TOTEM | CYBERSECURITY COMPLIANCE **SIMPLIFIED**

TOTEM.TECH

NIST 800-171 Security Assessment Preparation Checklist

□ Determine if your IT system receives, processes, stores, and/or transmits Controlled Unclassified Information (CUI) for the DoD, e.g.: research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code

□ Determine and list which components or subsystems contain CUI.

Are the parts of your IT system that contain CUI somehow segregated from other parts of the system that don't?

□ Develop a written summary of why the system exists, who operates it, and what types of CUI it receives, processes, stores, and/or transmits

□ Gather any existing system security plans and policies, e.g.:

- Acceptable Use Policy
- Configuration Management Plan
- Incident Response Plan
- Network Monitoring/Auditing Plan
- Service Level Agreements with IT vendors and/or cloud service provider
- Windows Group Policy

□ If you use a cloud service provider (CSP), have them provide any security-related documentation they are willing to release

□ Gather any existing system diagrams, e.g.:

- Physical facility diagram
- Physical IT system diagram
- Network architecture diagram
- Interface diagram
- Data flow diagram

□ Gather existing system hardware, software, and firmware lists

□ Gather lists of personnel authorized for physical and logical access to system, e.g.:

- List of employees with facility access badges or keys
- List of user accounts on the system

□ Gather results of any previous security assessments, audits, scans, and/or penetration tests

□ Provision a temporary system account for the assessor to use to perform privileged functions, such as scanning a server

□ Determine locations for possible network taps to conduct network scans. For instance, a switchport for connection to the subnet that contains CUI

□ Allocate time from IT staff/vendor for the duration of the assessment, and time from executive staff for a portion each day of the assessment

□ Prepare a working and meeting space (e.g. conference room) for the assessor for the duration of assessment

□ Designate an IT system “owner” who will sign off and authorize the resultant system security plan

□ Designate an Incident Response coordinator, even if you don’t have an Incident Response Plan yet; this person will be responsible for the Cyber Incident Reporting requirement in the DFARS

□ Designate a spot on your network, e.g. file server, to securely store all the resultant system security plan, assessment results, and supporting artifacts

□ Most importantly: Don’t Panic! Have an open mind during the assessment; try to view the assessor as a benevolent member of the organization, who is just looking to help you improve your cybersecurity posture. All organizations have vulnerabilities and cyber risks. The goal is to get plans in place to mitigate those risks.