

Allocation of Information Security Requirements to Security Enclaves Based on System Risk and Criticality – Moderate Risk

| Moderate Risk Protection Profile Requirement | WAN | LAN/ Facility Comm. | Application System |
|--|--------------------------------------|--------------------------------------|--|
| <p>3.8.5.A All NAS systems shall provide the required level of security functionality and security integrity based upon vulnerability, threat, and risk analyses. The threat analysis, risk analysis, and risk mitigation priority are documented in Section 3 of a Protection Profile and Security Target. This information is used to determine the security objectives stated in Section 4 and the security functional requirements, security assurance requirements, and evaluation assurance level specified in Section 5.</p> | X | X | X |
| <p>3.8.5.B All NAS systems shall provide the required level of security training based upon the vulnerability, threat, and risk analyses.</p> <p>ADO_DEL.1 Delivery procedures</p> <p>ADO_IGS.1 Installation, generation, and start-up procedures</p> <p>AGD_ADM.1 Administrator guidance</p> <p>AGD_USR.1 User guidance</p> | X | X | X X |
| <p>3.8.5.C All NAS systems shall be protected from threats to compromise integrity.</p> <p>FDP_DAU.1 Basic data authentication</p> <p>FDP_ROL.1 Basic rollback</p> <p>FDP.SDI.2 Stored data integrity monitoring and action</p> <p>FDP_UIT.1 Data exchange integrity</p> <p>FPT_AMT.1 Abstract machine testing</p> <p>FPT_FLS.1 Failure with preservation of secure state</p> <p>FPT_ITI.2 Inter-TSF detection and correction of modification</p> | X X X X | X X X X | X X X X |

| Moderate Risk Protection Profile Requirement | WAN | LAN/ Facility Comm. | Application System |
|--|---|---|---|
| FPT_ITT.2 TSF data transfer separation | X | X | X |
| FPT_PHP.2 Notification of physical attack | X | X | X |
| FPT_PHP.3 Resistance to physical attack | X | X | X |
| FPT_RPL.1 Replay detection | X | X | X |
| FPT_SSP.1 Simple trusted acknowledgement | X | X | |
| FPT_TDC.1 Inter-TSF data consistency | | | X |
| FPT_TRC.1 Internal TSF consistency | | | X |
| FPT_TST.1 TSF testing | X | X | X |
| 3.8.5.D All NAS systems shall be protected from threats to compromise availability . FPT_ITA.1 Inter-TSF availability FRU_FLT.2 Limited fault tolerance FRU_PRS.2 Full priority of service FRU_RSA.1 Maximum quotas | X X X X | X X X X | X X X |
| 3.8.5.E All NAS systems shall provide access control . FDP_ACC.2 Complete access control FDP_ACF.1 Security attribute based access control FDP_ETC.1 Export of user data without security attributes FDP_IFC.1 Subset information flow control FDP_IFF.1 | X X X X X | X X X X X | X X X X X |

| Moderate Risk Protection Profile Requirement | WAN | LAN/ Facility Comm. | Application System |
|--|---|--|--|
| <p>All NAS systems shall provide for information confidentiality based upon the result of a security assessment.</p> <p>FCS_CKM.1 Key generation</p> <p>FCS_CKM.2 Key distribution</p> <p>FCS_CKM.3 Key access</p> <p>FCS_CKM.4 Key destruction</p> <p>FCS_COP.1 Cryptographic operation</p> <p>FDP_RIP.2 Full residual information protection</p> <p>FDP_UCT.1 Basic data exchange confidentiality</p> <p>FPR_ANO.1 Anonymity</p> <p>FPR_PSE.1 Pseudonymity</p> <p>FPT_ITC.1 Inter-TSF confidentiality during transmission</p> <p>FPT_ITT.2 TSF data transfer separation</p> | <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p></p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> | <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p></p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> | <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p></p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> |
| <p>3.8.5.H NAS systems shall implement identification and authentication at a level based upon a security assessment, and non-repudiation when appropriate.</p> <p>FCO_NRO.1 Selective proof of origin</p> <p>FCO_NRR.1 Selective proof of receipt</p> <p>FIA_AFL.1 Authentication failure handling</p> <p>FIA_ATD.1 User attribute definition</p> <p>FIA_SOS.1 Verification of secrets</p> | <p></p> <p></p> <p></p> <p>X</p> <p>X</p> <p>X</p> | <p></p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> | <p></p> <p></p> <p></p> <p>X</p> <p>X</p> <p>X</p> |

| Moderate Risk Protection Profile Requirement | WAN | LAN/ Facility Comm. | Application System |
|--|-----|---------------------------|-----------------------|
| FIA_SOS.2 Generation of secrets | X | X | X |
| FIA_UAU.2 User authentication before any action | X | X | X |
| FIA_UAU.3 Unforgeable authentication | X | X | X |
| FIA_UAU.4 Single-use authentication mechanisms | X | X | X |
| FIA_UAU.5 Multiple authentication mechanisms | X | X | X |
| FIA_UAU.6 Re-authenticating | X | X | X |
| FIA_UAU.7 Protected authentication feedback | X | X | X |
| FIA_UID.2 User identification before any action | X | X | X |
| FIA_USB.1 User-subject binding | | X | X |
| FTP_ITC.1 Inter-TSF trusted channel | X | X | |
| FTP_TRP.1 Trusted path | X | X | |
| 3.8.5.I All NAS systems shall provide recovery measures from security incidents. | | | |
| FDP_UIT.3 Destination data exchange recovery | X | X | X |
| FPT_RCV.3 Automated recovery without undue loss | X | X | X |
| FPT_RCV.4 Function recovery | X | X | X |
| 3.8.5.J All NAS systems shall provide the capability to centrally manage security functions. | | | |
| FMT_MOF.1 Management of security functions behavior | X | X | X |
| FMT_MSA.1 Management of security attributes | X | X | X |

| Moderate Risk Protection Profile Requirement | WAN | LAN/ Facility Comm. | Application System |
|---|-----|---------------------------|-----------------------|
| FMT_MSA.2 Secure security attributes | X | X | X |
| FMT_MSA.3 Static attribute initialization | X | X | X |
| FMT_MTD.1 Management of TSF data | X | X | X |
| FMT_MTD.2 Management of limits on TSF data | X | X | X |
| FMT_MTD.3 Secure TSF data | X | X | X |
| FMT_REV.1 Revocation | X | X | X |
| FMT_SAE.1 Time-limited authorization | X | X | X |
| FMT_SMR.1 Security roles | X | X | X |
| FTA_LSA.1 Limitation on scope of selectable attributes | | | X |
| FTA_MCS.1 Basic limitation on multiple concurrent sessions | | | X |
| FTA_SSL.1 TSF-initiated session locking | | | X |
| FTA_SSL.3 TSF-initiated termination | | | X |
| FTA_TAB.1 Default TOE access banners | | | X |
| FTA_TSE.1 TOE session establishment | | | X |