the project

The Project team comprises the following,

- Project Director, Ms. Onu expertise in eGovernance and Project Management,
- Project Operations, Mr. Josephe O'flaherty , expertise in Project Management, Engineering and Networking
- Project IT Specialist , Mr. Gavin Newton , Computer Science Specialist
- Project Security Consultant, to be contracted
- Administrative Manager

This team will coordinate Project Staff in assisting experts during the whole duration of the project.

A.6.2 Financial management of the services

Financial management of the contracts is seen as an important aspect requiring adequate organisation and expertise. CCPM Ltd. will ensure :

- the appropriate management of the chart of account in line with the budget breakdown and codification as mentioned in the proposal;
- the use of guidelines for the disbursement, accounting for, reporting, and auditing of the project funds are stipulated in this proposal.
- An accounts clerk and auditor will be assigned to support the financial reporting aspects of the project.

A.6.3 Management of the operational budget and cash flow projections

Mr. O'Flaherty and Ms. Onu will guarantee the management of the operational budget and cash flow.

A.6.4 Quality supervision

The quality assurance of the envisaged project is a horizontal task covering all aspects of the contract. The primary objective of the quality management is to undertake the monitoring of the project and ensure that all the targets set forth are met.

CCPM Ltd. places the utmost importance in the implementation of a Quality Managements System, which will guarantee the uninterrupted and efficient contract completion. The shaping of our approach to quality is based on a number of key principles, which are given below.

- **Proactive approach**. First and foremost, the proactive approach is concerned with CCPM Ltd's team. Its members will be educated and empowered so that they can actively seek opportunities to improve quality, based on early indications for potential problems obtained from the continuous monitoring of the project quality. Our approach will be to seek measures that will solve problems before they even appear.
- **Continuous process improvement**. Quality improvement will be a continuous activity, aiming at having better process effectiveness and efficiency. It will be necessary to constantly evaluate working and management practices, guidelines, modes of operations etc. with a view to improve the resulting quality.
- **Measuring satisfaction**. Satisfaction is the result of a number of positive and negative factors that are experienced by the Beneficiary's users at the receiving end of the project. For a successful service delivery, it is essential that the vast majority of users are highly satisfied. Satisfaction will be assessed in order to obtain quantitative figures that will be used to gauge the effectiveness of the project and how to improve it.
- **Close collaboration with the Beneficiary.** Continuous exchange of information between the Beneficiary and CCPM Ltd. . Participation in all meetings envisaged and preparation of concrete and realistic agendas, proposals and suggestions.

2.4.2 Quality Management System

The success of CCPM Ltd. depends on the quality of every aspect of the project. It is fully recognised that quality does not happen by simple stating its importance but rather by its constant pursue in and through every level of the project activities. It is our view that in order to achieve high quality levels, a Quality Management System and maintaining such an efficient and successful

Quality Management System:

- **Establishment of the quality framework.** The QMS has to be an effective one covering all aspects of the contract. In order to achieve it, support of the project management team is essential.
- **Production of the necessary documentation**. In order to have an effective QMS it is necessary that it is well documented, well understood and followed by the whole project team. The documentation will:
    - Define procedures for all processes and phases;
    - Be available to all team members;
    - Be readily used and understood by all so that everyone knows what is expected from each one;

The description of the (QMS) must be adopted. The system will provide a framework to cover every aspect of the project. For the purposes of the envisaged contract, the following steps are regarded as essential in setting-up

- **procedures.** It will specify how the quality objectives will be met in practice. In this respect, the primary document will be the Project Quality Plan (PQP).

