Technical Support INTERNATIONAL Professional IT Services

TSI's CMMC Solutions

Addressing the CMMC regulatory requirements can be a daunting task for any organization working within the DoD supply chain primes, 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 CMMC requirements & the services TSI provide addressing those very areas.

17 Domains & How We Address Them All

- Access Control (AC)
- Asset Management (AM)
- Audit & Accountability (AU)
- Awareness & Training (AT)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE)
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)
- System & Communications Protection (SC)
- System & Information Integrity (SI)

Technical Support INTERNATIONAL Professional IT Services

Access Control (AC):

ACCESS CONTROL (AC)		TSI COMPETENCY
LEVEL 1		
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	✓
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	✓
AC.1.003	Verify and control/limit connections to and use of external information systems.	✓
AC.1.004	Control information posted or processed on publicly accessible information systems.	✓
LEVEL 2		
AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.	✓
AC.2.006	Limit use of portable storage devices on external systems.	✓
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	✓
AC.2.008	Use non-privileged accounts or roles when accessing non- security functions.	✓
AC.2.009	Limit unsuccessful logon attempts.	✓
AC.2.010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	✓
AC.2.011	Authorize wireless access prior to allowing such connections.	✓
AC.2.013	Monitor and control remote access sessions.	✓
AC.2.015	Route remote access via managed access control points.	✓
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	✓
LEVEL 3		
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	✓
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	✓
AC.3.019	Terminate (automatically) user sessions after a defined condition.	✓
AC.3.012	Protect wireless access using authentication and encryption.	✓
AC.3.020	I Control connection of mobile devices.	✓
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	✓
AC.3.021	Authorize remote execution of privileged commands and remote access to security-relevant information.	✓
AC.3.022	Encrypt CUI on mobile devices and mobile computing platforms.	✓

LEVEL 4		
AC.4.023	Control information flows between security domains on connected systems.	✓
AC.4.025	Periodically review and update CUI program access permissions.	✓
AC.4.032	Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role.	✓
LEVEL 5		
AC.5.024	Identify and mitigate risk associated with unidentified wireless access points connected to the network.	✓

Asset Management (AM):

ASSET MANAGEMENT (AM)		TSI COMPETENCY
LEVEL 3		
AM.3.036	Define procedures for the handling of CUI data.	✓
LEVEL 4		
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	✓

Audit and Accountability (AU):

AUDIT AND ACCOUNTABILITY (AU)		TSI COMPETENCY
LEVEL 2		
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	✓
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	✓
AU.2.043	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	✓
AU.2.044	Review audit logs.	✓
LEVEL 3		
AU.3.045	Review and update logged events.	✓
AU.3.046	Alert in the event of an audit logging process failure.	✓
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.	✓
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	✓
AU.3.050	Limit management of audit logging functionality to a subset of privileged users.	✓

AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	✓
AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.	✓
LEVEL 4		
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	✓
AU.4.054	Review audit information for broad activity in addition to per-machine activity.	✓
LEVEL 5		
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	✓

Awareness and Training (AT):

AWARENESS AND TRAINING (AT)		TSI COMPETENCY
LEVEL 2		
AT.2.056	Ensure that managers, system administrators, and users of organizational 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 those systems.	✓
AT.2.057	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	✓
LEVEL 3		
AT.3.058	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	✓
LEVEL 4		
AT.4.059	Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.	✓
AT.4.060	Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training.	✓

Configuration Management (CM):

CONFIGURATION MANAGEMENT (CM):		TSI COMPETENCY
LEVEL 2		
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	✓
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	✓

CM.2.063	Control and monitor user-installed software.	✓
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	✓
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	✓
CM.2.066	Analyze the security impact of changes prior to implementation.	✓
LEVEL 3		
CM.3.067	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	✓
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	✓
CM.3.069	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny- all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	✓
LEVEL 4		
CM.4.073	Employ application whitelisting and an application vetting process for systems identified by the organization.	✓
LEVEL 5		
CM.5.074	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).	✓

