Brilliant *at the* Basics

Top 10 IT Cybersecurity Best Practices for Defense Industrial Base (DIB) Partners

The "Brilliant at the Basics" Cybersecurity Campaign is designed to empower our Defense Industrial Base (DIB) partners — particularly innovative small and mid-sized businesses — with streamlined, practical guidance to confidently protect their operations without the burden of massive compliance overhead. In alignment with the Department of War's (DoW) mission to supercharge the "Arsenal of Freedom," this guide distills vital cybersecurity principles into clear, actionable steps for Information Technology (IT) environments.

As we work together to streamline compliance and remove administrative barriers, protecting sensitive defense information remains a vital, shared responsibility. By adopting these foundational core practices, DIB partners can fortify their networks, reduce technical debt, and enable the rapid, secure delivery of superior technology to the tactical edge—ultimately delivering peace through technical strength.

1 *Phishing-Resistant Multi-Factor Authentication (MFA)*

Upgrade your authentication mechanisms to require strong phishing-resistant MFA methods for user accounts. Moving away from legacy MFA methods such as SMS text messages or push notifications forms the foundation of a modern security stack. By combining explicit identity verification with least-privilege principles, you minimize the utility of compromised credentials and significantly reduce the risk of unauthorized access to sensitive systems.

2 *Comprehensive Asset Inventory Management*

Establish and maintain a dynamically updated inventory of enterprise assets, including hardware, software, identities, and data across your estate. An effective inventory goes beyond a simple static list by providing a highly contextualized understanding of every asset. By continuously tracking and validating authorized assets with deep context, you establish the operational visibility required to detect anomalies, manage complex vulnerabilities, maintain compliance, and build a truly resilient defense.

3 *Strategic Technical Debt Reduction*

Minimize your attack surface by aggressively identifying, modernizing, consolidating, or retiring unused legacy infrastructure, redundant data stores, unsupported software, and unnecessary interfaces. Unmanaged "shadow IT" represents prime targets for adversarial exploitation and undermines modern zero-trust controls. Decommissioning these outdated technologies directly hardens your enterprise resilience, lowers operational complexity, and allows you to securely deploy capabilities at the speed of the mission.

4 *Flexible Technology Stack*

Design and maintain a flexible, interoperable stack that supports modular integration of best-in-class commercial technologies. Prioritize open standards and solutions that facilitate interoperability and secure data exchange. Maintaining a modular architecture enables continuous operational agility and mitigates the strategic risk of being locked into a single proprietary vendor ecosystem.

5 *Logical Segmentation to Limit Adversary Lateral Movement*

Implement software-defined segmentation to divide your environment into secure, isolated logical zones. Because adversaries actively attempt to move laterally to high-value targets once they gain initial access, flat networks pose a severe risk to sensitive data. Restricting lateral pathways limits the “blast radius” of any compromise and isolates sensitive Department data even if an individual endpoint is breached.

Brilliant *at the* Basics

Top 10 IT Cybersecurity Best Practices for Defense Industrial Base (DIB) Partners

6 *Risk-Based Vulnerability Management*

Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.

7 *Integrate Security Early in the Development Lifecycle*

Integrate secure coding standards and automated vulnerability scanning directly into the earliest phases of your engineering lifecycle. By shifting security left and testing software components, including all third-party dependencies, during the development phase, you are better positioned to deliver secure capabilities to the warfighter at speed and scale.

8 *Secure AI Adoption and Data Protection*

Establish clear policies and technical guardrails governing the use of artificial intelligence and automation tools across your workforce. Explicitly prohibit the input of sensitive Department data into public, commercial AI systems. By implementing content filtering, endpoint controls, and approved enterprise AI environments, you prevent accidental data exposure while enabling the safe adoption of advanced technologies.

9 *Resilient Backup and Disaster Recovery Architecture*

Protect critical data from adversarial destruction and ransomware by establishing a secure, immutable backup architecture. Maintain redundant copies of all intellectual property, proprietary data, and Department records within a logically vaulted or offline environment. Ensure these backups are secure using isolated credentials distinct from your primary network, and enforce strict protections to prevent unauthorized modification or deletion. Regularly conduct full-system restoration drills to validate that your recovery pipelines can meet operational timelines in the event of a catastrophic compromise.

10 *Continuous Technical Workforce Readiness*

Continuously develop your technical and security personnel on modern enterprise architecture, data protection, and defensive security operations. Operational resilience is directly bottlenecked by workforce capability. Prioritizing targeted technical training across your entire environment equips your team with the essential skills to defend sensitive information and counter evolving threats at the speed of the mission.

*Scan to visit our **Brilliant at the Basics** webpage for more information*

Your Security is Our Security