

Security Architecture and Design for Blue Stripe Tech

Millie Altman

ISSC 481 Summer

Dr. Heidi Huhn

31 August 2025

Introduction

As Blue Stripe Tech enters into a major contract with the U.S. Air Force Cyber Security Center, compliance with U.S. Department of Defense security requirements becomes a critical obligation. In this draft, there will be an outline of the key compliance laws, directives, and frameworks that will shape the organization's policies and infrastructure. The goal is to align our IT security practices with DoD standards to ensure proper protection of sensitive government data and systems.

Compliance Laws and DoD Directives

The Federal Information Security Modernization Act, abbreviated to FISMA, mandates that federal agencies and contractors establish robust information security programs to safeguard government data. This law directly applies to organizations such as Blue Stripe Tech, which must implement structured approaches to risk management, incident response, and continuous monitoring of systems. Compliance with FISMA is not optional; it is a legal requirement for maintaining partnerships with federal entities (Office of Management and Budget [OMB], 2014).

In addition to FISMA, the Gramm-Leach-Bliley Act, or GLBA, imposes data privacy standards that extend beyond financial institutions. While originally designed to regulate financial services, its principles apply to any organization that processes or stores sensitive data, including personally identifiable information, abbreviated to PII. For Blue Stripe Tech, GLBA serves as an important benchmark for secure data transmission and privacy protection in the context of handling government-related information (Federal Trade Commission [FTC], 2023).

The Cybersecurity Maturity Model Certification, or the CMMC, represents another key framework affecting defense contractors. Developed by the Department of Defense, CMMC

ensures that contractors adhere to appropriate cybersecurity practices based on the sensitivity of the data that is managed. To remain eligible for DoD contracts, Blue Stripe Tech will likely need to achieve at least Level 2 certification, which establishes foundational security controls for protecting controlled unclassified information, abbreviated to CUI, (Department of Defense [DoD], 2023).

Complementing these requirements is DoD Instruction 8510.01, also known as the Risk Management Framework, or RMF. This directive establishes structured processes for assessing and mitigating cybersecurity risks, implementing appropriate safeguards, and maintaining continuous authorization of systems. Blue Stripe Tech must adopt RMF to ensure its systems are consistently monitored and compliant with DoD standards (Department of Defense, 2019).

There are strict requirements that govern the handling of controlled unclassified information. Executive Order 13556 mandates that organizations implement protections for CUI, including strict access controls, encryption protocols, and both physical and logical security measures (Department of Defense, 2019). Compliance with these standards is essential for contractors like Blue Stripe Tech that manage sensitive but unclassified government information (National Archives, 2023).

Finally, the Defense Federal Acquisition Regulation Supplement, abbreviated to DFARS, 252.204-7012 specifies requirements for safeguarding covered defense information, also known as CDI. This regulation requires contractors to report cybersecurity incidents within 72 hours and to maintain detailed cyber-incident response capabilities (National Institute of Standards and Technology [NIST], 2021). DFARS also incorporates NIST SP 800-171, which outlines best practices for securing CDI across contractor systems and networks (NIST, 2021).

Role of Policy Frameworks

Blue Stripe Tech will need to align with several established policy frameworks to ensure a comprehensive and compliant security posture following DoD standards. NIST Special Publication 800-53 Revision 5 provides a detailed catalog of security and privacy controls applicable to federal information systems (NIST, 2020a). NIST SP 800-171 outlines requirements for safeguarding Controlled Unclassified Information within nonfederal systems, serving as a foundational standard for defense contractors (NIST, 2020b). Building on these requirements, the Cybersecurity Maturity Model Certification 2.0 establishes maturity levels that assess the security readiness of contractors supporting the Department of Defense (DoD, 2021). Additionally, Department of Defense Instruction 5200.01 provides specific guidance for implementing information security in DoD-affiliated systems (DoD, 2020a). Working cohesively together, these frameworks ensure compliance with the Federal Information Security Modernization Act and Defense Federal Acquisition Regulation Supplement, which positions the Blue Stripe Tech company to meet the cybersecurity expectations of the U.S. Air Force Cyber Security Center.

