**White Paper: Cybersecurity and Compliance**

Frameworks, Threat Modeling, and Accessibility in Federal Digital Services (VA Context)

White Paper: Cybersecurity and Compliance – Frameworks, Threat Modeling, and Accessibility in Federal Digital Services (VA Context)

## Executive Summary

Cybersecurity and compliance are foundational to building secure, resilient digital systems within the Department of Veterans Affairs (VA). These principles ensure that sensitive Veteran data is protected, accessible, and handled in accordance with federal mandates and agency-specific guidelines. This paper outlines the essential compliance frameworks (FISMA, NIST 800-53, FedRAMP), introduces secure design techniques (STRIDE, DREAD), and explores how accessibility (Section 508, WCAG) is a component of both security and user experience.

1. Compliance Frameworks

## 1.1 FISMA (Federal Information Security Modernization Act)

- Purpose: Mandates federal agencies implement comprehensive security programs.

- Key Requirements:

- Annual security audits and ATO (Authorization to Operate)

- Categorization via FIPS 199

- Continuous monitoring with eMASS or equivalent

- VA Implementation:

- Applies to internal and contractor systems

- Conducted within RMF lifecycle with roles: AO, ISSO, System Owner

## 1.2 NIST SP 800-53

- Scope: Defines security and privacy control baselines.

- Control Families:

- AC (Access Control), SC (System & Communications Protection), AU (Audit), IR (Incident Response), PT (Privacy)

- VA Context:

- Tailored to Moderate/High FISMA levels

- Used during ATO and VA TRM assessments

- Generates SSP, POA&M, CIS documentation

## 1.3 FedRAMP

- Purpose: Applies NIST controls to cloud service providers.

- Participants: CSPs, 3PAOs, FedRAMP PMO, VA sponsor

- Steps:

1. Documentation (SSP, ISCP, CP)

2. 3PAO testing

3. PMO authorization

- VA Context:

- Moderate-level authorization for Salesforce, AWS GovCloud

- TRM overlays enforced via VA Handbook 6500

## 1.4 VA Handbook 6500

- Purpose: Governs security implementation across VA systems.

- Policies:

- Encryption, incident response, system interconnection

- Aligns with NIST 800-53 and overlays

- Integrated into CRISP program

- Applies To:

- All VA-owned and partner systems

- Required for security reviews and contractor onboarding

2. Secure Design Methodologies

## 2.1 STRIDE

- Acronym: Spoofing, Tampering, Repudiation, Information Disclosure, DoS, Elevation of Privilege

- VA Use Cases:

- DGIB sync flows, VA.gov design reviews

- Mitigation documented in Architecture Decision Logs

## 2.2 DREAD

- Components: Damage, Reproducibility, Exploitability, Affected Users, Discoverability

- VA Application:

- MPI and VA Profile integration risk scoring

- Supports budgeting and engineering prioritization

3. Accessibility and Cybersecurity

## 3.1 Section 508

- Mandate: Federal IT systems must be accessible to people with disabilities

- Scope:

- VA.gov, VHA portals, My Education Benefits

- Admin portals like VA Profile UI

- Requirements:

- Keyboard support, screen reader compatibility, color contrast

## 3.2 WCAG 2.1

- Principles: Perceivable, Operable, Understandable, Robust

- VA Implementation:

- Level AA compliance required

- Validated using WAVE, Axe, NVDA

- Compliance Risk:

- May trigger audits or constituent complaints if unaddressed

## 4. Tools and References

| Function | Tools/Sources |

|----------|----------------|

| Security Controls | NIST OSCAL, eMASS, OpenControl |

| Threat Modeling | OWASP Threat Dragon, MS TMT |

| Accessibility Testing | Axe, Lighthouse, WAVE, NVDA |

| Frameworks | NIST CSF, VA 6500, FedRAMP Templates |

## 5. Architecture Example: VA Benefits Portal

- Compliance:

- FISMA Moderate boundary

- FedRAMP Moderate hosting on AWS GovCloud

- VA Handbook 6500-aligned SSP, CP

- Security:

- STRIDE for DGIB address flows

- IAM scoped policies, logging via Splunk

- TLS 1.2 and KMS encryption for data in transit/rest

- Accessibility:

- Section 508 testing before go-live

- Keyboard navigation validated via NVDA

## Conclusion

VA digital systems must integrate security and compliance from day one. Adhering to NIST, FedRAMP, and accessibility requirements ensures Veteran trust and resilient IT delivery.

## Next Steps:

- Run 800-53 overlay gap analysis

- Build STRIDE/DREAD threat models in reviews

- Automate accessibility and security scans in pipelines

- Expand EA reviews to include compliance gate checks