- **Controlling of the development and implementation processes**. The development and implementation processes for the system are at the heart of delivering the project. The essential elements for effective control of that processes are:
    - Planning and definition of the processes;
    - Ensuring that all service elements are identified in the processes to prevent the risk of errors;
    - Planning how to verify that the project meets the user requirements;
    - Planning how to protect the project from quality degradation.
- **Corrective action**. It has to be clearly stated that prevention is better than cure. In this, fixing problems after critical alarms have been raised may have service level degradation implications. For this reason, it is always better to avoid as much as possible having quality defects in the first place. The QMS will be based on the concept that the processes operate in a manner such that arising of quality defects will be prevented in the first place. Of course, when the project level falls below the targets, immediate remedial actions will be undertaken. Once the project level falls below the targets for the same reason, the root cause of the problem will be investigated and a cure will be sought.
- **Maintenance of the quality framework**. During the execution of the contract, the quality framework will evolve to reflect the changing environment in which the project will operate. It will have to adapt in order to continuously meet the needs of the Beneficiary.

1.4 Project Timeline

	1	2	3	4	5	6	7	8	9	10	11	12
COMPONENT 1 : COMMUNICATIONS & INFORMATION NETWORK												
Phase 1: Preparation, Planning and Analysis												
i. Development of National Security Information and Communication Architecture												
o Site Surveys and Mapping												
o Technical, Process and Skill Audits												
ii. Development of Transition and Change Management & Training Plan												
iii. Establishment of Project Steering												
iv. Set up of Project Management Office & Project Management Platform												
v. Procurement												
Phase 2: Infrastructure Design, Development & Establishment of the National Security Network Operations and Control Centre (NSNOCC)												
i. Design interior of Network Operations and Control Centre												
ii. Construction and Installation of Finishing and Furnishing of Network Operations and Control Centre												
iii. Establish Back Up Network Operations and Control Centre and Satellite Centre												
iv. A) Build and implementation of Police HQ Local Area Network (LAN)												
v. B) Build St. Kitts & Nevis Police Districts Wide Area Network (WAN) & VPN												
vi. C) Wireless Mesh Network & Video Surveillance Hardware												
Basseterre												
Cayon, Sandy Point and Charlestown(Nevis)												
Wireless WAN Redudancy												
vii. Digital Radio Conventional System Infrastructure & Radios												
vili. Process Mapping, Reingineering & Central Services Design - – Police Intelligence Information Management System												

Phase 3: National Security Command and Control Platform												
i. Unified VOIP Communications												
ii. Computer Aided Dispatch & 911 Call Management Platform												
iii. Locations Based Map Software & Server												
iv. 911 SMS Software and Management												
v. Central Services Development & Implementation – Police Intelligence Information Management System & Applications												
vi. Deployment of Mobile Terminals In Vehicles, Handhelds and Installation of PC Terminals												
COMPONENT 2 : AWARENESS, SENSITISATION AND TRAINING OF NATIONAL SECURITY PERSONNEL												
Training of National Security Personnel												
COMPONENT 3: PROJECT MANAGEMENT & ADMINISTRATION												
i. Administrative and logistic support to project implementation												
ii. Financial management of the services as described the the Proposal												
iii. Management of the operational budget and cash flow projections												
iv. Quality supervision												
v. Liaise and report to the contracting authority												

Belize Defense Force Headquarters
Communications & Signals Department
Price Barracks, Ladyville
Belize

BELIZE DEFENSE FORCE'S NETWORK PROPOSAL

DRAFT

Submitted by: *Lieutenant Justine J Swift*
Appointment: *Chef Communications Officer*
Submitted to: *Taiwanese Embassy, Belize*
Date of submission: *September, 14th 2011*

PREFACE

This document provides the all the necessary information relating to the current network configuration, disadvantages, as well as the proposed network the Belize Defence Force would like to implement. It also highlights briefly the tactical Military Communications network and infrastructure which may play a vital role in further enhancements.

HANDLING INSTRUCTIONS

This document is the property of the Belize Defence Force intended for official use only to authorized personnel. The information on this document should not be communicated directly or indirectly to the press or any person who is not authorized to receive it.