Identification and Authentication (IA):

IDENTIFICATION AND AUTHENTICATION (IA):		TSI COMPETENCY
LEVEL 1		
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	✓
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	✓
LEVEL 2		
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	✓
IA.2.079	Prohibit password reuse for a specified number of generations.	✓
IA.2.080	Allow temporary password use for system logons with an immediate change to a permanent password.	✓
IA.2.081	Store and transmit only cryptographically-protected passwords.	✓
IA.2.082	Obscure feedback of authentication information.	✓
LEVEL 3		
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	✓
IA.3.084	Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.	✓

IA.3.085	Prevent the reuse of identifiers for a defined period.	✓
IA.3.086	Disable identifiers after a defined period of inactivity.	✓

Incident Response (IR):

INCIDENT RESPONSE (IR):		TSI COMPETENCY
LEVEL 2		
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	✓
IR.2.093	Detect and report events.	✓
IR.2.094	Analyze and triage events to support event resolution and incident declaration.	✓
IR.2.096	Develop and implement responses to declared incidents according to pre-defined procedures.	✓
IR.2.097	Perform root cause analysis on incidents to determine underlying causes.	✓
LEVEL 3		
IR.3.098	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	✓
IR.3.099	Test the organizational incident response capability	✓
LEVEL 4		
IR.4.100	Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.	✓
IR.4.101	Establish and maintain a security operations center capability that facilitates a 24/7 response capability.	✓
LEVEL 5		
IR.5.106	In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.	✓
IR.5.102	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.	✓
IR.5.108	Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.	✓
IR.5.110	Perform unannounced operational exercises to demonstrate technical and procedural responses.	✓

Maintenance (MA):

MAINTENANCE (MA):		TSI COMPETENCY
LEVEL 2		
MA.2.111	Perform maintenance on organizational systems.	✓

MA.2.112	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	✓
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	✓
MA.2.114	Supervise the maintenance activities of personnel without required access authorization.	✓
LEVEL 3		
MA.3.115	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	✓
MA.3.116	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	✓

Media Protection (MP):

MEDIA PROTECTION (MP):		TSI COMPETENCY
LEVEL 1		
MP.1.118	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	✓
LEVEL 2		
MP.2.119	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	✓
MP.2.120	Limit access to CUI on system media to authorized users.	✓
MP.2.121	Control the use of removable media on system components.	✓
LEVEL 3		
MP.3.122	Mark media with necessary CUI markings and distribution limitations.	✓
MP.3.123	Prohibit the use of portable storage devices when such devices have no identifiable owner.	✓
MP.3.124	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	✓
MP.3.125	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	✓

Personnel Security (PS):

PERSONNEL SECURITY (PS):		TSI COMPETENCY
LEVEL 2		
PS.2.127	Screen individuals prior to authorizing access to organizational systems containing CUI.	✓
PS.2.128	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	✓

Physical Protection (PE):

PHYSICAL PROTECTION (PE):		TSI COMPETENCY
LEVEL 1		
PE.1.131	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	✓
PE.1.132	Escort visitors and monitor visitor activity.	✓
PE.1.133	Maintain audit logs of physical access.	✓
PE.1.134	Control and manage physical access devices.	✓
LEVEL 2		
PE.2.135	Protect and monitor the physical facility and support infrastructure for organizational systems.	✓
LEVEL 3		
PE.3.136	Enforce safeguarding measures for CUI at alternate work sites.	✓

Recovery (RE):

RECOVERY (RE):		TSI COMPETENCY
LEVEL 2		
RE.2.137	Regularly perform and test data back-ups.	✓
RE.2.138	Protect the confidentiality of backup CUI at storage locations.	✓
LEVEL 3		
RE.3.139	Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined.	✓
LEVEL 5		
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	✓

Risk Management (RM):

