NIST SP 800-171: DFARS Compliance Solutions

Addressing DFARS regulatory requirements can be a daunting task for any small manufacturer with a limited budget, time or internal technological resources. TSI helps navigate the compliance requirements & ensure that you have the tools & resources in place to focus on growing your business while assuring you have the safeguards in place that will satisfy your industry's compliance requirements. Please refer to the chart below for an overview of the DFARS requirements & the services TSI provide addressing those very areas.

3.1 Access Control: TSI Access Control Enforcement, Mobile Device Management, Azure Rights Management, Log Monitoring, & Log Auditing

Basic Security Requirements			TSI Solution
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices.	✓	Access Control
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	✓	Access Control
Derived Security Requirements			**TSI Solution**
3.1.3	Control the flow of CUI in accordance with approved authorizations.	✓	Access Control
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	✓	Access Control
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	✓	Access Control
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	✓	Access Control
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	✓	Log Monitoring
3.1.8	Limit unsuccessful logon attempts.	✓	Access Control
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	X	N/A
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	✓	Access Control
3.1.11	Terminate (automatically) a user session after a defined condition.	✓	Access Control
3.1.12	Monitor and control remote access sessions.	✓	Log Monitoring & Auditing
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	✓	Access Control
3.1.14	Route remote access via managed access control points.	✓	Access Control
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	✓	Access Control
3.1.16	Authorize wireless access prior to allowing such connections.	✓	Access Control
3.1.17	Protect wireless access using authentication and encryption.	✓	Access Control
3.1.18	Control connection of mobile devices.	✓	Mobile Device Management
3.1.19	Encrypt CUI on mobile devices.	✓	Azure Rights Management
3.1.20	Verify and control/limit connections to and use of external information systems.	✓	Access Control

3.1.21	Limit use of organizational portable storage devices on external information systems.	✓	Access Control
3.1.22	Control information posted or processed on publicly accessible information systems.	✓	Log Monitoring

3.2 Awareness & Training: TSI Security Awareness Training & Security Policy Documentation

Basic Security Requirements			TSI Solution
3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	✓	Security Awareness Training & Security Policy Documentation
3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	✓	
Derived Security Requirements			**TSI Solution**
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	✓	Security Awareness Training

3.3 Audit & Accountability: TSI Access Enforcement Control, Log Monitoring, & Log Auditing

Basic Security Requirements			TSI Solution
3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	✓	Log Monitoring & Auditing
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	✓	Log Monitoring & Auditing
Derived Security Requirements			**TSI Solution**
3.3.3	Review and update audited events.	✓	Log Monitoring & Auditing
3.3.4	Alert in the event of an audit process failure.	✓	Log Monitoring & Auditing
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	✓	Log Monitoring & Auditing
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	✓	Log Monitoring & Auditing
3.3.7	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	✓	Professional Services
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	✓	Professional Services
3.3.9	Limit management of audit functionality to a subset of privileged users.	✓	Professional Services

3.4 Configuration Management: TSI Access Enforcement Control, Internal Vulnerability Scanning, Log Monitoring, & Managed Services

Basic Security Requirements			TSI Solution
3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, & documentation) throughout the respective system development life cycles.	✓	Professional Services
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	✓	Internal Vulnerability Scanning
Derived Security Requirements			**TSI Solution**
3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	✓	Log Monitoring, Professional Services, Internal Vulnerability Scanning
3.4.4	Analyze the security impact of changes prior to implementation.	✓	Professional Services
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	✓	Log Monitoring & Professional Services
3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	✓	Log Monitoring & Auditing
3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	✓	Professional Services & Internal Vulnerability Scanning
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	✓	Professional Services
3.4.9	Control and monitor user-installed software.	✓	Professional Services or Managed Services

3.5 Identification & Authentication: TSI Security Assessment, Access Control Enforcement, Security Policy Documentation, Passportal

Basic Security Requirements			TSI Solution
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	✓	Security Assessment
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	✓	Professional Services
Derived Security Requirements			**TSI Solution**
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	✓	Professional Services
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	✓	Professional Services
3.5.5	Prevent reuse of identifiers for a defined period.	X	N/A
3.5.6	Disable identifiers after a defined period of inactivity.	✓	Professional Services
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	✓	Professional Services
3.5.8	Prohibit password reuse for a specified number of generations.	✓	Professional Services
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	✓	Security Policy Documentation
3.5.10	Store and transmit only encrypted representation of passwords.	✓	Passportal

3.5.11	Obscure feedback of authentication information.	✓	Security Policy Documentation

3.6 Incident Response: TSI Security Policy Documentation

Basic Security Requirements			TSI Solution
3.6.1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	✓	Security Policy Documentation
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	✓	Security Policy Documentation
Derived Security Requirements			**TSI Solution**
3.6.3	Test the organizational incident response capability.	✓	Professional Services