Next Steps

In the upcoming sections of this project, these laws and frameworks will be systematically mapped to specific IT infrastructure domains, including the User, Workstation, Local Area Network, Wide Area Network, Remote Access, and System/Application domains. This mapping process is critical because each domain has unique vulnerabilities and security requirements that must be addressed to ensure full compliance with Department of Defense (DoD) standards. For example, the User Domain will emphasize policies related to identity management and user training, while the Workstation Domain will focus on endpoint protection

and patch management (DoD, 2020a). Similarly, the LAN and WAN domains will require robust network security measures, including boundary defenses, intrusion detection, and encryption of data in transit (DoD, 2020a). Remote Access policies will address secure authentication and VPN requirements, while the System/Application Domain will incorporate access controls, logging, and secure software development practices (NIST, 2021). By aligning domain-specific controls with the appropriate laws and frameworks, the project will ensure that Blue Stripe Tech's IT infrastructure is both compliant with federal and DoD regulations and resilient against continuously evolving cybersecurity threats.

Selected Policy Frameworks

For the development of security policies at Blue Stripe Tech in support of its Department of Defense contract, the Risk Management Framework, abbreviated to RMF, for DoD Information Technology, outlined in DoD Instruction 8510.01, will serve as the primary guiding framework (Department of Defense [DoD], 2019). RMF establishes a structured, six-step lifecycle process that integrates security and risk management into every phase of the system development life cycle, abbreviated to SDLC (DoD, 2019). This process includes the steps of categorizing, select, implement, assess, authorizing, and monitor (DoD, 2019). Utilizing this approach will ensure that security considerations are embedded throughout the design, deployment, and operation of systems, and not treated as an afterthought or consideration. By aligning these security policies with RMF, Blue Stripe Tech will not only meet DoD's strict compliance requirements but also create a proactive stance in identifying risks, implementing mitigations, and maintaining continuous authorization for its systems. In addition, RMF is directly aligned with the security and privacy controls outlined in NIST Special Publication 800-53, Revision 5, which provides a

comprehensive catalog of safeguards that address threats across multiple domains of information security (DoD, 2019).

Working in agreement with the RMF, the project will align with the Committee on National Security Systems Instruction, or the CNSSI, No. 1253, and DoD Instruction 8500.01, which will provide further guidance on categorizing information systems, determining impact levels, and assigning cybersecurity responsibilities (DoD, 2014). CNSSI 1253 is indispensable for mapping security controls to National Security Systems (NSS), ensuring consistency in how systems are classified and secured. Meanwhile, DoD Instruction 8500.01 establishes the overarching DoD cybersecurity policy framework, reinforcing accountability at both organizational and individual levels while prescribing standards for confidentiality, integrity, and availability. Collectively, these frameworks guarantee that Blue Stripe Tech's security posture remains aligned with the rigorous standards of federal and defense cybersecurity requirements for proper protection.

By integrating the RMF, CNSSI 1253, and DoD Instruction 8500.01, Blue Stripe Tech positions itself to surpass the cybersecurity requirements mandated for defense contractors. This alignment ensures compliance and operational readiness to support DoD missions, including those directed by specialized agencies such as the Air Force Cyber Security Center, also known as the AFCSC (DoD, 2020b). Ultimately, this comprehensive framework adoption will enable Blue Stripe Tech to build resilient systems capable of defending against evolving cyber threats while maintaining the trust and confidence of DoD partners.

