Project Part Four – Final Report

Charles Oddo - Tristan Michalak - Katelynn Ketchum

Kent State University

IT-24000-300: Developing and Implementing Security Policies

Benjamin Darby

5/9/2025

Project Part Four – Final Report

The purpose of this report is to ensure Blue Stripe Tech is Department of Defense (DoD) compliant in protecting national security information. Included in this document are recommendations and requirements that will need to be implemented in a security policy to conform to industry standards and DoD compliance regulations.

The DoD and the Defense Industrial Base (DIB) have developed the Cybersecurity Maturity Model Certification (CMMC) that will align with existing information security requirements for the DIB and assist in protecting Controlled Unclassified Information (CUI) (About CMMC, n.d.). The CMMC provides a tiered model that implements cybersecurity standards at progressively advanced levels depending on the sensitivity of information. DoD contractors and subcontractors must achieve a specific level as a condition of being awarded a contract (About CMMC, n.d.).

DoD instructions 8510.01, titled Risk Management Framework (RMF) assigns responsibilities for executing and maintaining the framework. It provides comprehensive guidance on managing cybersecurity risks for DoD IT systems (Sherman, DoD Instructions 8510.01, 2022). This framework applies to all DoD IT systems that receive, process, store, display or transmit DoD information including contractors (Sherman, DoD Instructions 8510.01, 2022).

NIST Special Publication 800-53 provides a catalog of security and privacy controls for federal information systems and organizations (NIST SP 800-53 Rev. 5, 2020). The NIST SP 800-53 framework provides a significant group of security and privacy controls for federal information systems and organizations. It is widely used within the DoD to ensure that comprehensive security measures are accomplished.

This framework includes access control, audit and accountability, configuration management, incident response, maintenance, physical and environmental protection, risk assessment, system and information integrity and more (NIST SP 800-53B, 2020).

The following list is of the required compliance laws that Blue Stripe Tech needs to follow to remain DoD compliant.

- Federal Information Security Act (FISMA) (FAR Clause 52.204-21 Basic Safeguarding of Covered Contractor Information Systems., 2021)
- Sarbanes-Oxley Act (SOX) (DFARS clause 252.204-7012 Safegaurding Covered Defense Information and Cyber Incident Reporting, 2024)
- Cybersecurity Maturity Model Certification (CMMC) while not a law, CMMC is a mandatory compliance framework for DoD contractors (About CMMC, n.d.).

Blue Stripe Tech will implement security controls across seven key IT domains per NIST SP 800-53 and DoDI 8500.01.

User Domain: Multifactor Authentication (MFA), Role-Based Access Control (RBAC), mandatory cybersecurity training and awareness, and implementing user activity monitoring and logging to detect and respond to unauthorized access attempts (NIST SP 800-53 Rev. 5, 2020).

Workstation Domain: Strong password requirements, data is backed up properly and regularly, encrypting data through use of a virtual private network (VPN), implementation of firewalls, regular patching, and a defense-in-depth approach ensuring multiple security controls are in place (NIST SP 800-53 Rev. 5, 2020).

LAN Domain: Physical security controls need to be placed in data centers, wiring closets, and computer rooms, strong access control policies ensuring only those allowed access to have it, principle of least privilege, vulnerability assessments, and implementing LAN server and configuration standards, procedures, and guidelines (NIST SP 800-53 Rev. 5, 2020).

LAN-to-WAN Domain: Implementing proper access controls, like the LAN domain, physical security would need to be implemented, content filtering, having a DMZ, and access controls (NIST SP 800-53 Rev. 5, 2020).

Remote Access Domain: Session Termination, monitoring and control methods, and cryptographic mechanisms (NIST SP 800-53 Rev. 5, 2020).

System/Application Domain: privilege levels for code execution, development and testing environments, physical security controls, and interactive application security testing (NIST SP 800-53 Rev. 5, 2020).

This is a list of the required standards for common devices by domain required for Blue Stripe Tech to become DoD compliant utilizing the chosen NIST SP 800-53 framework.

User Domain: Password complexity requirements, biometric authentication standards, account lockout standard, security awareness and training standard, removable media control standard.

Workstation Domain: Secure baseline configurations, antivirus standards, system hardening, automatic system lockout standard, application whitelisting standard, local administrator account standard.

LAN Domain: Network encryption standards, physical security, network time synchronization standard, secure DNS standard, wireless network security standard.

LAN-to-WAN Domain: Secure tunneling protocols, intrusion detection system standard, zero trust architecture standard, DDoS mitigation standard.