3.7 Maintenance: TSI Managed Services & Access Control Enforcement

Basic Security Requirements			TSI Solution
3.7.1	Perform maintenance on organizational information systems.	✓	Managed Services
3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	✓	Managed Services
Derived Security Requirements			**TSI Solution**
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	✓	Professional Services
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	✓	Professional Services
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	✓	Managed Services
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	✓	Professional Services

3.8 Media Protection: TSI Security Policy Documentation, Access Enforcement Control, Azure Rights Management, Centralized Device & File Encryption

Basic Security Requirements			TSI Solution
3.8.1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	✓	Security Policy Documentation
3.8.2	Limit access to CUI on information system media to authorized users.	✓	Professional Services
3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	✓	Professional Services
Derived Security Requirements			**TSI Solution**
3.8.4	Mark media with necessary CUI markings and distribution limitations.	✓	Azure Rights Management
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	✓	Azure Rights Management
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	✓	Centralized Device & File Encryption
3.8.7	Control the use of removable media on information system components.	✓	Professional Services

3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	✓	Professional Services
3.8.9	Protect the confidentiality of backup CUI at storage locations.	✓	Professional Services

3.9 Personnel Security: TSI Security Policy Documentation

Basic Security Requirements			TSI Solution
3.9.1	Screen individuals prior to authorizing access to information systems containing CUI.	✓	Security Policy Documentation
3.9.2	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	✓	Security Policy Documentation
Derived Security Requirements			**None**

3.10 Physical Protection: TSI Services Not Applicable

Basic Security Requirements			TSI Solution
3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	X	N/A
3.10.2	Protect and monitor the physical facility and support infrastructure for those information systems.	X	N/A
Derived Security Requirements			**TSI Solution**
3.10.3	Escort visitors and monitor visitor activity.	X	N/A
3.10.4	Maintain audit logs of physical access.	X	N/A
3.10.5	Control and manage physical access devices.	X	N/A
3.10.6	Enforce safeguarding measures for CUI at alternate work sites	X	N/A

3.11 Risk Assessment: TSI Security Assessment, Internal & External Vulnerability Scanning, Access Control Enforcement

Basic Security Requirements			TSI Solution
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	✓	Security Assessment
Derived Security Requirements			**TSI Solution**
3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	✓	Internal & External Vulnerability Scanning
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	✓	Professional Services

3.12 Security Assessment: TSI Security Assessment

Basic Security Requirements			TSI Solution
3.12.1	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	✓	Security Assessment
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	✓	Security Assessment

3.12.3	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	✓	Security Assessment
Derived Security Requirements			**None**

3.13 System & Communications Protection: TSI Network Segmentation, Office 365 DLP, Access Control Enforcement, Log Monitoring, Azure Rights Management, File Encryption, AD, Firewall Configuration, VPN Appliance Configuration, Centralized Device & File Encryption, Managed Services, Anti-Virus & Anti-Malware, Removeable Media Restrictions

Basic Security Requirements			**TSI Solution**
3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	✓	Office 365 DLP
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	✓	Network Segmentation
Derived Security Requirements			**TSI Solution**
3.13.3	Separate user functionality from information system management functionality.	✓	Professional Services
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	✓	Log Monitoring, Azure Rights Management, File Encryption
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	✓	Network Segmentation
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	✓	Firewall Configuration
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	✓	VPN Appliance Configuration
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	✓	Azure Rights Management, File Encryption
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	✓	AD, Firewall, Application Configuration
3.13.10	Establish and manage cryptographic keys for cryptography employed in the information system.	✓	Access Control, Centralized Device & File Encryption
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	✓	Access Control
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	✓	Access Control
3.13.13	Control and monitor the use of mobile code.	✓	Managed Services, Anti-Virus, Anti-Malware, Removeable Media Restrictions

3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	X	N/A
3.13.15	Protect the authenticity of communications sessions.	X	N/A
3.13.16	Protect the confidentiality of CUI at rest.	✓	Centralized Device & File Encryption, Azure Rights Management

3.14 System & Information Integrity: TSI Managed Services, Patch Management, Anti-Virus, Anti-Malware

Basic Security Requirements			TSI Solution
3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	✓	Patch Management
3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	✓	Anti-Virus, Anti-Malware
3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.	✓	Managed Services, Log Monitoring & Log Auditing
Derived Security Requirements			**TSI Solution**
3.14.4	Update malicious code protection mechanisms when new releases are available.	✓	Managed Services, Log Monitoring & Log Auditing
3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	✓	Managed Services, Log Monitoring & Log Auditing
3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	✓	Log Auditing
3.14.7	Identify unauthorized use of the information system.	✓	Log Monitoring & Log Auditing