Web System Security Plan (WSSP-v1.0)

# Eagle Defense Systems, LLC

For SaaS Deployment: www.eagledefensesys.tech

Date: June 2025

Version: v1.0

Author: Eagle Defense Systems Security Office

## 1. System Identification

|  |  |
| --- | --- |
| System Name | Eagle Defense Systems SaaS Platform |
| Primary Domain | www.eagledefensesys.tech |
| Hosting Provider | Vercel |
| Registrar | Google Domains (via Google Workspace) |
| DNS Hosting | Google Cloud DNS |
| Repository | GitHub (securedbyjc organization) |
| SSP Version | v1.0 |
| Date | June 2025 |
| Author | Eagle Defense Systems Security Office |

## 2. System Description

Eagle Defense Systems (EDS) operates a SaaS web platform hosted on Vercel. The platform provides security consulting, client engagement intake, and internal research tools (LexSentinel AI, SwiftEagle AI). The SaaS environment is governed by security controls aligned to CMMC, NIST SP 800-171, FedRAMP Low, and GovCon SaaS best practices.

## 3. System Boundary Diagram

- SaaS Layer: Vercel deployment environment  
- CI/CD Layer: GitHub (branch protection + MFA)  
- Registrar Layer: Google Domains (MFA)  
- DNS Layer: Google Cloud DNS (secured)  
- IAM Layer: Google Workspace, GitHub, Vercel Teams  
- DevOps Artifacts: Secure repository access only

## 4. Security Controls Implemented

|  |  |  |
| --- | --- | --- |
| Control Family | Control | Status |
| Access Control | MFA enabled (all platforms) | Implemented |
| Configuration Management | next.config.js security headers | Implemented |
| System Integrity | Branch Protection Rules | Implemented |
| Communications Protection | TLS 1.3 only | Implemented |
| Deployment Security | Deployment Protection via Vercel | Implemented |
| Secure Headers | CSP, HSTS, X-Frame, Permissions Policy | Implemented |
| Secret Management | Encrypted Vercel environment variables | Implemented |
| Code Security | Dependabot enabled on GitHub | Implemented |
| Compliance Mapping | Phase 1 compliance mapping initiated | In Progress |

## 5. IAM Policy Summary

- GitHub: MFA enforced, role-based access controls.  
- Vercel: Deployment Protection enabled, MFA enforced.  
- Google Workspace: Admin MFA enforced, global 2FA policy.  
- DNS Registrar: MFA enabled, registrar lock engaged.

## 6. Backup and Recovery

- Codebase fully versioned within private GitHub repositories.  
- Vercel deployment rollback enabled for disaster recovery.  
- Local encrypted backups maintained for strategic code archives.

## 7. Change Management Process

- Code changes require pull request submission.  
- All pull requests require peer review and approval.  
- Deployment occurs only after successful PR merges and CI/CD validation.

## 8. Monitoring & Logging

- Vercel deployment logs retained.  
- GitHub repository logs and audit trails preserved.  
- Google Workspace Admin logs enabled for account activity monitoring.

## 9. Planned Enhancements (Phase 2)

- WAF integration via Cloudflare Zero Trust or GCP Armor.  
- Third-party SaaS security scanning.  
- Expanded compliance mapping (CMMC Level 2 & FedRAMP prep).  
- Insider Threat Monitoring and AI Security Modules.  
- System Audit Log Aggregation for centralized monitoring.

## 10. Approval

|  |  |  |
| --- | --- | --- |
| Role | Name | Date |
| Security Officer | Jeffrey Collins | June 2025 |
| Compliance Officer | — | TBD |
| Executive Officer | — | TBD |