代號：10960
頁次：2－1

112年公務人員特種考試司法人員、法務部調查局調查人員、海岸巡防人員、移民行政人員考試及112年未具擬任職務任用資格者取得法官遴選資格考試試題

考 試 別：司法人員
等　　別：三等考試
類 科 組：檢察事務官電子資訊組
科　　目：資通安全
考試時間：2 小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、隨著 5G 時代的來臨，其所用的網路架構為軟體定義網路（Software Defined Networking, SDN），針對其網路架構及其可能遇到的威脅，請回答下列問題：
㈠請詳述軟體定義網路。（4 分）
㈡請畫圖並詳述 SDN 網路架構。（12 分）
㈢請詳述 SDN 網路各階層所面臨的威脅。（12 分）

二、依據「國家資通安全發展方案（110 年至 113 年）」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任架構資安防護環境，推動政府機關導入零信任架構，以完善政府網際服務網防禦深廣度。我國政府零信任架構係參考 NIST 零信任架構，同時結合向上集中之防護需求，採取資源門戶之部署方式。請列出並詳述此部署方式之三大核心機制。（24 分）

三、學者 Pipkin 指出資安事故指標為有可能、極有可能、明確等三種不同類別，用以檢查某個事件是否成為一個可能的事故或稱為嫌疑事故（Incident Candidate），請回答下列問題：（每小題 12 分，共 24 分）
㈠依據資訊安全原則，請列出至少三項並詳述如何確認發生真實資安事故。
㈡當真實資安事故發生時，資訊安全相關人員必須立刻啟動應對的事故回應計畫（Incident Response Plan）。請列出至少四項事故處理應該採取的行動並詳述之。

四、為防範各種不同的網路弱點及達到資安通報的機制，請回答下列問題：（每小題 12 分，共 24 分）

㈠請詳述 CVE（Common Vulnerabilities and Exposures）、NVD（National Vulnerability Database）及 CPE（Common Platform Enumeration）之意義為何？並說明 CVE、NVD 及 CPE 彼此之間的運作情形。

㈡請詳述資通安全弱點通報機制（Vulnerability Alert and Notification System）及其運作方法。