It's Just Results

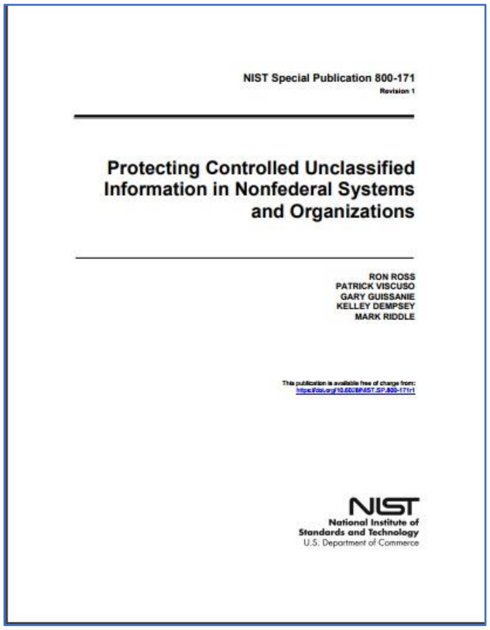
It’s Just Results Compliance Services

NIST 800-171 Getting It Done

Sustainable Security Through Rapid Compliance

NIST 800-171 Getting It Done

DFARS – The Shoe Drops



NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The U.S. Department of Defense's Federal Acquisition Regulation (DFAR) 252.204-7012 for Safeguarding Covered Defense Information has established December 31, 2017 as the deadline for implementing NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

With the deadline for completing the implementation of the controls defined in NIST SP 800-171 many companies are struggling with implementation. They are facing a chaotic situation on determining what needs to be done, how it needs to be done, and how to do it the right way.

The following highlights a recommended path forward. Copy it, use it, modify it to create your own customized path. Make sure the shoe does not hit you!

What Needs to Be Done

The easy answer is "let's get compliant". The right answer is "let's improve security". There is overlap, but they are different. If you focus on the first, you may in fact be putting lipstick on the pig and hoping nobody looks. It is easier to create documentation, do a couple of quick tweaks to the infrastructure and confidently say, "we spend extensive resources on our policies and hardening the infrastructure". Really? Be honest with yourself and consider the implications for your firm's capital (i.e. assets): people, information, organization (brand and culture), and financial; as well as implications for your customer base. Given the ramifications, this is the last place you want to be taking short cuts.

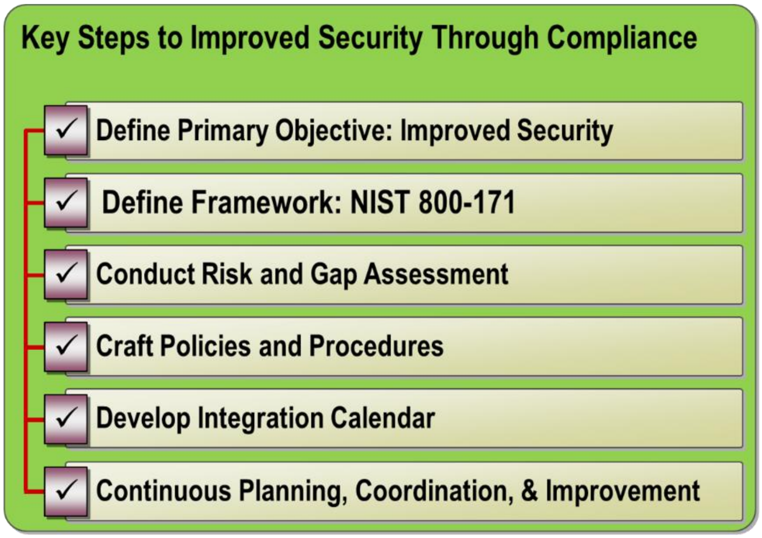
- **Improve Security**
- **Implement Controls**
- **Get Compliant**

There are 110 controls in 800-171 and these controls, and Appendix E must be part of the foundation. These controls, if addressed, along with establishing baseline Non-Federal Organization policies, procedures, and actions have been well thought out and provide an effective "mechanism", this is the operative word, to improve security. Your primary objective, should not be to improve compliance. Improved compliance is only a means to an end of your real primary objective; "Improved Security". Compliance must be achieved, it is valuable as part of the process, but for any of it to have value and provide results, it must be done the right way, and by recognizing that compliance is merely a path.

