It's Just Results

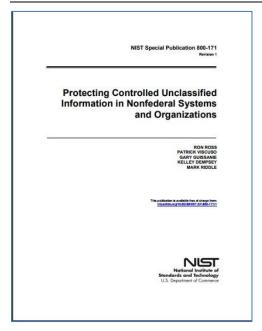It's Just Results Compliance Services

NIST 800-171

Sustainable Security Through Rapid Compliance

It's Just Results, LLC
© 2017

NIST 800-171 So Many Questions

Questionnaire Scenario

You go about your daily work. Without much warning, you receive notification about an inquiry regarding your compliance with National Institute of Standards and Technology Special Publication (NIST SP) 800-171. The full special publication is available on the NIST website; (https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final). Notionally, you may know what it is, but when looking at a questionnaire or examining the Special Publication a bit of unease begins to creep in.

The inquiry may come from many sources. A source could be your own contracts organization who is pointing out that this document is referenced in a contract solicitation. It may also come from a government procurement official. You may also be asked by a major Aerospace and Defense contractor who as your prime, participates in the Exostar program, and requires that you fill out the questionnaire.

There are hundreds of questions. You may think, "who needs to know all this detail", we run a tight ship. Truth be told you need to know. You know that, but you are thinking, "my gosh, with all on our plates, where will we find the time?"

Implications

The immediate implications to your business if you do not respond to the questionnaire or questions from your clients include losing a business partner, failing an audit, losing a contract, and lost revenues. That is a steep price to pay.

- **Losing A Partner**
- **Failing an Audit**
- **Losing a Contract**
- **Lost Revenues**

Here is some of what may happen:

- **Losing a Partner**: Not meeting the cybersecurity requirements of one of "the Exostar Partners" or failing to respond to 800-171 related questions from a government agency
- **Failing an Audit**: Failing a review / audit because there is no real understanding of what needs to be done by the entire company in governing the information and cyber security program
- **Losing a Contract**: Losing a contract that you hold or not being able to pursue a contract you believe you are best suited to win

- **Lost Revenues**: Losing revenues for a brief period can impact immediate cash flow. Cash is king. It can also impact future procurements and revenues as evaluations of your capabilities push you to the bottom of the evaluation list.

The implications can result in immediate and long-term revenue loss. With little time on your plate, how can you do it quickly and who can help?

Rapid Response Support

Start by taking a deep breath.

You, and many others, are part of the current wave of compliance activities in government as well as other industries. The compliance wave requires you to answer the questions in the questionnaire you received. In the case of the Department of Defense, it could be from Exostar or based on a Department of Defense (DoD) procurement you wish to bid on, or any other of many triggers that caused you to look the questionnaire in the face. NIST 800-171 consists of 110 controls. You have many of them in place already and do not even know it. Hooray, things are not as bad as you think!

Our team is called when we receive calls from customers asking our assistance to fill in the questionnaires. They parallel our own assessments. We perform a variety of assessments on a regular basis, so we understand the **Key Factors (see graphic)**, such as the questions, what is being asked, and how best to respond in your environment. Once we come into your organization we can work through the questionnaires before they become an issue or challenge for you.

Key factors in responding to NIST 800-171 Questionnaires include:
- ✓ 800-171 Assessment: 100 Controls with CIS 20
- ✓ Policy Package: w/ Action Plans & Calendar
- ✓ SIEM Integration for Environmental Control
- ✓ Cybersecurity Controls Hardening
- ✓ Coaching & Communications: Clients - Staff
- ✓ Sustainable Governance Program

We will walk you through the process and do the heavy lifting so you can continue to focus on your business. At each step, we carefully explain each of the questions and what they mean for you. Then by looking at your environment (existing policies and procedures), looking at your infrastructure, speaking to several key individuals, **we assess gaps and risks** and rapidly guide your response. Once we are done we explain why we are answering the questions the way we are.

NIST 800-171 So Many Questions

After completing the questionnaire, understanding gaps and risks, we begin to prioritize what you need to do. We work quickly (**days not weeks or months**) and provide you with best practices guidance on a prioritized set of steps or solutions you need to put into place. We apply the Center for Internet Security (CIS) 20 framework (https://www.cisecurity.org/controls/) within the 800-171 to define specific controls to **harden your environment**. Exostar uses the CIS 20 approach in its questionnaire.

In addition, most companies do not have **security and event information** readily available, or actionable for staff or management to make decision. We recommend deploying a tool as part of the upfront work to gain immediate control of the environment. For example, Netwatcher, is a Security Information and Event Management (SIEM) tool has capabilities to identify, communicate, and report many of the control areas in the questionnaire you are accountable to manage. Implementing their toolset is not only easy, it is a highly cost-effective tool that accelerates hardening the security environment for mid-sized and small businesses.

We will also deploy our **800-171 custom policy package**. We do refinement with you, but the package has been developed to address 800-171 controls.

Immediate Benefits You Receive

- A completed 800-171 Questionnaire. We develop this for you and ease your workload.
- Custom recommendations regarding tools and modifications that can be immediately implemented to harden your security environment and mature your cyber security systems (e.g. Exostar seeks you have attained level 03 maturity)
- Meets expectations of the Exostar and Government Client base (provides the communications materials to instill confidence in your program)
- Fifty (50) tailored 800-171 policies and procedures (either provided by our team or modifications made to your policies). Each policy has an action plan and we provide an integrated calendar so that you are clear on how the policies fit together.
- We provide hands on guidance in understanding and communicating with outside organizations on the questions, the policies, the controls, and the ongoing administration of the controls

First Action Steps to Take (FAST)

Getting the questions answered quickly is a requirement faced by the Department of Defense its contractors, as well as other agencies and their contractors. In the next year similar questionnaires will land on everyone's doorstep.

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.