Is there a NIST 800-171 Solution for Your Company?

The federal government is mandating that their partners all be compliant with NIST 800 which was designed for larger federal agencies. eSecurity Solutions is providing a solution for small – mid-sized companies who have been caught up in this requirement and need a solution. Because of our experience, we have sifted through the 8-10 documents on NIST 800 and have a solution that can scale to your business and still meet federal regulations.

Read the document below to understand:

1) How NIST relates to your business
2) What are expected to do to comply
3) **How eSecurity Solutions can help you to become compliant**

NIST 800-171 Security and How It Relates to Non-Federal Agencies Businesses

DFARS Clause 252.204-7012 requires DoD contractors, **including small businesses**, to:

1. Provide **adequate security** to safeguard covered defense information that resides in or transits through their internal unclassified information systems from unauthorized access and disclosure. In this case, controlled defense information is referred to as **Controlled Unclassified Information (CUI)**.
2. **Rapidly report** cyber incidents to DoD at https://dibnet.dod.mil.
3. When contractors or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer.
4. Preserve and protect images of all known affected information systems identified and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

What is adequate security?

Minimum cybersecurity standards are described in NIST Special Publication 800-171 and break down into 14 areas. In each of these areas, there are specific security requirements that DoD contractors must implement. Full compliance is required no later than December 31, 2017. Contractors must notify the DoD CIO within 30 days of contract award of any security requirements not implemented at the time of contract award. Contractors can propose alternate, equally effective measures to DoD's CIO through their Contracting Officer.

If DoD determines that other measures are required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability, contractors may also be required to implement additional security precautions.

How do small businesses attain these standards?

The standards for securing Non-Federal contractors are contained in NIST 800-171, and multiple other supporting documents including **NIST 800-200**, **NIST 800-53**, **FIPS 199**, **FIPS 200, NIST SP 800-37, and others**, which goes into more detail about the controls and security framework process.

Basic Assumptions of NIST 800-171

The security requirements described in this publication have been developed based on three fundamental assumptions:

• Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;

• Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal systems and organizations; and

• Security requirements for NIST 800-171 ensure that the **Confidentiality requirement** of NIST 800 is met.

- **Two levels** of security requirements are defined and audited against**.** **Basic** requirements are taken from FIPS Publication 200. **Derived** security requirements are taken from FIPS Publication 199.15 and require that no less than a ***moderate*** level baseline of compliance is achieved.

There are **fourteen families of security requirements** (including basic and derived requirements) for protecting the confidentiality of CUI in nonfederal systems and organizations. These security control categories are listed below. Each category had multiple sub-categories and the controls required for each business will vary based upon the data or system protected and the baseline required.

- Access Control
- Audit & Accountability
- Identification & Authentication
- Maintenance
- Maintenance
- Physical Protection
- System & Communication Protection
- Awareness & Training
- Configuration Management
- Incident Response
- Media Protection
- Personnel Security
- Risk Assessment
- System & Info Integrity

Nonfederal organizations can implement a variety of potential security solutions either directly or using *managed services*, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a particular requirement.

