Switches and Sweets: Belsnickel Brings Defense Contractors and Subcontractors New Cybersecurity Controls in Preholiday Revisions of NIST Cybersecurity Publication

Related People:
Alexander W. Major

Government Contracts Alert

12.28.2016

If you are aware of German Christmas folklore (and really, who isn't?), you know that Belsnickel is a legendary companion of St. Nick who carries a switch with which to punish naughty children and a pocketful of sweets to reward good ones. This holiday season, many are feeling the sting of a switch of another kind, this one involving the December 20, 2016, issuing by the National Institute of Standards and Technology (NIST) of a preholiday revision of Special Publication 800-171 (SP 800-171), *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*. If SP 800-171 sounds familiar, it is because the publication is the source of the cybersecurity controls that defense contractors must follow and flow down to subcontractors pursuant to DFARS Subpart 204.73 and its operative clauses (*e.g.*, DFARS 252.204-7008 and DFARS 252.204-7012). Essentially accompanying St. Nick (perhaps Santa *Clause* may be more appropriate) this season, the NIST's revised publication may resemble Belsnickel's switch (pun intended) to contractors who already have existing SP 800-171 controls in place (as the controls have been required, in various forms, since November 2013) or who have started down the road toward SP 800-171 adherence in advance of the DFARS-directed December 2017 deadline. With that in mind, let's take a quick look at the implications that switch (pun still intended) brings to the security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations:

- Perhaps the most significant change in the SP is the inclusion of a basic security assessment requirement that requires contractors to proactively create system security plans. While no level of detail in these plans is required, contractors still must "develop, document and periodically update system security plans that describe system boundaries, system environments or operation, how security requirements are implemented and the relationships with or connection to other systems." (*See* SP 800-171, 3.12.4.) Accordingly, contractors operating under DFARS Subpart 204.73 are now affirmatively required to create system security plans that are thorough, accurate, and current.
- There is also a potentially huge substantive change in the sweeping elimination of the word "information" from what once read "information system." The SP now intends adherents to take a much more "holistic" view of their controls, recognizing that such controls should not be applied to just information systems but also to "industrial and process control systems; cyber-physical systems; and individual devices that

are part of the Internet of Things." While reflecting the realities of our ever-connected modern world, this change also means that defense contractors need to take a much broader view of what "cybersecurity" means to their company and data practices. The good news is that in the SP, "system" is formally defined the same as "information system," that is, as "[a] discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." The bad news is that the SP includes the new, undefined term "organizational system" as well. While the definition may be cobbled together through marrying the definitions of "system," above, with "organization" ("an entity of any size, complexity, or positioning within an organizational structure"), its ubiquity in the SP should give contractors operating under DFARS Subpart 204.73 serious pause when examining the scope of their aforementioned system security plan.

- The SP also now addresses more clearly the presence of CUI in not only "mobile devices" but also "mobile computing devices." While this appears at first blush to create a distinction, the change is largely superficial, as the definition of "mobile device" has always included "portable computing device[s]" that include "smartphones, tablets, and E-readers." (*See* SP 800-171, 3.1.19.)

The good news is that the revised special publication isn't without some "sweets" in its pocket:

- The revised SP more clearly limits its control requirements to focus on CUI. This is actually a nice change in that access-control-derived requirements now are intended to apply to CUI posted or processed on publicly accessible systems and not simply the loosely defined "information" of old. (*See* SP 800-171, 3.1.22.)
- The revised SP also expressly allows a carve-out for dedicated video conferencing systems from controls that prohibit remote activation of collaborative devices to secure system and communications protection. The exclusion of these types of conferencing systems allows those systems that rely on one of the participants calling or connecting to the other party to activate the video conference to elude the implications of the SP 800-171 rubric. (*See* SP 800-171, 3.13.12.)

If, as a contractor, you believed that the government's cybersecurity requirements would be static and slow to change, then the realities underlying the existence of Santa Claus and Belsnickel may come as a shock. For the rest of you, one thing is very real – contractors need to make sure that cybersecurity planning is at the top of their New Year's resolutions list. Come this time next year, defense contractors will want to find themselves on the cyber "nice list." Because in the real world of government contracts cybersecurity, federal regulators are armed with something far bigger than a switch.