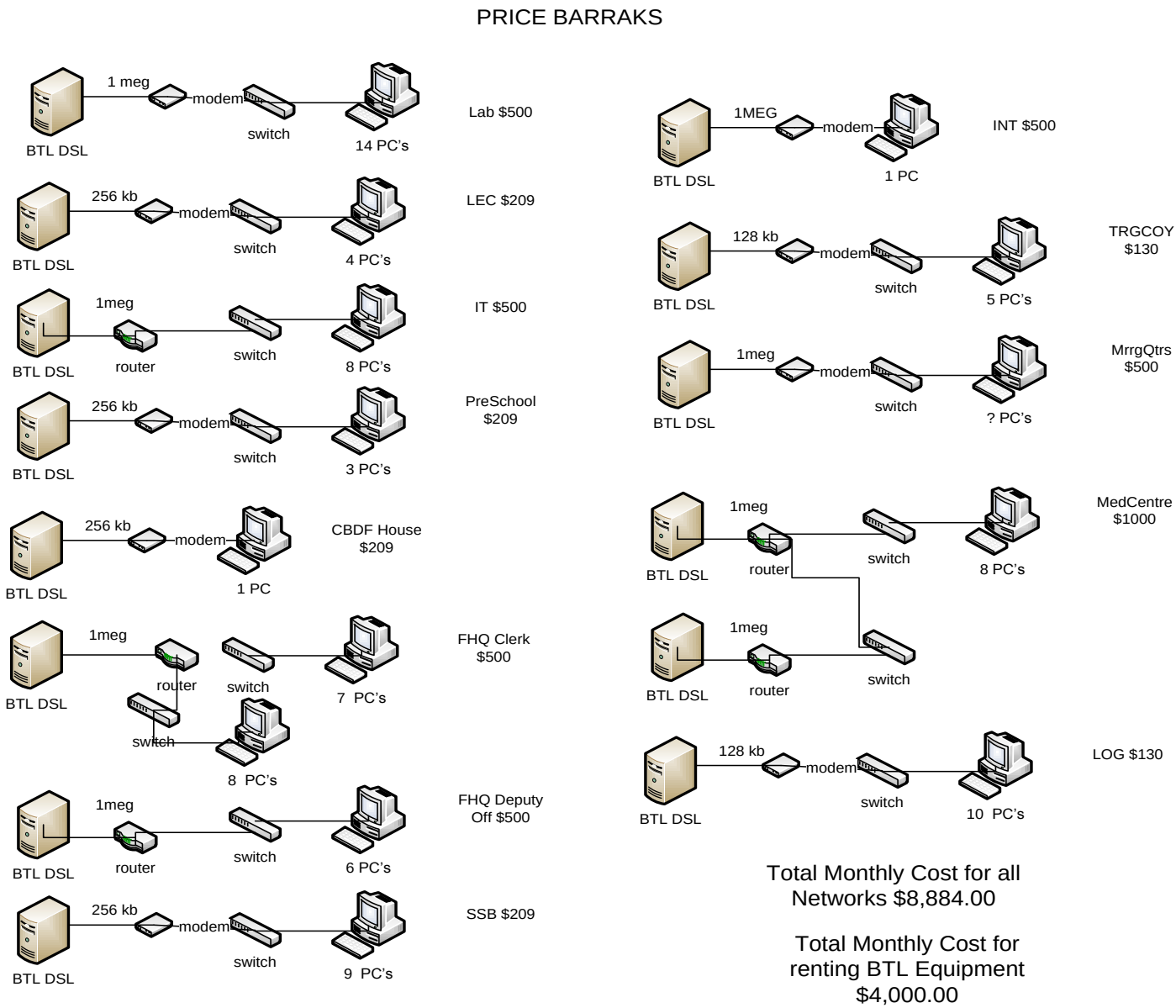
CONTENTS

INTRODUCTION

The national security force of Belize, the BDF should have superior communication capabilities internally and nationally. However the internal communication infrastructure is overcome with flaws from a poorly constructed and outdated Ethernet network which in turn propose limits on Ethernet communication with external forces. This is detrimental to the completion of mission essential task and limits overall productivity. Additionally, there is a communication deadlock; where by the cost and quality of the local phone and internet connections has inversely proportionate relationships. While the bills keep increasing, the quality of the services remains the same. It is imperative that the Belize Defence Force takes immediate action to remedy this dilemma.

