

數位發展部資通安全署 函

地址：100235臺北市中正區北平東路2號
聯絡人：莊馥羽
電話：(02)23808500分機8733
電子郵件：yuyu422924@acs.gov.tw

受文者：教育部

發文日期：中華民國115年9月18日
發文字號：資安輔導字第1153000879號
速別：普通件
密等及解密條件或保密期限：
附件：如說明 (3000879_附件-各機關基於風險導向之弱點處置期限評估指引草案.pdf)

主旨：本署擬定「各機關基於風險導向之弱點處置期限評估指引」草案，請資通安全責任等級B級以上之公務機關及特定非公務機關，於115年9月30日前惠示卓見，請查照。

說明：

- 一、公務機關與特定非公務機關依《資通安全責任等級分級辦法》應辦事項規定，知悉資通安全弱點時，應適時修補或採行緩解措施。
- 二、因應AI快速發展導致自動化攻擊與弱點武器化加速之趨勢，並參考國際新版弱點管理規範（如美國CISA BOD 26-04文件），特訂定旨揭指引（如附件），協助各機關採取基於風險導向之弱點處置策略，落實資通安全弱點管理，以提升整體資通安全防護能力。
- 三、旨揭指引草案重點說明如下：
 - （一）評估指標與流程：提供弱點處置期限評估指標及作業流程，協助機關據以判定資訊資產弱點處置時限。
 - （二）弱點處置範疇：包含執行安全性更新、關閉有弱點的服



務或功能、停用資訊資產、進行網路隔離，或其他為降低風險至機關可接受程度所採行的各項弱點緩解或補償性控制措施。

(三)內部程序與例外管理：各機關應訂定弱點處置之內部評估程序，其中弱點處置期限原則應依指引所訂評估流程定之；如有例外情形，得依相關個案情形衡酌營運衝擊，經資訊（安）主管核准後自訂處置期限，並留存紀錄備查。

四、草案修正意見，請免備文逕以線上表單回復（網址：

<https://s.moda.gov.tw/3toQnlakibWY>，以利研議修正。

正本：總統府第二局、國家安全會議秘書處、行政院資訊處、司法院資訊處、立法院資訊處、考試院資訊處、監察院綜合業務處、行政院各部會行總處、本部資訊處、各直轄市政府、各縣（市）政府

副本：