RISK MANAGEMENT (RM):		TSI COMPETENCY
LEVEL 2		
RM.2.141	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	✓
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	✓
RM.2.143	Remediate vulnerabilities in accordance with risk assessments.	✓
LEVEL 3		

RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	✓
RM.3.146	Develop and implement risk mitigation plans.	✓
RM.3.147	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	✓
LEVEL4		
RM.4.149	Catalog and periodically update threat profiles and adversary TTPs.	✓
RM.4.150	Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	✓
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	✓
RM.4.148	Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.	✓
LEVEL 5		
RM.5.152	Utilize an exception process for non-whitelisted software that includes mitigation techniques.	✓
RM.5.155	Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.	✓

Security Assessment (CA):

SECURITY ASSESSMENT (CA):		TSI COMPETENCY
LEVEL 2		
CA.2.157	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	✓
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	✓
CA.2.159	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	✓
LEVEL 3		
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	✓
CA.3.162	Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.	✓
LEVEL 4		
CA.4.163	Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.	✓
CA.4.164	Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.	✓

CA.4.227	Periodically perform red teaming against organizational assets in order to validate defensive capabilities.	✓

Situational Awareness (SA):

SITUATIONAL AWARENESS (SA):		TSI COMPETENCY
LEVEL 3		
SA.3.169	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	✓
LEVEL 4		
SA.4.171	Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.	✓
SA.4.173	Design network and system security capabilities to leverage, integrate, and share indicators of compromise.	✓

System and Communications Protection (SC):

SYSTEM AND COMMUNICATIONS PROTECTION (SC)		TSI COMPETENCY
LEVEL 1		
SC.1.175	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.	✓
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	✓
LEVEL 2		
SC.2.178	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	✓
SC.2.179	Use encrypted sessions for the management of network devices.	✓
LEVEL 3		
SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	✓
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	✓
SC.3.181	Separate user functionality from system management functionality.	✓
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.	✓
SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	✓
SC.3.184	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	✓

SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	✓
SC.3.186	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	✓
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	✓
SC.3.188	Control and monitor the use of mobile code.	✓
SC.3.189	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	✓
SC.3.190	Protect the authenticity of communications sessions.	✓
SC.3.191	Protect the confidentiality of CUI at rest.	✓
SC.3.192	Implement Domain Name System (DNS) filtering services.	✓
SC.3.193	Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).	✓
LEVEL 4		
SC.4.197	Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization.	✓
SC.4.228	Isolate administration of organizationally defined high-value critical network infrastructure components and servers.	✓
SC.4.199	Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.	✓
SC.4.202	Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries.	✓
SC.4.229	Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization.	✓
LEVEL 5		
SC.5.198	Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizationally defined boundaries.	✓
SC.5.230	Enforce port and protocol compliance.	✓
SC.5.208	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	✓

System and Information Integrity (SI):

SYSTEM AND INFORMATION INTEGRITY (SI):		TSI COMPETENCY
LEVEL 1		
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	✓

SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	✓
SI.1.212	Update malicious code protection mechanisms when new releases are available.	✓
SI.1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	✓
LEVEL 2		
SI.2.214	Monitor system security alerts and advisories and take action in response.	✓
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	✓
SI.2.217	Identify unauthorized use of organizational systems.	✓
LEVEL 3		
SI.3.218	Employ spam protection mechanisms at information system access entry and exit points.	✓
SI.3.219	Implement email forgery protections.	✓
SI.3.220	Utilize sandboxing to detect or block potentially malicious email.	✓
LEVEL 4		
SI.4.221	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	✓
LEVEL 5		
SI.5.222	Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.	✓
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	✓

Additional Areas of Expertise

- ✓ ITAR
- ✓ EU GDPR
- ✓ HIPAA
- ✓ NY Cyber Act
- ✓ California Consumer Privacy Act
- ✓ ISO 27001
- ✓ GLBA
- ✓ PCI DSS
- ✓ NY Shields Act

Our Partnership and Membership Organizations

New Horizons 2020 – March 9 - 11