CURRENT CONFIGURATION

The Belize Defence Force does not have a centralized network. Below is the current network configuration for Price Barracks, where the Military Headquarters is located.



This is a decentralized network, whereby each building has a separate DSL internet line.

COST BREAKDOWN

High Speed Internet	Speed	Location	Cost
airwing@btl.net	512K	Air Wing Office	$340.00
bdf_edu@btl.net	1M		$600.00
bdfairwing@btl.net	256K	Air Wing Office (OTTIS)	$209.00
bdfairwingops@btl.net	512K	Air Wing Office (CNIES)	$310.00
bdfedu1@btl.net	1M	PB Force Lab	$540.00
bdfengineers@btl.net	256K	PB Lec	$209.00
bdfit@btl.net	1M	PB IT Office	$530.00
_	512K	PB Force Hospital	$330.00
bdfpreschool@btl.net	256K	PB Preschool	$209.00
cayo@btl.net	1M	Cayo Camp Belizario	$610.00
ceo_gillett@btl.net	256K	CBDF House	$179.00
clerk@btl.net	1M	PB IT Office	$610.00
corozalbdf@btl.net	128K	Corozal Drill Hall	$130.00
dangrigabdf@btl.net	128K	Dangriga Drill Hall	$130.00
deputy@btl.net	1M	PB Deputy House	$600.00
deputy1@btl.net	1M	PB Deputy Office	$600.00
eyles@btl.net	256K	Orange Walk Eyle Camp	$209.00
intelligence@btl.net	1M	PB Int Office	$530.00
lccn@btl.net	256K	PB SSB HQ	$209.00
log@btl.net	128K	PB Logistics Coy	$140.00
medcen@btl.net	1M	PB Force Hospital	$610.00
medcen1@btl.net	1M	PB Force Hospital	$500.00
melitia@btl.net	512K	Bze City Militia Hall	$330.00
trgcoy@btl.net	128K	PB Training Coy	$130.00
			$8,794.00

This is the cost breakdown of each individual DSL line and their various speeds.