NIST 800-171 Getting It Done

How It Needs to Be Done

I guess Google is one answer, or buying a stack of policy documents in another. In the first case you can search, download and sign; and in the second case you can purchase, download and sign. Put them into your corporate digital depository, create a three-ring binder, and let the company and your customers know. Voila, compliance! Researching and buying information is okay. However, if you do not take these inputs through a rigorous process with your own organization and people and it is copy and paste, maybe these cases should be categorized as "fake compliance" or "fake security".


Key Steps to Improved Security Through Compliance

- ✓ Define Primary Objective: Improved Security
- ✓ Define Framework: NIST 800-171
- ✓ Conduct Risk and Gap Assessment
- ✓ Craft Policies and Procedures
- ✓ Develop Integration Calendar
- ✓ Continuous Planning, Coordination, & Improvement

The process you should establish begins and flows in the following way:

- **Define your objective:** IMPROVED SECURITY (please agree with me on this)
- **Define your scope and framework:** Define the scope of the information management system and apply a requirements framework (we are discussing 800-171, but it can as well be other requirements frameworks such as NIST 800-53, ISO 27001, FFIEC, or NIST Cybersecurity Framework (CSF) and similar New York Department of Financial Service's 23 NYCRR 500)
- **Conduct the assessment:** Using your framework, assess the value of your data and key risks and gaps
- **Craft Policies and Procedures:** Develop policies that speak to your culture, are actionable with specific deliverables and frequency defined, and achieve the stated security control objectives.
- **Develop a Calendar:** With all the talk of security, it boils down to getting it done, so develop an integrated calendar for recurring and ad hoc activities as well as projects/initiatives that will be started to improve security.
- **Continuous Planning & Coordination:** Think agility and working lean. Work in sprints with regular communications. You need to turn this into a day to day getting it done approach.

The process works. It works on steroids if you have the right people involved in the program.

NIST 800-171 Getting It Done

How to Do It Right

With the right objective and an understanding of what needs to be done, you have two of the three legs to your stool. The other leg is to consider the underlying drivers that will make the difference. Some of the differences already show up in the process as it has been structured (e.g. having a goal, a risk based approach, actionable policies, integrated calendar, and daily coordination), but there are several other key elements (not mutually exclusive). People are at the core of a successful and sustainable implementation.

- **Leadership Involvement:** Begin with leadership. Leadership must be actively involved in implementing your risk based security and compliance program and responsibility for the program should not be delegated to the operational team. The reasoning is to recall what this is all about; being responsible to customer and corporate capital governance. Those entrusted with decision making about the assets should lead this program.

- **Involve Stakeholders:** Creating the right context for the risk based security and compliance program also requires including nurturing stakeholder interests and requirements and making the capturing of those interests are part of an effective implementation process. You can't start with a configuration (e.g. firewall setting), or a control (e.g. access control), you must start with requirements that will be obtained from a variety of sources such as your customer base (they may define requirements in many cases) as well as your system owners.

- **Agile Team based approach:** The team will work with an integrated and prioritized calendar that will reprioritize as work is completed. The calendar is structured so that the highest-risk items will be done first. Recruit team representatives from Legal/Contracts, and Human Resources, Information Technology (IT), Security, and Compliance. Interact with Leadership and Stakeholders. Establish regular communications and feedback. This results in a better understanding of requirements, policies that are understood by leadership and the team that will be implementing and managing the policies on a day to day basis, and ongoing improvement of all activities.

First Action Steps to Take (FAST)

Time is running out. You still have time to slow down and implement the right objectives, establish a holistic process to achieve the objectives, and do it the right way by making people the drivers of the right outcome; Improved Security.

We launched **It's Just Results** to help firms respond to the compliance mandates you are facing while at the same time improving security.

Send us an email at info@itsjustresults.com or call us at 703-570-4266.