# NIST SP 800-171: The New Normal for Defense Contractors 2018. Are You Ready?

By Christopher Michaud, Chief Technology Officer
McLaughlin Research Corporation
Founder, NeQter Labs

As you read these words, thousands of malicious intrusions are being perpetrated around the globe: some rogue criminal activity, some state-sponsored cyber espionage: Naval Contractor Hacked by China. Sometimes it feels like the invisible army hunting for our data is endless.

As head of IT at a mid-sized defense contractor, my job is to stop these malefactors from entering my company's network. The problem is everywhere. It is estimated that there are over 10 million cyber hits daily against the Pentagon alone. As frightening as that number is, it doesn't account for the attacks leveled against government contractors. McLaughlin Research Corporation faces, on average, 8,000 malicious intrusion attempts each day.

***On television, in the newspaper, the stories are piling up. Stolen emails and credit card numbers. Data breaches. Every industry has been touched, every industry has suffered.***

- Christopher Michaud

The consequence of having your data stolen is chilling. For defense contractors, it's more than a blight on your reputation; it's an issue of national security. Implementing robust cyber security is not optional.

So, where do we start? The US government has an idea. In November 2013, DoD published the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, requiring the safeguarding of Controlled Unclassified Information (CUI) on contractor information systems. This supplement requires that all data breaches be reported within 72 hours of occurrence. CUI encompasses a lot of things, including most of what a typical defense contractor handles. To add teeth, DoD mandated that defense contractors conform to the National Institute of Standards and Technology in Special Publication 800-171 (NIST SP 800-171).

I am constantly surprised how many in our industry have little or no idea what NIST SP 800-171 is or what it requires of companies. Concisely, NIST SP 800-171 sets a baseline for cybersecurity. It includes 110 security requirements relating to network auditing and accountability, policies and procedures, and implementation of best practices. The requirements force contractors to review their current security controls, procedures and best practices to ensure sufficient protections against the loss of CUI. Companies that decide to meet these requirements will likely need to update their network systems and policies following a gap analysis. The deadline for implementation has passed, with DoD contractors expected to have been fully compliant by December 31, 2017. The consequences of procrastination could mean significant loss of business, or worse. For me, the prospect of seeing our 300-person organization with a 70-year history of providing engineering services to the US Navy, shut down or unable to bid on key contracts, was unacceptable. Something had to be done.

## *Chris Michaud's Guide for Implementing NIST SP 800-171*

- NIST SP 800-171 is more than IT, it requires an examination of all company policies and procedures (eg, HR and Contracts).
- Diversify your implementation team. Get buy-in from senior executives.
- Collaborate with peers, even competitors, to share questions and solutions. We are in this together.
- Do not get hung up merely implementing the individual elements of a checklist. The guidance requires holistic thinking and pragmatism.
- Focus on progress, not perfection.
- Don't anticipate where an auditor will focus his or her attention. The policies, the technical implementation, the SSP - it's all important.
- NIST compliance is the new baseline for DoD and will spread to other industries. Learn it, because it's here to stay.

Let me be clear, the NIST mandates are a step in the right direction. When we, at McLaughlin Research, started our journey toward NIST compliance, we had only a vague idea of what it would entail. When we plunged deeper into NIST SP 800-171, we realized it was a massive undertaking.

Implementing NIST SP 800-171 can be fraught with obstacles. A main problem is interpretation. The 110 requirements are written in language that is vague and, at times, opaque. To successfully implement NIST SP 800-171, one needs to know the rules, inside and out. Unfortunately, IT professionals supporting small-to-mid-sized DoD contractors are already overworked and underfunded. How can they be expected to simultaneously put out the myriad fires and methodically work through inches of complex guidance documents? What they'll discover after digesting all 110 mandates is the guidance contains almost no useful information on how they are to be implemented.

My early assumption was that we would coast through compliance, a few security updates here, some policy tweaks there. Wrong.

For example, how was NIST SP 800-171 supposed to map to the established guidance, NIST SP 800-53, an existing standard for handling classified data? How were we to revise our existing procedures? Both my brilliant network engineer (who is a cyber security specialist) and I were left scratching our heads. Clearly, we needed help.

We queried a half a dozen cyber risk-assessment firms, some big, some small. The unified answer was that a turnkey solution did not exist, nor did companies offering NIST expertise in our price range. A piecemeal solution from one of these established consulting firms was going to cost a fortune, perhaps more than $150K in the first year alone. Since NIST requires continual updates and improvements, what would we be paying year after year? And there was the real possibility that we would still fall short of NIST compliance.

It brought some questions to my mind. Who out there understood the emerging cybersecurity threats? Who was best qualified to figure out what these opaque mandates really meant? Who wouldn't charge us $1,200 an hour? The answer: millennials, of course. What if I hired a group of undergraduate and graduate-level cybersecurity experts and set them upon the task of breaking down NIST SP 800-171 into understandable chunks, and to then painstakingly and systematically map each requirement to a specific action? What if

I locked these cyber experts into a room and told them to emerge when they could recite the NIST mandates like the Pledge of Allegiance?

We did that. Here's what happened.

We ground down the NIST elements to their simplest form. We then interpreted and mapped them appropriately. Once we had all information and analyses in hand, we augmented the team with two of our brightest mechanical engineers to pressure test and simplify it. Engineers would approach the problem logically, unburdened by excessive technical knowledge, and find the simplest, most logical connections between each mandate and its corresponding action. In the end, this cross-functional team made McLaughlin Research Corporation compliant with NIST SP 800-171. Now we live NIST.

Along the way, we built what previously did not exist. First, we developed a network appliance to address the auditing and accountability requirements of NIST SP 800-171. Now we, and our auditors, would have access to all our cyber data in real time, visualized in an elegant and intuitive dashboard. After an internal audit showed us that our written cyber policies fell short of the NIST mandates, we built a second tool, a policy builder. This tool helps contractors write their policies, including a System Security Plan (SSP), to match the NIST guidance one-to-one, and create their plan of actions and milestones (POAM). To the best of our knowledge, this is the world's first suite of hardware and software designed to help companies achieve robust security and NIST SP 800-171 compliance.


*The NeQter Compliance Engine*

***My early assumption was that we would coast through compliance, a few security updates here, some policy tweaks there. Wrong.***

With the mystery of compliance removed, we sought to scale our solution and pass it along to other contractors. With some simple, well designed tools, we made NIST compliance achievable.

It is not feasible for the thousands working within DoD to do what we did, but there are solutions. In the cyber world of tomorrow, cyber security will become intertwined into the very fabric of day-to-day business. Those of us in DoD have the privilege of marking the trail and showing other industries how cyber security is done. The countdown to NIST compliance is on, and five years from now, the elements of NIST SP 800-171 will be second nature; we will be hard pressed to remember a time when it was any other way.

NeQter Labs

Originally published July 2017 revised June 2018