PHONE EXTENSION SYSTEM

COST BREAKDOWN

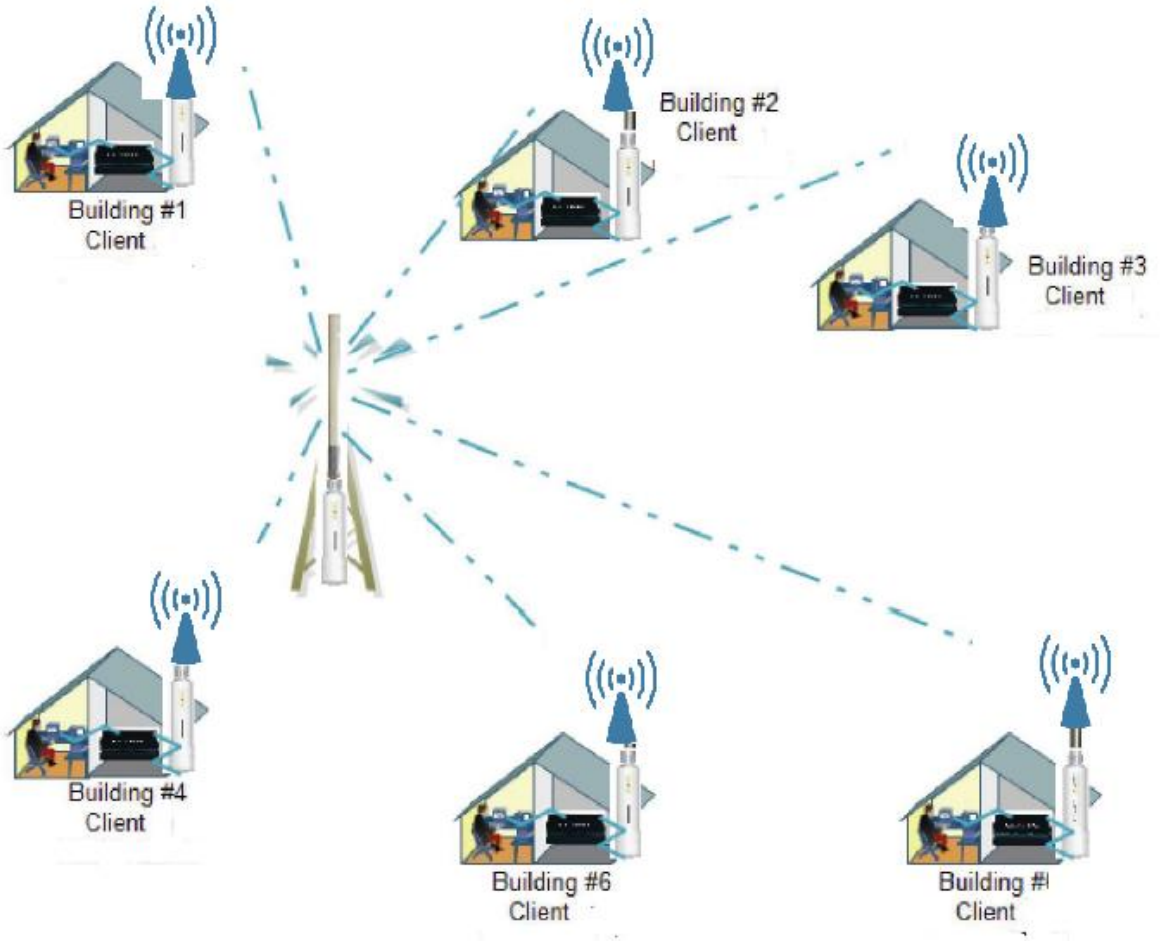
This is the cost break down of phone extension system. All the equipment below is rented from the Belize Telemedia Phone Company.

Customer Premise Equipment	BELL/STINGER90(1)	$20.00
Customer Premise Equipment	CARD/LINE CARD(4)	$300.00
Customer Premise Equipment	EXT/PARA(2)	$11.00
Customer Premise Equipment	EXTN/PARA(1)	$5.00
Customer Premise Equipment	EXTN/SUPERSET(2)	$70.00
Customer Premise Equipment	FRPH/FI125(4)	$28.00
Customer Premise Equipment	HTLN/HOTLINE(1)	$20.00
Customer Premise Equipment	KSU/MER616(1)	$51.00
Customer Premise Equipment	LNCRD/16 SLIC(1)	$40.00
Customer Premise Equipment	OTHER/LINE CARD(2)	$150.00
Customer Premise Equipment	PBX/PAN1232(3)	$522.00
Customer Premise Equipment	PBX/PAN616(3)	$267.00
Customer Premise Equipment	PBX/PAN624(1)	$79.00
Customer Premise Equipment	PBX/PERIPHERAL(1)	$540.00
Customer Premise Equipment	PBX/SX-200(1)	$1,350.00
Customer Premise Equipment	PBX/SX200(1)	$3,190.00
Customer Premise Equipment	PHACC/HEADSET(1)	$10.00
Customer Premise Equipment	PHACC/MIRAGE(1)	$15.00
Customer Premise Equipment	SET/2500(9)	$54.00
Customer Premise Equipment	SET/2500-EXEXT(24)	$543.00
Customer Premise Equipment	SET/2500-EXT(217)	$2,606.00
Customer Premise Equipment	SET/2500-INT(228)	$1,406.00
Customer Premise Equipment	SET/7150-INT(3)	$18.00
Customer Premise Equipment	SET/KXT7731SET(1)	$30.00
Customer Premise Equipment	SET/M7208-INT(57)	$764.00
Customer Premise Equipment	SET/M7310-INT(1)	$21.00
Customer Premise Equipment	SET/M7324-INT(5)	$135.00
Customer Premise Equipment	SET/PAN308-INT(1)	$15.00
Customer Premise Equipment	SET/PAN32-INT(2)	$36.00
Customer Premise Equipment	SET/PAN616-INT(2)	$28.00
Customer Premise Equipment	SET/SUPER 420(9)	$225.00
Customer Premise Equipment	SET/SUPER 430(9)	$225.00
Customer Premise Equipment	SET/SUPERSET(2)	$61.00
Customer Premise Equipment	SET/SUPERSETS(1)	$10.00
Customer Premise Equipment	UPS/500(4)	$177.00
Customer Premise Equipment	UPS/SP1200(1)	$60.00
Customer Premise Equipment	UPS/SP400(2)	$90.00
	Total Service Bill	**$13,172.00**