DoD-Compliant Policies, Standards, and Controls by Domain

In the User Domain, the primary objective is to ensure that end-users are fully aware of their security responsibilities and consistently follow established protocols to minimize organizational risk. These actions are achieved through the implementation of multiple cybersecurity policies and controls set by various organizations. The Acceptable Use Policy, abbreviated to AUP, requires all users to sign and comply with DoD-approved guidelines that clearly define prohibited activities, restrictions on personal device use, and rules for handling sensitive data (Department of Defense [DoD], 2020a). There should be mandatory security awareness and role-based training programs that are enforced annually to strengthen cybersecurity knowledge across the workforce (National Institute of Standards and Technology [NIST], 2020). Robust account management controls are essential, encompassing stringent provisioning and deprovisioning of accounts, regular access reviews, and strict adherence to the principle of least privilege to ensure users retain only the access required to perform their designated responsibilities (NIST, 2020).

The Workstation Domain focuses on protecting both individuals and computing devices from unauthorized access, malware, and data leakage. Endpoint protection policies mandate that all workstations be configured with DoD-approved antivirus and anti-malware solutions, host-based intrusion detection systems, and encryption software (DoD, 2020a). Furthermore, system hardening practices necessitate the use of baseline images in accordance with the Defense Information Systems Agency Security Technical Implementation Guides, thereby creating secure configurations across all devices in use (DoD, 2020a). Patch management policies ensure compliance with automatic updates for operating systems and applications, requiring compliance with DoD vulnerability timelines to minimize security gaps (DoD, 2020a).

In the LAN Domain, the objective is to safeguard internal network resources from unauthorized access while ensuring secure and efficient communication. Network segmentation is upheld by isolating research and development, administrative, and production environments through the use of virtual local area networks and access control lists, known as VLANs and ACLs (DoD, 2019). Access control measures require port-level security and authentication mechanisms such as IEEE 802.1X to prevent unauthorized network access (DoD, 2020a). Monitoring and logging policies require the centralized collection of LAN traffic data, configuration modifications, and device access records to facilitate forensic analysis and strengthen incident response capabilities (DoD, 2020b).

The LAN-to-WAN Domain focuses on securing communications between internal systems and external networks, including both internet connections and DoD partner integrations. In order to achieve this, the organization enforces a perimeter defense policy based on a layered security strategy (DoD, 2020b). Next-generation firewalls and cloud-based secure web gateways filter outbound traffic and prevent data loss, ensuring the protection of sensitive information (DoD, 2020b). Working in compliance with intrusion detection and prevention requirements, inline IDS/IPS solutions such as Cisco Secure IPS continuously inspect inbound and outbound traffic for malicious activity (DoD, 2020b). Additionally, boundary protection controls enforce rigorous content inspection, deny-all-except rules, and strict port and protocol restrictions on perimeter devices, ensuring that only authorized communications are permitted (DoD, 2020b).

DoD-Compliant Policies, Standards, and Controls

WAN Domain

Policies

- Enforce DoD-approved boundary protection and perimeter security in compliance with DoDI 8500.01 (DoD, 2014).
- Implement continuous monitoring, intrusion detection, and intrusion prevention at WAN ingress/egress points (DoD, 2014).
- Require encryptions for all external WAN connections using FIPS 140-3 validated cryptographic modules (NIST, 2020).
- Apply network segmentation to protect sensitive DoD traffic from lateral movement (DoD, 2020a).
- Require the use of the DoD Public Key Infrastructure, or PKI, for authenticating devices and users (DoD, 2020a).

Standards

- Configure routers, firewalls, and WAN edge devices, aligning with the DISA Security Technical Implementation Guides (DoD, 2020a).
- Secure Border Gateway Protocol sessions using DoD-approved authentication mechanisms (DoD, 2020a).
- Maintain redundant WAN connections for mission availability and continuity of operations (DoD, 2020a).
- Retain logging and packet capture data at WAN boundaries for a minimum of 90 days (NIST, 2020).

Controls

- AC-17: Limit WAN access to authorized devices (NIST, 2020).
- SC-7: Require perimeter firewalls and gateways for boundary protection (NIST, 2020).
- SI-4: Mandate system monitoring with DoD-approved IDS/IPS (NIST, 2020).
- IA-5: Enforce authenticator management with CAC/PIV for admin access (NIST, 2020).