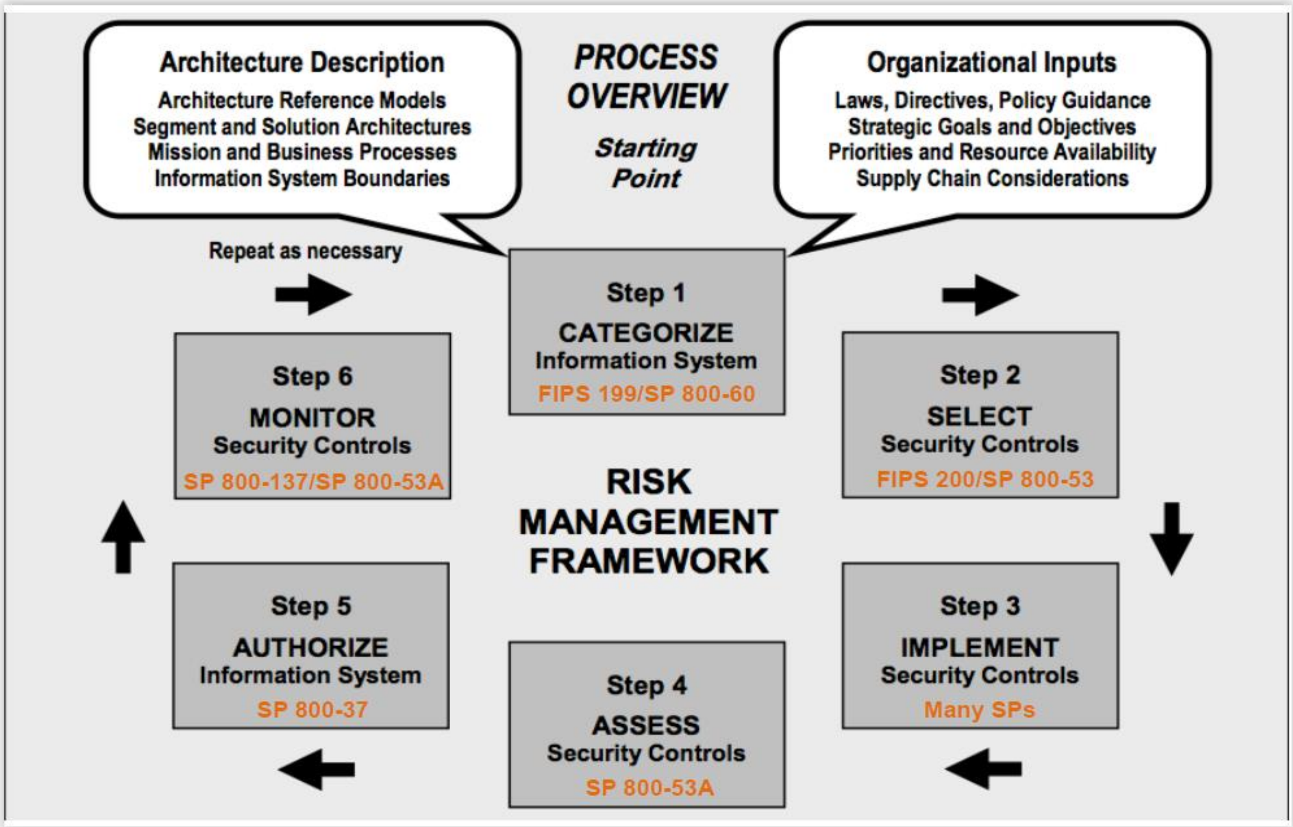
What You Need to Prove Compliance

Nonfederal organizations should describe in a:

- **System Security Plan (SSP)**, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the **protected information system boundary**; the **operational environment**; **how the security requirements are implemented**; and **the relationships with or connections to other systems**.
- Nonfederal organizations should also develop **a Plan of Action & Milestones (POA&M)** *that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented*. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

NIST 800-171 is implemented using a framework shown below. It describes a process for defining, assessing and implementing and appropriate control infrastructure to protect CUI.

NIST RISK MANAGEMENT FRAMEWORK



eSecurity Solutions' NIST Solution for Small – Mid-Sized Companies

eSecurity Solutions provides a solution for small to mid-size companies that need to be compliant with NIST 800-171 that enables compliance without hiring a dedicated security staff. **The eSecurity Solutions Risk Management Process guides companies through the NIST framework by providing necessary services and documentation that enable compliance with the NIST defined goals.**

Security Compliance Process

Step 1: Scope Assessment:

Do initial security assessment to determine the scope and requirements of the NIST compliance project. Creates the foundation to scope and create a security compliance program.

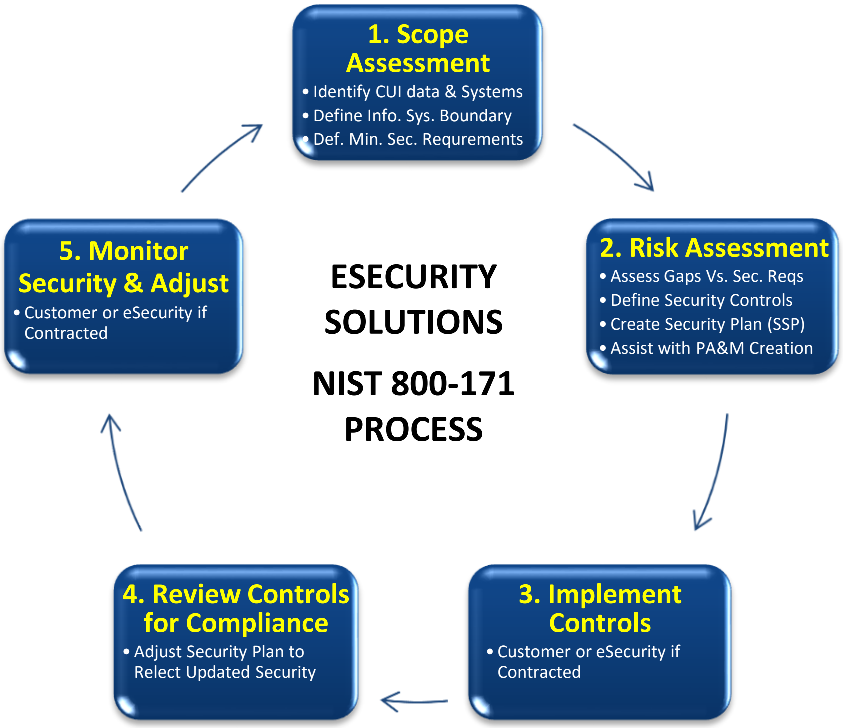
- Identify CUI information and related Information system components to be protected.
- Define the Information System boundaries & document.
- Define minimum security requirements.

Step 2: Do a Security Assessment to determine the necessary controls

- Create and document a System Security Plan (SSP)
- Help you to Define your own Plan of Action & Milestones (POA&M)

Step 3: Implement Recommended controls & assess quality

- Performed by Customer or by eSecurity if we are contracted


1. Scope Assessment
• Identify CUI data & Systems
• Define Info. Sys. Boundary
• Def. Min. Sec. Requrements
2. Risk Assessment
• Assess Gaps Vs. Sec. Reqs
• Define Security Controls
• Create Security Plan (SSP)
• Assist with PA&M Creation
3. Implement Controls
• Customer or eSecurity if Contracted
4. Review Controls for Compliance
• Adjust Security Plan to Relect Updated Security
5. Monitor Security & Adjust
• Customer or eSecurity if Contracted
ESECURITY SOLUTIONS
NIST 800-171 PROCESS

Step 4: Review Implemented Controls for Compliance with Security Plan

- Performed by Customer or by eSecurity if we are contracted

Step 5: Monitor Security system & Adjust as Necessary

- Performed by Customer or by eSecurity if we are contracted

Summary

In summary, eSecurity Solutions can help company with their NIST-800 compliance requirements. We can provide all the services necessary to define what you need, provide a roadmap, document your plan, and help you implement your solution.

Call us today to discuss how we can help and to provide you with a quote or email us at sales@esecuritysolutions.com .