Ideally we would like to eliminate this cost with the VOIP system.

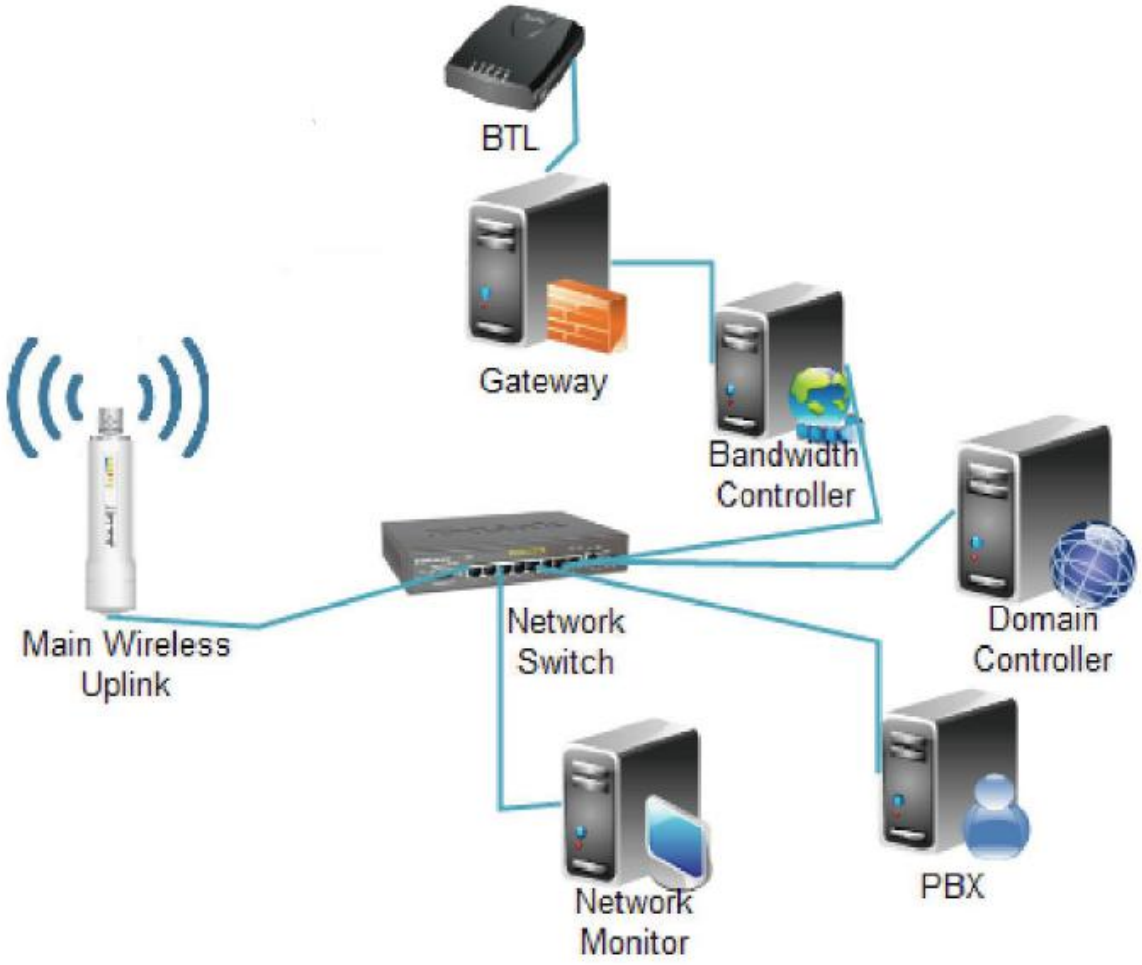
PROPOSED NETWORK

Below is a diagram of the overall picture of the proposed network.



