SECURITY VITALS
ENTERPRISE DATA SECURITY

18 W Lawrence St
Pontiac, MI 48342
Phone: 866.802.9405
E-mail: sales@securityvitals.com
Web : www.securityvitals.com

7 Key Elements of a System Security Plan (SSP)

for NIST SP 800-171 and CMMC

Information provided by Security Vitals

Department of Defense Interim Rule

The Department of Defense (DoD) issued an interim rule that amends the Defense Federal Acquisition Regulation Supplement (DFARS). The new rule requires organizations to complete an assessment that validates cybersecurity requirements for protecting unclassified information within the DoD supply chain.

As of November 30, 2020, contractors and their sub contractors must have a score representing their NIST SP 800-171 progress published in a federal database before receiving any contract award. Prior to completing the self-assessment, all contractors must develop a System Security Plan (SSP) to accompany the assessment results. If there are any compliance gaps, the score and SSP must also be submitted with a date upon which all requirements will be implemented.

System Security Plan Overview

At a high-level the SSP defines the scope and approach an organization will employ for protecting Controlled Unclassified Information (CUI). It needs to be a stand-alone document that includes specific details about the environment, how it will be managed, and what type of controls are implemented. The following section describes specific criteria that must be included in a SSP.

SSP Criteria

An effective SSP includes key components required to define the environment, roles, and controls for NIST SP 800-171 and CMMC compliance.

System Details

A clear description of the systems where CUI will be stored and accessed provides the foundation for an effective SSP. At a minimum, the system details must include:

✔ IDENTIFICATION

Descriptive details about the environment including the name, responsible organization, owner, administrator, authorized official, and security administrator.

✔ DESCRIPTION/PURPOSE

An explanation of the planned use and types of data that will be stored in the environment.

✔ OPERATIONAL STATUS

Description of the status for the environment (operational, operational but offline, operational but undergoing modification, in design/development, or initial deployment).

✔ ENVIRONMENT

High level description of the environment that includes where it is located, how it is managed, ownership, and network connectivity.

✔ CONNECTIVITY

A description of any other systems that have connectivity to the CUI environment. Must include description of access controls that will ensure the ongoing integrity of the data stored in the CUI environment.

✔ NETWORK ENVIRONMENT DIAGRAM

An architectural drawing of the system environment that depicts the location(s), assets, and logical boundaries

✔ SYSTEM INVENTORY

A complete listing of the assets including description of the types and quantities that will be used to support the CUI environment.

Risk Assessment

It is important to provide a status of the assessment to indicate if it is underway (with a planned completion date) or completed with a detailed mitigation status. Listed below are the details that should be part of any assessment:

- ✔ **APPLICABLE LAWS & REGULATIONS IMPACTING PLAN**
  Description of the specific laws or regulations included in the plan.
- ✔ **MINIMUM REQUIRED CONTROLS**
  A listing and high-level status (compliant/non-complaint) of the controls included in the plan.
- ✔ **SECURITY CONTROLS INCLUDED**
  A listing of the baseline controls included in the assessment plan.
- ✔ **STATUS OF SECURITY CONTROLS BY GROUP**
  Detailed breakdown of individual control groups that list each control and provide a detailed status on the disposition of the control.

Work with Security Vitals

The DOD requires all contractors to submit accurate assessment details and has utilized the False Claims Act to discipline organizations caught submitting misleading or false information.

Since 2016, Security Vitals has helped organizations implement the process and technology necessary to meet NIST 800-171 and CMMC requirements; ultimately helping them retain and secure government contracts. Our team can help with assessments, scoring details, and development of a SSP.

BE CMMC COMPLIANT

Work with Security Vitals:

sales@securityvitals.com | 866-802-9405 | www.securityvitals.com