## APPENDIX D. FEDRAMP+ SECURITY CONTROLS AND PARAMETER VALUES

Table D-1 lists the required FedRAMP+ security controls (NIST 800-53 Rev 5) parameter values and the FedRAMP security control for which DOD requires adjustment. Refer to Sections 3.4 and 3.5 for further information. These security controls and associated parameter values are published here as a benchmark for CSPs and will be used for CSP assessment toward receiving a PA. **It is not a complete list of all security controls that a CSP must meet**.

For Impact Level 5, National Security Systems will require the additional CNSSI 1253 controls for those systems. The parameters will be the DOD RMF TAG value (DSPAV, DOD Specific Assignment Value), CNSSI 1253 value if no DOD RMF TAG value exists, or AO tailored value unless designated by this document. Refer to the DOD RMF website at https://rmfks.osd.mil/.

For Impact Level 6, the application of the CNSSI 1253 Classified Information Overlay will modify some of the values of security control presented below as well as other security controls not listed. Overlay values take precidence.

DOD Componets/Mission Owners must use, define, and/or tailor the parameter values for the applications they instantiate in IaaS/PaaS cloud services in accordance with the values defined by the DOD RMF TAG. DOD/FedRAMP predefined and CSP-defined parameter values assessed for DOD PA award are inherited by the Mission Owners' systems/applications. If the Mission Owner needs alternate values for these inherited values, they must be negotiated with the CSP and reflect the change in their SLA/contract.

In addition to parameter values required for the implementation of FedRAMP+ security controls, Table D-1 contains security controls where the value is nonexistent or requires adjustment. The controls listed that are part of the FedRAMP baseline must use the value listed in the table.

**Table D-1: FedRAMP+ Additions/Adjustments to Parameter Values for FedRAMP+ Security Controls/Enhancements**

| Control | Parameter Values | Impact Level |
|---|---|---|
| AC-7 | For privileged users, DOD required an account lock after three unsuccessful attempts for Impact Levels 2/4/5 and after five unsuccessful attempts for accounts using a SIPR token. All levels must be configured to require an administrator unlock the account. For nonprivileged users, if rate limiting, DOD will allow 10 attempts with the account automatically unlocked after 30 minutes. If rate limiting is not used, normal DSPAV will be required. | IL4, IL5, IL6 |
| AU-5(1) | CSP/CSO may use FedRAMP value. | IL4, IL5, IL6 |
| CM-7(5) | DSPAV must be used. | IL4, IL5, IL6 |
| IA-5(1) | DSPAV must be used. | IL4, IL5, IL6 |
| PE-15 | DSPAV must be used. | IL4, IL5, IL6 |
| PS-3(4) | All information systems.<br>Users: U.S. citizens, U.S. nationals, or U.S. persons, foreign personnel as allowed by current DOD polices with AO approval. | IL4, IL5, IL6 |

| Control | Parameter Values | Impact Level |
|---|---|---|
| | Administrators: U.S. citizens, U.S. nationals, or U.S. persons. Refer to Section 5.5.2, CSP Personnel Requirements, for more information. | |
| MA-5(1) | DSPAV must be used. | IL4 |
| MA-5(2) | | IL6 |
| MA-5(3) | | IL6 |
| MA-5(4) | | IL6 |
| MA-5(5) | | IL4, IL5, IL6 |
| MA-6 | CSP/CSO may use FedRAMP value. | IL4, IL5, IL6 |
| PS-4 | CSP/CSO may use FedRAMP value. | IL4, IL5, IL6 |
| SA-4(5) | DSPAV must be used. | IL4, IL5, IL6 |
| SA-9(1) | DSPAV must be used. | IL4, IL5, IL6 |
| SA-9(3) | DSPAV must be used. | IL4, IL5, IL6 |
| SA-9(5) | SA-9 (5)-1 [information processing, information or data, AND system services].<br>SA-9 (5)-2 [U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction].<br>SA-9 (5)-3 [all data, systems, or services]. | IL4, IL5, IL6 |
| SA-9(6) | | IL4, IL5, IL6 |
| SA-9(7) | | IL4, IL5, IL6 |
| SA-9(8) | | IL4, IL5, IL6 |
| SC-12(6) | | IL4, IL5, IL6 |
| SC-17 | DODI 8520.02, Public Key Infrastructure (PKI) and Public Key Enabling (PKE). | IL4, IL5, IL6 |
| SC-18 | | IL4, IL5, IL6 |
| SC-18 (2) | DSPAV must be used. | IL4, IL5, IL6 |
| SC-18 (3) | Supplemental guidance:<br>For the protection of the infrastructure supporting a CSO, CSPs are required to apply this control to their organizational IT systems and the infrastructure supporting their CSO(s).<br>For the protection of Mission Owners, their end users, and networks, CSP CSOs must not support the downloading of mobile code, which is deemed unacceptable to DOD.<br>Refer to Section 5.11, Mobile Code, for more information. | IL5, IL6 |
| SC-18 (4) | Software applications such as but not limited to email, scriptable document/file editing applications that support documents with embedded code (e.g., Microsoft Office applications/documents), etc.<br>Prompting the user for permission. | IL5, IL6 |
| SC-24 | DSPAV must be used. | IL4, IL5, IL6 |
| SC-46 | DSPAV must be used. | If CDS is used |