Remote Access Domain

Policies

- Require DoD-approved VPN solutions with multifactor authentication, in compliance with DoDI 8170.01 (DoD, 2019).
- Require the use of Common Access Card or Personal Identity Verification authentication for all remote logins (DoD, 2019).
- Prohibit split tunneling to ensure all traffic routes are monitored through DoD networks (DoD, 2020b).
- Conduct endpoint compliance checks, like posture assessments, before granting remote access to users (NIST, 2021).
- Require all remote users to acknowledge and sign an Acceptable Use Policy (DoD, 2019).

Standards

- Enforce VPN encryption using AES-256 with SHA-256 for data integrity (NIST, 2020).

- Configure remote access gateways according to the DISA VPN Security Technical Implementation Guide (DoD, 2020a).
- Require automatic session timeouts after 15 minutes of inactivity on all devices (NIST, 2020).
- Mandate the deployment of up-to-date antivirus or Endpoint Detection and Response solutions on all remote devices (NIST, 2020).

Controls

- AC-17(2): Require encryption of remote access sessions (NIST, 2020).
- IA-2: Enforce multifactor authentication for remote logins (NIST, 2020).
- SC-13: Require FIPS-validated encryption (NIST, 2020).
- CM-6: Mandate secure configuration baselines for all remote devices (NIST, 2020).

System/Application Domain

Policies

- Require applications to follow Secure Software Development Life Cycle practices according to the DoDI 8500.01 (DoD, 2014).
- Enforce compliance with DISA application STIGs for web, database, and application servers (DoD, 2020a).
- Mandate the implementation of DoD Public Key Infrastructure for user authentication (DoD, 2020a).
- Enforce role-based access control and least privilege principles (NIST, 2020).

- Require vulnerability scanning and patching within 72 hours of DoD and vendor advisories (DoD, 2020a).

Standards

- Require TLS 1.2 or higher with DoD-approved cipher suites for secure communications (NIST, 2020).
- Enforce audit logging per AU-2 for audit events and AU-6 for audit review, analysis, and reporting (NIST, 2020).
- Require cloud-hosted applications to comply with the DoD Cloud Computing Security Requirements Guide (DoD, 2023).
- Conduct static and dynamic application security testing prior to production deployment outlined in various regulations (DoD, 2023).

Controls

- SI-2: Require timely remediation of application vulnerabilities (NIST, 2020).
- SC-23: Protect against session hijacking (NIST, 2020).
- AC-6: Enforce least privilege access (NIST, 2020).
- SA-11: Require security testing and evaluation of application code before release (NIST, 2020).

References

Department of Defense. (2014). *DoD Instruction 8500.01: Cybersecurity*.

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.

Department of Defense. (2019). *DoD Instruction 8510.01: Risk Management Framework (RMF) for DoD IT*.

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf>.

Department of Defense. (2019). *DoD Instruction 8170.01: Online Information Management and Electronic Messaging* (issued January 2, 2019).

Department of Defense. (2020a). *DoD Manual 5200.01, Vol. 1: DoD Information Security Program*.

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol1.pdf.

Department of Defense. (2020b). *DoD Instruction 8170.01: Online Information Services and Internet-Based Capabilities*.

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/817001p.pdf>.

Department of Defense. (2023). *Cybersecurity Maturity Model Certification (CMMC) 2.0 Overview*. <https://dodcio.defense.gov/CMMC/>.

Federal Trade Commission. (2023). *Gramm-Leach-Bliley Act (GLBA)*. <https://www.ftc.gov>.

National Archives. (2023). *Controlled Unclassified Information (CUI)*.

<https://www.archives.gov/cui>.

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5)*.

<https://doi.org/10.6028/NIST.SP.800-53r5>.

NIST. (2021). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (SP 800-171 Rev. 2)*.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>.

Office of Management and Budget. (2014). *Federal Information Security Modernization Act (FISMA) Implementation Guidance*. <https://www.whitehouse.gov>.