Sinclair
COPYWRITING

CYBERSHEATH
SERVICES INTERNATIONAL

WORK SAMPLE

CLIENT: CyberSheath Services International
PROJECT: Blog Posts on Cybersecurity

by Louise Sinclair | louise@sinclaircopywriting.com | www.sinclaircopywriting.com

THE PROCRASTINATOR'S BLUEPRINT FOR NIST 800-171 COMPLIANCE

On December 31 2017, the deadline for compliance with the NIST 800-171, a mandate for contractors serving local and federal governments, came and went.

This Special Publication provided guidance on the processes and procedures needed to adequately safeguard controlled unclassified information (CUI), defined as any information created by the government or entities on behalf of the government that is unclassified, but still must be appropriately safeguarded.

While some companies were quick to adapt to these new regulatory measures, many companies fell behind because of a lack of resources, confusion over the head-spinning compliance process, or just downright procrastination.

With the deadline long gone and the Department of Defense (DoD) making it crystal-clear that NIST 800-171 is here to stay, becoming compliant is an absolute must for those looking to remain competitive in the industry.

A common problem

Unlike previous security mandates, this is the first that impacts sub-contractors working further down the federal supply chain. This means that for many companies, it's the first time they're having to figure out compliance.

If this describes your company, you're by no means alone. Because these standards must be met by anyone who stores, processes, or transmits CUI for the DoD, General Services Administration (GSA), NASA, or other federal or state agencies, many contractors are struggling to wrap their heads around the complex process ahead.

As it's critical to a supplier's ability to win new business and keep current defense contracts, both prime and sub-contractors will want to confirm that they are, at the very least, on the path to compliance with NIST 800-171.

Achieving compliance

Of course, becoming compliant is easier said than done. The fact that there is no certification process for NIST means contractors work on the honor system, attesting that they have reviewed and heeded the applicable requirements specified in the regulation.

This also means that becoming compliant is not a one-time achievement. Rather, it's an ongoing process of continuous evaluation. Here are the three key actions you can take to get started…

Assess your compliance level

First, you'll need to do due diligence in identifying CUI as it applies to you. Check with your contracting officers or look through your contract to see if CUI has been clearly defined. In many cases, it may not be, and you'll have to review the CUI registry to find similar examples of CUI.

Once you've clearly defined what you need to protect, you can begin to figure out if it's actually being protected sufficiently. You'll have to carefully review your critical systems, including servers, laptops, storage devices, network devices, end-user workstations. You'll also need to assess the physical security of those devices that contain CUI to make sure they are properly safeguarded.

Design a plan of action

Chances are there will be a gap between where you are now and where you need to be. This is common so don't worry!

Fortunately, clause 3.12.4 allows for the submission of a Security System Plan (SSP) and a Plan of Actions and Milestones (POA&M) to buy yourself some time as you work towards your compliance goal. Since many contractors are not yet compliant, these documents are required to show procurement officials you are heading in the right direction.

An SSP will provide an overview of the security requirements needed for every system you use, describe the current controls you have in place, and outline the expected behaviors of all who access them. Your POA&M will show a clearly defined corrective strategy for exactly when and how you plan to resolve any security weaknesses.

Begin implementation

All this planning and assessing means nothing if you don't step up and deliver! Once you've put milestones in place, you'll need to train your staff and ensure they adhere rigorously to these deadlines. You'll also need to document critical advancements in your quest for compliance, properly maintaining your records as you go.

Still nowhere near compliance? Don't panic!

If you missed the December 2017 deadline and you're starting to feel the pressure, don't panic. CyberSheath's Managed Security Services can help you to define your CUI obligations, create a plan of action, and move step-by-step towards full compliance. Contact us today for a free consultation.

END OF SAMPLE

by Louise Sinclair | louise@sinclaircopywriting.com | www.sinclaircopywriting.com