This is a centralized wireless network, with one main internet DSL line. This will eliminate the need for all the individual DSL lines.

Internal Network



This is the internal framework of the proposed network. Our current network does not have any internal servers to manage the network.

VOIP setup

This is the VOIP system which may very well replace our current phone extension system and eliminate the cost of renting all those equipment from the Belize Telemedia Phone Company.

COST BENEFIT ANALYSIS

Internet

Cost	Monthly	Yearly
Current Network	**$ 12,884.00**	**$ 154,608.00**
New Network	**$ 3,500.00**	**$ 42,000.00**
Savings	**$ 9,384.00**	**$ 112,608.00**

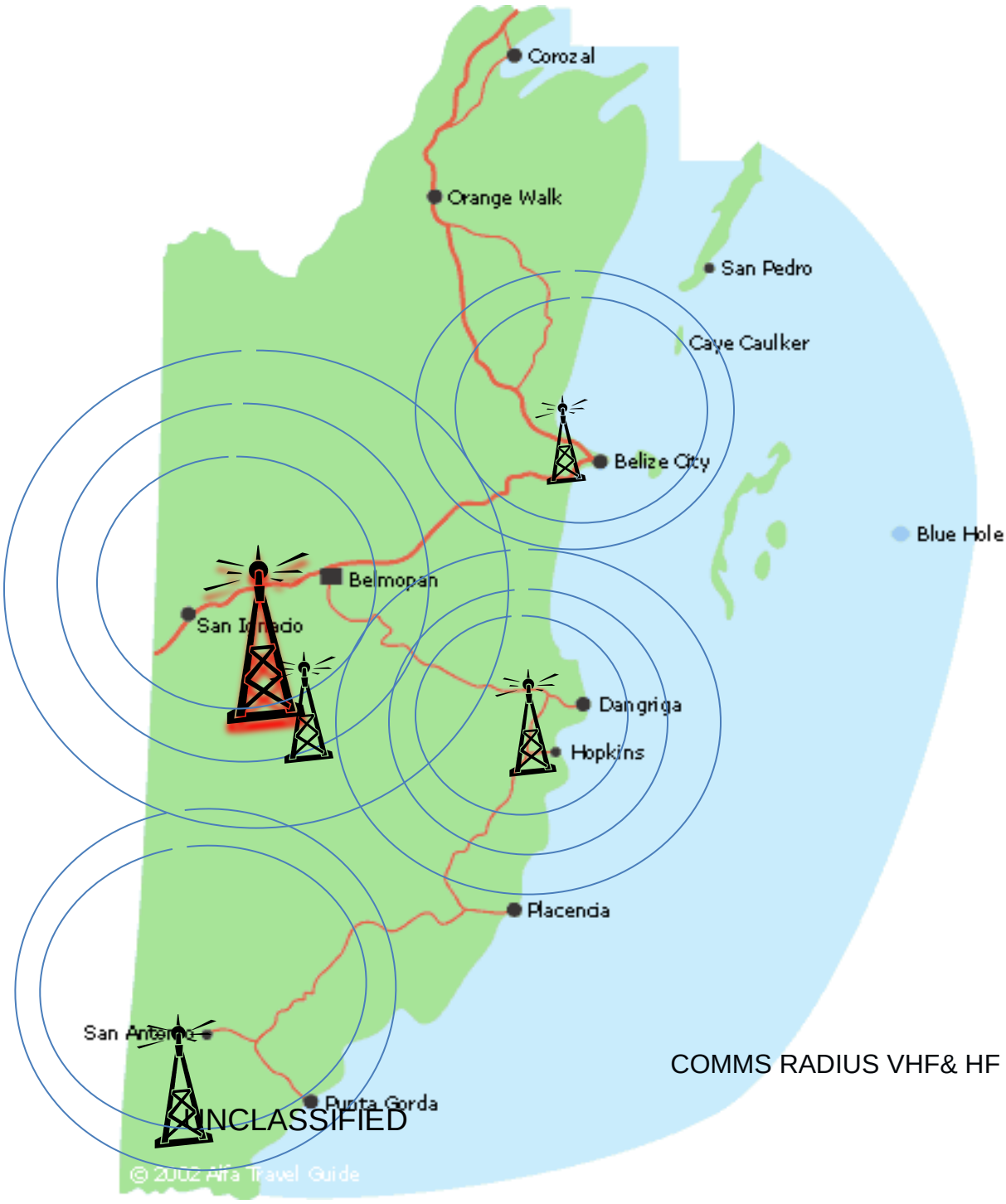
Currently we spend over twelve thousand dollars on the present network. This is due to the individual DSL lines for every office and the various cost of renting the equipment. With the new network, we would only need one DSL line for the ISP