Remote Access Domain: VPN encryption standards, endpoint security policies, split tunneling prevention standard, remote workstation security standard.

System/Application Domain: Secure coding standards, software patching practices, API security standard, database encryption standard, logging and audit standard.

Blue Stripe Tech will implement a series of policies to meet Department of Defense (DoD) compliance requirements while securing critical infrastructure. Each policy will align with the implemented frameworks to ensure regulatory compliance.

Access Control Policy:

Description: The access control policy protects sensitive information, systems that access information, and physical areas from unauthorized use and access. This policy will outline who can access what information and how they are allowed to access said information. This policy looks to protect an abundance of things within the System/Application Domain by making it clear as to who can and who can't access important or critical assets and information. Those who do not follow the rules as to who can and who can't access things that they don't have the authorization for will face consequences. Overall, this policy will help to keep data and assets secure by making it so that critical and important things

can’t be accessed without proper authorization which will all around help to secure the system/application domain.

Domains: User domain, System/Application domain

Standards used:

- Access enforcement NIST SP 800-53 AC-3
- Least Privilege NIST SP 800-53 AC-6
- Identification and Authentication NIST SP 800-53 IA-2

Controls implemented:

- Multi-factor authentication
- Role-Based access control
- Account lockout

Data Encryption Policy:

Description: The WAN Encryption Policy will define DoD approved encryptions methods per NIST 800-53 SC-8 Transmission Confidentiality and Integrity (NIST SP 800-53 Rev. 5, 2020).

Domains: LAN domain, LAN-to-WAN domain, Remote Access domain.

Standards used:

- Encryption standard
- Cryptographic key establishment NIST SP 800-53 SC-12
- Cryptographic key protection NIST SP 800-53 SC-13

Controls implemented:

- Mandatory AES-256 encryption for all stored and transmitted sensitive data
- TLS 1.2 or IPsec encryption

- Regular key rotation and key management.

Network Security Policy:

Description: The network security policy establishes the necessary security controls and protocols to protect Blue Stripe Tech's local area network (LAN), wide area network (WAN), and LAN-to-WAN connections from unauthorized access, cyber threats, and data breaches. This policy ensures that network infrastructure remains resilient, secure, and compliant with DoD standards and industry best practices (NIST SP 800-53 Rev. 5, 2020).

Domains: LAN Domain, WAN Domain, LAN-to-WAN Domain

Standards used:

- Boundary protection NIST SP 800-53 SC-7
- System monitoring NIST SP 800-53 SI-4
- Configuration settings NIST SP 800-53 CM-6

Controls implemented:

- Firewall protection with strict access control rules at all WAN entry points
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor activity
- VLAN segmentation to isolate critical systems.

Remote Access Policy:

Description: The remote access policy will ensure the secure connection to the internal network and systems from a remote site. It will ensure compliance and security for remote workers and protect sensitive data off premises. The remote access policy will follow NIST SP 800-53 Rev.5, DoDI 8500.01, DoD 8510.01.

Domains: Remote Access Domain.

Standards used:

- Remote Access NIST SP 800-53 AC-17
- Cryptographic protection NIST SP 800-53 SC-12
- Mobile device access control NIST SP 800-53 AC-19.

Controls implemented:

- Use VPN with AES-256 encryption for all remote connections
- Enforce session time out
- Restrict mobile access to compliant devices only.

Incident Response Policy:

Description: The Incident Response Policy is a document that directs individuals of the organization how to detect, respond and recover from a computer security incident.

Domains: All domains

Standards used:

- Incident handling NIST SP 800-53 IR-4
- Audit review NIST SP 800-53 AU-6
- Incident response plan development.

Controls Implemented:

- Security Information Event Management (SIEM) tools to identify threats in real time
- Incident reporting procedures
- Quarterly training for incident response team.

Software Development Policy:

Description: The Software Deveolpment Policy follows the Software Development Life Cycle, secure coding, and change management. This policy dictates the proper way for an organization to create, manage, and maintain the software within the company.

Domains: System/Application domain

Standards used:

- Developer security testing NIST SP 800-53 SA-11
- Supply chain risk management NIST SP 800-53 SA-12

Controls Implemented:

- Industry best practice secure coding guidelines
- Automated software patching and updates.

Physical Security Policy:

Description: The Physical Security Policy will outline procedures for protecting a company's physical assets like buildings, equipment, and people. This policy will help protect physical assets from unauthorized use and ensure employees and visitors have a safe work environment.

Domains: LAN domain - System/Application domain

Standards used:

- Physical security access control NIST SP 800-53 PE-3
- Monitoring physical access NIST SP 800-53 PE-6
- Physical protection of information systems.

