# MLB SERVICE GROUP • SYSTEM SECURITY PLAN (SSP)

NIST SP 800-171 Revision 3 Master Control Alignment Matrix

**SPRS SCORE: 110 / 110**

Boundary: Single-User Workstation (Brent Barnard)

| CONTROL ID | REQUIREMENT NAME | STATUS | OPERATIONAL IMPLEMENTATION & EVIDENCE VERIFICATION SUMMARY |
|---|---|---|---|
| **3.1 Access Control & Account Management** | | | |
| **3.1.3** | Information Flow Control | **Implemented** | CUI restricted strictly to single workstation. Encrypted flow to government systems (**PIEE/SPRS**) via TLS/HTTPS. No public routing. |
| **3.1.4 / .5** | Separation of Duties / Least Privilege | **Implemented** | Sole-operator accountability (**Brent Barnard**). Standard user profiles utilized daily; admin credentials restricted for maintenance. |
| **3.1.6 / .10** | Inactivity Screen & Session Locks | **Implemented** | Workstation locks automatically after period of inactivity. Re-authentication via secure PIN/biometrics mandatory. |
| **3.1.7 / .11** | Login Lockout & Session Term. | **Implemented** | Account lockout triggers automatically after 5 failed attempts. Total session termination enforced after 30 minutes of inactivity. |
| **3.1.8 / .9** | Display Privacy & Login Banner | **Implemented** | Workstation angled away from public view. System access presents a legal authorization warning banner prior to login profile entry. |
| **3.1.12 / .16** | Remote Access / Wireless Security | **Implemented** | Remote desktop capabilities completely disabled. Local wireless environment secured via high-entropy **WPA2-PSK** passphrase. |
| **3.1.18 / .20** | Mobile Devices & Portal Access | **Implemented** | Workstation restricted to family residences. View-only exception for emergency mobile access via secured Technical Director phone. |
| **3.3 Audit and Accountability** | | | |
| **3.3.1 / .2** | Log Generation & User Traceability | **Implemented** | Native OS logs + **Bitdefender** capture logon events, admin rights, and alerts. Traceable to unique username profile; retained 1 year. |
| **3.3.3 / .4** | Audit Review & Failure Response | **Implemented** | Manual log reviews performed monthly. System generates immediate on-screen warnings if storage limits or logging failures occur. |
| **3.3.5 / .6** | Time Correlation & Log Protection | **Implemented** | System clock synchronized with internet authoritative NTP server. Audit tracks locked by kernel to prevent unauthorized modification. |
| **3.4 Configuration Management** | | | |
| **3.4.1 / .2** | Baseline Config & Change Log | **Implemented** | Documented secure configuration state baseline. All modifications evaluated and tracked by the Technical Director in Appendix E. |
| **3.4.3 / .6** | Least Functionality Hardening | **Implemented** | Unnecessary software, games, background services, and legacy protocols completely uninstalled. Firewalls block all unapproved ports. |
| **3.4.4 / .8** | Restricted Software Enforcement | **Implemented** | Standard profiles blocked from installers. "Allow-by-exception" architecture locks environment to Microsoft, Browsers, and Bitdefender. |
| **3.4.10 / .11** | Component Inventory & Locations | **Implemented** | Master hardware and software asset log maintained. Spatial footprint mapped; CUI local storage strictly forbidden on mobile interfaces. |
| **3.5 - 3.16 Core Safeguards (MFA, Incident Handling, Local Media, Air-Gaps, Custom Code)** | | | |
| **3.5.3 / .12** | Multi-Factor & Authenticator Mgmt | **Implemented** | MFA enforced for all environments; token challenges generated locally via the offline mobile **2FAS application**. |
| **3.6.1 / .5** | Incident Response Plan Testing | **Implemented** | Contains automated alert containment protocols and a mandatory 72-hour government reporting loop. Validated through annual tabletop text exercises. |
| **3.8.3 / .9** | Media Protection & Air-Gapped Backups | **Implemented** | Zero-Cloud Storage Mandate. Backups isolated on local external hard drives, fully air-gapped from network infrastructure after sync. |
| **3.9.1 / 3.10** | Personnel Vetting & Physical Perimeter | **Implemented** | Operator holds federal FAA A&P tracking credentials. Workstation housed behind heavy physical perimeters and locked entry access layouts. |
| **3.14.2 / .6** | Malicious Code & System Monitor | **Implemented** | **Bitdefender Real-Time Guard** continuously parses memory, scans incoming assets, forces definitions daily, and intercepts web traffic. |
| **3.16.1** | Systems Security Engineering | **Implemented** | Avoids vulnerable content management platforms and heavy extensions. Web presence built manually using clean, raw **HTML and CSS**. |
| **3.17 Supply Chain Risk Management** | | | |
| **3.17.1** | Supply Chain Risk Plan | **Implemented** | Strict procurement controls. Equipment sourced solely from authorized OEM channels. No open-box components or third-party sellers. |
| **3.17.2** | Secure Acquisition Methods | **Implemented** | All installations downloaded via cryptographically signed HTTPS pages. Compulsory Bitdefender executable signature scans run before install. |
| **3.17.3** | Supply Chain Flowdown Processes | **Implemented** | Mandatory down-flow clauses require external affiliates or specialty suppliers to meet identical data handling and immediate breach notice rules. |