SECURITY VITALS
ENTERPRISE DATA SECURITY ANALYTICS

7 BASIC STEPS
to Achieving NIST 800-171 Compliance

There are many ways that an organization can achieve NIST 800-171 compliance, but the most critical factor in the equation is the ability to minimize risk. While this variable may seem like the obvious answer to a simple question...the reality is much different.

Your road map to NIST 800-171 Compliance

WWW.NISTNOW.COM

SIMPLIFYING PROCESSES

The Solution You've Been Looking For

Because NIST 800-171 is focused on Controlled Unclassified Information (CUI), an organizations' ability to limit the how, when, and where this information is accessed will have a huge impact on its ability to effectively reduce risk. Since CUI data is largely comprised of drawing (math) data, part numbers, and financial costing data, moving the data to a separate network simplifies the process of protecting it.

The following steps highlight an effective road map for achieving NIST 800-171 compliance:

STEP 1

CONDUCT INTERNAL REVIEW TO IDENTIFY CUI

The first and most basic step toward compliance is developing a keen understanding of where CUI resides and who uses it. Create a tracking spreadsheet and map the data sources and user community.

STEP 2

ESTABLISH CUI ENVIRONMENT AND MIGRATE DATA

Shrinking the footprint for CUI data not only limits overall risk exposure, but it reduces the cost of protecting it. For this reason, it is important to create a separate environment on the network to store all CUI data. The most effective means for accomplishing this task is to install (or configure existing) a firewall and create a CUI network segment.

After creating a secure and separate environment for CUI data, identify the required data storage devices and migrate them to the new environment. Remember to consider how this action will impact the disaster recovery approach as it is still necessary to maintain backup copies of the CUI data. Once the information is properly copied, delete all other versions of CUI data from the environment.

Shrinking the footprint for CUI data not only limits overall risk exposure, but it **reduces the cost** of protecting it.

Because compliance requires **specialized technologies**, you need to allow for sufficient time to select a solution that meets the process needs of the organization.

STEP 3

IMPLEMENT TECHNICAL CONTROLS

The technical controls represent some of the greatest challenges for manufacturing organizations. Because they require specialized technologies and skillsets, allowing sufficient time to evaluate, select, and implement solutions is a must.

SECURITY/FILE INTEGRITY MONITORING

Logs from devices that reside on the CUI environment are collected and evaluated by a security monitoring technology to identify anomalies in system and file access.

VULNERABILITY SCANNING

All devices on the CUI environment (including the firewall) must be scanned on a frequent basis to identify security gaps (vulnerabilities) in software and operating systems. Equally important to collecting vulnerability data is the process of repairing (applying patches) to remediate the gaps. Ensure that maintenance activities are scheduled in similar frequency to the vulnerability scanning process.

MULTIFACTOR AUTHENTICATION

Any employee that needs access to CUI data will be required to utilize multifactor authentication to access the segmented CUI environment. This process requires each person to provide a username, password and 3rd type of validation. There are varied systems available to support multifactor authentication including smartphone and key fob applications as well as fingerprint (biometric) readers.

DEVELOP POLICIES AND CONDUCT AWARENESS TRAINING

Policies are a critical factor in achieving NIST 800-171 compliance as they provide both process and technical guidelines on how CUI data will be managed. Policy templates are available to "jump start" the development and reduce the timeline. As the policies are finalized, the effort will transition to creating awareness training content to educate all employees on the implications of effectively protecting CUI data. Awareness training can be delivered in person or through web-hosted meetings but ensure that each employee is exposed to the training materials.

CONDUCT SECURITY AND RISK ASSESSMENTS

These assessments are designed to help the organization understand what controls are required to effectively protect CUI data and then evaluate their effectiveness at protecting it. Investigate online Excel-based templates as they provide a great starting point and efficiencies that will save time. Conducting the assessments is a process that can be completed with internal resources or outsourced to firms that are more familiar with the process and outcome.

DEVELOP AND PUBLISH AN INCIDENT RESPONSE PLAN

An incident response plan serves as the focal point for handling elevated threats to CUI information. Both technical controls (Step 4) and process controls (Steps 5 and 6) are evaluated and documented to identify thresholds of risk that require notification/involvement from organization stakeholders to sufficiently investigate and resolve. Template resources are also available online to assist with developing the plan; but each plan needs to be sufficiently tailored to meet the unique needs of the organization.

DEVELOP AND PUBLISH A SYSTEM SECURITY PLAN

A System Security Plan summarizes identified risks and describes how the organization addresses (or plans to address) the NIST 800-171 requirements. It defines the environment in which the system operates and how the security requirements are implemented. Template resources are also available online to assist with developing the plan; but it must be tailored to meet the specific needs of the organization.

OTHER **STRATEGIC RESOURCES**

Purchase NIST Compliance as a Service

No doubt some of these steps seem overwhelming and difficult to complete. Our approach is focused on the most cost and resource effective means to addressing NIST 800-171 compliance, but it does require specialized knowledge and skills. For organizations that want to complete the process themselves, it is important to consider strategically leveraging experienced resources as they can reduce the timeframe and drive efficiencies that offset the additional cost.

An alternative option is to purchase NIST compliance as a packaged service. This type of offering provides turn-key delivery of the seven compliance steps and allows manufacturers to focus on their core competency. In fact, the cost of purchasing Compliance as a Service is about one-third of what it would cost a manufacturer to deliver the same capability. Security Vitals offers a compelling Compliance as a Service program that addresses the NIST 800-171 requirements.

For more information, please send an inquiry to sales@securityvitals.com.

Ph: 1-866-802-9405

Email : sales@securityvitals.com

www.nistnow.com

SECURITY VITALS

ENTERPRISE DATA SECURITY ANALYTICS