Controls Implemented:

- Restrict access to data centers using electronic badge readers
- Video surveillance
- Monitor environmental aspects of data center.

Application Security Policy:

Domains: System/Application domain

Description: The Application security policy ensures that all software applications, API's, databases, and systems within Blue Stripe Tech follow secure development, testing and deployment practices to prevent cyber threats. The policy protects application integrity, prevents unauthorized access, and enforces security controls to comply with DoD cybersecurity requirements, including NIST SP 800-53 and NIST SP 800-218.

Standards used:

- Secure software development practices NIST 800-218
- Separation of environments standard NIST SP 800-53 SA-11
- production data for testing standard NIST SP 800-53 SC-3P

Controls Implemented:

- Necessary privilege levels for code execution
- Must utilize separate environments for developing and testing applications
- Application security testing tools must be available for utilization if needed

Policy Name: Access Control Policy

Policy Statement:

Blue Stripe Tech will implement access controls to ensure that only authorized personnel can access critical systems.

Purpose/Objectives:

To enforce role-based access, prevent unauthorized entry, and comply with DoD requirements.

Scope:

This policy applies to all Blue Stripe Tech employees, contractors, and third-party vendors accessing company systems.

Standards:

- Enforce multi-factor authentication (MFA) for all accounts. NIST 800-53 IA-2
- Ensure role-based access control (RBAC) NIST SP 800-53 AC-6
- Require strong password policies following NIST SP 800-63B

Procedures:

- Employees must authenticate using both a password and a secondary factor such as biometrics or security tokens.
- Access permissions shall be reviewed quarterly to ensure compliance.
- Any unauthorized access attempt will trigger automated security alerts and will be investigated.

Guidelines:

Users must safeguard login credentials and report suspicious activity immediately. Never share access credentials.

Blue Stripe Tech High-Level Deployment Plan for Implementation

Step 1: Policy Finalization

- Review and finalize compliance policies ensuring DoD alignment
- Map requirements to NIST SP 800-53 and CMMC guidelines

Step 2: Technical Implementation

- Deploy required security tools (firewalls, IDS/IPS, access control)
- Enforce encryption standards for sensitive data

Step 3: Training and Awareness

- Conduct in person and or remote video training for employees on compliance standards.
- Create response protocols for incidents

Step 4: Auditing and Continuous Monitoring

- Implement scheduled audits to assess compliance
- Adjust security policies as necessary based on risk assessments.

Cost Considerations

- Acquiring necessary hardware and software
- Employee training
- Creating incident response

References

About CMMC. (n.d.). Retrieved Feb 6, 2025, from Cheif Information Officer U.S. Department of Defense: https://dodcio.defense.gov/CMMC/About/form/MG0AV3/

(2019). *Department of Defense Instruction 8500.01.* Retrieved Feb 2025, from https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

DFARS clause 252.204-7012 Safegaurding Covered Defense Information and Cyber Incident Reporting. (2024, May). Retrieved Feb 2025, from Aquisition.gov: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

FAR Clause 52.204-21 Basic Safeguarding of Covered Contractor Information Systems. (2021, Nov). Retrieved Feb 2025, from Acquisition.gov: https://www.acquisition.gov/far/part-52#FAR_52_204_21

FIPS PUB 140-3 Security Requirements For Cryptographic Modules. (2019, March 22). Retrieved April 2025, from NIST: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

Johnson, R., & Easttom, C. (2022). *Security Policies and Implementation Issues* (Third ed.). Jones & Bartlett Learning, LLC.

NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. (2020, Dec. 10). Retrieved Feb 2025, from NIST: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST SP800-53B, Control Baselines for Information Systems and Organizations. (2020, Dec 10). Retrieved April 2025, from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

Ross, R., & Pillitteri, V. (2024, May). *NIST SP 800-171 Rev. 3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* Retrieved Feb 2025, from NIST: https://csrc.nist.gov/pubs/sp/800/171/r3/final

Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R., & Bodeau, D. (2021, Feb). *NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171.* Retrieved Feb 2025, from NIST: https://csrc.nist.gov/pubs/sp/800/172/final

Sherman, J. B. (2022). *DoD Intruction 8510.01 Risk Management Framework for DoD Systems.* Office of th DoD Cheif Information Officer. Retrieved Feb 2025, from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300

Sherman, J. B., & Deasy, D. S. (2021). *DoD Instruction 8170.01 Online Information Management and Electronic Messaging.* DoD, Office of the Cheif Information Officer. Retrieved Feb 2025, from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/817001p.pdf