Phone

Cost	Monthly	Yearly
Current Network	**$ 13,172.00**	**$ 158,064.00**
New Network	**$ 0**	**$ 0**
Savings	**$ 13,172.00**	**$ 158,064.00**

The entire extension system for the Military is provided by the Belize Telemedia Phone Company at a cost of over thirteen thousand monthly. Using the VOIP system, there would be no need for the system we presently have.

TACTICAL NETWORK INFRASTRUCTURE



This is our tactical communication network. With both VHF and HF military radios, we are able to communicate for one end of the country to the other.

Each tower in the diagram is over 100ft tall. Eventually we would like to combine both our tactical and operational network to share and transfer voice and data at all the different military installations throughout the country and be independent of the various ISP's.

PHASES OF IMPLEMENTATION

Phase I

- Provide the necessary training for the team responsible to monitor, manage and maintain the Network. This includes the basic Information Technology and Network skills needed to keep the network fully operational

Phase II

- Proposed Network implementation at Price Barracks Ladyville. This includes the implementation of the centralized network architecture consisting of VOIP to replace the current phone extension system. This will be an intranet managed by the respective servers.

Phase III

- New Network implantation at Camp Belizario Cayo

Phase IV

- New Network implantation at Camp Fairweather, Punta Gorda

Phase V

- New Network implantation at Elyse Camp, Orange Walk

Phase VI

- New Network implantation at Militia Hall, Belize City

Phase VII

- New Network implantation at Drill Hall, Stann Creek

Phase VIII

- Combination of tactical and operational network. This is to use the Tactical infrastructure already in place throughout the country to enhance our operational network (operational network consist of the internet and phone systems to exchange information). This includes interconnecting all the military camps throughout the country to form one large. This will allow the secure transfer of voice and data and other forms of media over countrywide intranet.

Phase IX

- ❖ Interconnecting the OP's (Observational Positions) throughout the country with the rest of the network. This includes linking our tactical communication with non-tactical communications. Using the RF 6010 features on the Falcon II HF radios both forms of communication can be linked. This allows the HF radio to be linked to the phone extension system.

CONCLUSION

This proposed network will play a major role in further technological advancements in the BDF. For instance, the way information is stored and managed; this plays a key role in accountability of everything within the military. It provides additional security of all assets, for example, inexpensive wireless security cameras that can also be attached to the network to monitor activity throughout all the camps as well as OP's. This also creates more command and control of operations and makes the job a lot easier and efficient. At Price Barracks Camp in Ladyville the person working the operations room will have real-time surveillance of what's happening in all the other camps. Another key feature is the use of teleconferencing, which would mean that Commanding Officers won't have to leave there camps to see the boss, they will be able to communicate simultaneously via teleconferencing thus saving a vital commodity, fuel.