73.54數位計算機及通訊系統與網路防護

2009年11月23日前，授權運作一個核能電廠的每一個持照者，針對委員會的審查及核准，將提交一份資通安全計畫（如本章50.4與50.90所規範），滿足本節所描述要求。每一份提交必須包含一個實施期程。持照者的資通安全計畫的實施必須與核准的期程相符。持照者的資通安全程序的實施必須與核准的期程一致。針對運轉合約或在此規定的有效日之前已提交至委員會的聯合合約，申請者必須修正申請，需包含與本節符合之資通安全計畫。

1. 每個接受本節所規範需求的持照者應提供高度確保，使數位電腦、通訊系統、與網路適當地受到保護，抵抗資通攻擊，包括描述於73.1捷的設計基準威脅。
2. 持照者應保護以下相關之數位電腦、通訊系統、及網路
3. 安全相關及對安全性重要之功能；
4. 安全功能；
5. 緊急應變功能，包含離線通訊；
6. 支援系統及裝置，如遭受損害將對安全、保安、或緊急應變功能不利衝擊。
7. 持照者應保護(a)(1)節提到的系統及網路免於資通攻擊，造成
8. 資料及（/或）軟體的完整性或機敏性負面衝擊；
9. 系統、服務、及(/或)資料否定操作（存取）；以及
10. 系統、網路、及相關裝置的負面衝擊。
11. 為要完成此目的，持照者應
12. 分析數位電腦、通訊系統、及網路，以及辨識資產，必須被保護抵抗資通攻擊以便滿足(a)所述，
13. 建立、實施、維護資通安全程序以保護(b)(1)所辨識出的資產；及
14. 整合資通安全程序成為實體安全程序的一部分。
15. 資通安全程序必須設計用於：
16. 實施安全管控以保護(b)(1)所辨識出的資產免於資通攻擊
17. 應用及維護深度防禦之防護策略以確保偵測資通攻擊、回應資通攻擊、恢復資通攻擊之能力
18. 減緩資通攻擊之負面效果；及
19. 確保(b)(1)所描述辨識出的保護資產不受資通攻擊造成的負面衝擊。
20. 作為資通安全程序的部份，持照者應：
21. 確保適當的設施人員，包括合約商，了解資通安全需求及接受必要訓練以執行設計的任務與責任。
22. 評估與管理資通風險。
23. 確保由(b)(1)所辨識出的資產實施變動前被評估以確保保持(a)(1)所制定的資通安全效能目標
24. 執行資通安全事件通知與73.77一致。
25. 持照者應建立、實施、維護資通安全計畫，實施本節所述之資通安全程序需求。
26. 資通安全程序必須描述本節所述之需求將如何被實現及必須說明影響實施的特殊場域條件。
27. 資通安全計畫必須包含安全事件反應與資通攻擊回覆的評量。資通安全計畫必須描述持照者將如何：
28. 維持即時偵測與反應資通攻擊的能力；
29. 減輕資通攻擊的後果；
30. 修正明顯的弱點；及
31. 復原受資通攻擊影響的系統、網路、及(/或)裝置。
32. 持照者應發展及維持書面策略與實施流程以執行資通安全計畫。持照者運用之策略、實施流程、特定場域分析、及其他的支援技術資訊不需要提交作為委員會審查與核准，但應定期接受NRC人員的檢查。
33. 持照者應審查資通安全程序，作為實體安全程序一部分，與73.55(m)所述的需求一致，包括週期需求。
34. 持照者應保持所有記錄與支援技術文件以滿足本章需求，作為記錄直到委員會終止執照，以及應維護這些記錄的替代部分，在取代後至少3年，除非由委員會另訂之。

[74 FR 13970, Mar. 27, 2009; 80 FR 67275, Nov. 2, 2015]

文件最新修正日期，2015年12月2日星期三。