THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

JUNE 18, 2024 | VOLUME 66 | ISSUE 23

¶ 157 FEATURE COMMENT: A Rule Of Three: NIST Special Publication 800-171 Rev. 3—Finale Or Punchline?

Authors, comics, and storytellers tend to use certain "rules" in all forms of tales across the ages. Perhaps none are more ingrained than the "rule of three." As "School House Rock" may have taught many, three is a magic number. Be it architecturally inclined pigs, sensory-deprived monkeys, or swashbuckling French musketeers, humans have an affinity for three when addressing events, individuals, and even Jedi-related story arcs. It is a number that comes across as more effective, satisfying, or humorous. See! I did it right there. It felt right, didn't it? The rule of three speaks to us because, as Aristotle pointed out, it portends a beginning, a middle, and an end. But, in comedy, there's a twist to that comfort—it's called the "comedic triple," and it juxtaposes and plays against our innate expectations. Every joke consists of a setup, then a build that lures the listener or reader straight into a punchline they (hopefully) didn't see coming. If it lands, that shock and awe (or ah) results in an outburst called laughter. If not, get the hook. Sometimes, however, it may be challenging to figure out what rule of three applies—a pleasant denouement, release or an uncomfortable confusion? Comedy or tragedy?

On May 14, 2024, the National Institute of Standards and Technology (NIST) published its own "third" with its final versions of the much-anticipated guidelines for protecting sensitive Government information, commonly known as Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and its assessment companion NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, now both in Revision 3. While there is absolutely no indication that these documents are a conclusion to NIST's efforts to aid the Federal Government in safeguarding Controlled Unclassified Information (CUI), they do beg an inquiry into just how serious this particular part three is.

The Setup: You're Never Gonna Believe This—OK. A bunch of cybersecurity experts walk into a room. They look around, see all this sensitive information, and think, "We need to lock this stuff down tighter than a drumline in a library!" So, they huddle up, and after much debate, one of them says, "Let's create a guide that makes sure everyone knows exactly how to protect this info!" Voila! In June 2015, NIST SP 800-171 was born. A Cancer! (The zodiac symbol, not the disease). Its purpose is to help nonfederal entities protect CUI—a category of sensitive information requiring safeguarding or dissemination controls as defined by federal law, regulations, and Government-wide policies.

Just like the cybersecurity arena it serves, NIST SP 800-171 has changed through the years. Through versions, edits, and expansions, NIST has attempted to keep this publication truly special—and not just because it's a special publication—by keeping its pages fresh and in line with the threats it is designed to protect against. The challenge for contractors has been ensuring they are keeping up with those changes since NIST SP 800-171 is not a "regulation," per se, but an oft-cited guidance found in federal contract clauses, namely in Department of Defense contracts with Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Shortly after its inception, in December 2016, Revision 1 introduced clarifications and additional directions to improve the implementation and interpretation of security requirements. A few years later, released with little to no fanfare in December 2020, Revision 2 focused on refining controls and aligning with the evolving needs of federal contracts, including more precise guidelines on assessment and documentation. With Revision 3, however, NIST SP 800-171 brings substantial changes across several key areas: the structure of control families has been expanded to better address new threats, individual security controls have been updated to enhance overall system security, and the criteria for tailoring these controls to specific organizational needs have been clarified, all in an effort to adapt to the dynamic landscape of information security. In broad brush strokes, the overarching and more significant changes include:

- **NIST's New Math**: Revision 3 to 800-171 reduced the number of security requirements from 110 to 97. While that might sound like a boon, not so fast! The change is akin to cutting the number of dishes at a buffet but piling more food on each plate. The total number of tasks actually increased due to NIST adding extra security steps within those streamlined controls. That is apparent when one examines NIST SP 800-171A Rev. 3, which increased the number of assessment objectives from 320 in Revision 2 to 422. This change is similar to a restaurant where the menu shrinks, but each dish now includes an appetizer, a main course, and a dessert. Less to choose from but more to chew on.

- **A Growing Family Tree**: NIST SP 800-171 Revision 3 also includes a sort of expansion to the control families found in Revision 2. Previously consisting of 14 control families, Revision 3 added three "new" families of Planning (PL), System and Service Acquisition (SA), and Supply Chain Risk Management (SR). The good news is that these are more like elevated versions of pre-existing requirements related to the System Security Plan and Security Architecture. So, in terms of a family tree, consider it an expansion via an amicable divorce versus a birth.

- **Return of the ODPs**: Organization-defined parameters (ODPs) are back and stronger than ever, increasing from 34 to 49—resident in more than half of the now 97 requirements. ODPs are like customizable settings on your phone but for security policies. They allow agencies to fine-tune their quirky preferences, like "double-check all passwords on Wednesdays" and effectively becoming an agency-dependent game of "Simon Says."

- **Periodic Party's Over**: While providing additional choice to agencies with ODPs, Revision 3 removes it from contractors. The word "periodically" has been unceremoniously kicked out of the SP 800-171 vocabulary. Apparently, thinking that contractors were interpreting "periodically" too creatively, NIST removed the ability of contractors to color too far outside the lines.

The Conflict: Complicating the Already Complicated—The fewer security controls resident in NIST SP 800-171 Revision 3 appear to make things easy. But, like a pun, that change does not have the meaning some would attribute. NIST did not eliminate anything. It just moved stuff around to make 800-171 more svelte. The real change is in what it added and what it chose not to clarify: the 88 ODPs that become a "fill-in-the-blank" Mad Lib, each adding a new layer of complexity and perhaps a need for additional guidance to an already complicated compliance requirement.

The dark comedy of these ODPs lies in their flexibility, which generally benefits the Government over the contractor. The Frequently Asked Questions accompanying the issuance of Revision 3 tell us that an agency is to determine these ODP values and can be influenced by laws, executive orders, or simply the whim of the moment; as if a security amuse bouche, if you will, served by the ordering entity. That could even mean that different ordering activities in the same agency might pick different values for various orders, contracts, or purchases. Presently, there is no uniformity required.

That lack of uniformity complicates Revision 3 when you realize that the 88 ODP gaps are not random; they are sprinkled through more than half of the new 97 security requirements. It's like an Easter egg hunt, but you find uncertainty instead of candy. The map for those gaps is found in Appendix D to Rev. 3, where all of the ODPs are listed by family. Even the briefest of once-overs reflects the variety of choices that are left open and available to agencies, including:

- Additional actions
- Authorities
- Characteristic identifying individual status
- Circumstances
- Circumstances or situations requiring re-authentication
- Composition and complexity rules
- Conditions or trigger events requiring session disconnect
- Conditions requiring rescreening
- Devices or types of devices
- Events or potential indications of events
- Exceptions where remote activation is to be allowed
- Frequency
- Granularity of time measurement
- Numbers
- Personnel or roles
- Requirements for key establishment and management
- Response times
- Security functions
- Security requirements
- Security-relevant information
- System configurations
- Systems security engineering principles
- Time period
- Types of cryptography
- Functions, ports, protocols, connections, and/or services
- Types of system media

That is an unnerving variety of requirements requiring Gumby-like flexibility of the information security specialists, managed security providers, and the contractors they work for. From conditions requiring re-authentication to specific cryptographic rules, each family seems to possess its own set of "gotcha" surprises." For example:

- Requirement 03.06.02—Incident Monitoring, Reporting, and Response Assistance: Contractors must figure out or adjust to the required timing and identity of reporting a cyber incident. With each contractor needing an incident response plan, this variance could impact the effectiveness or uniformity of that necessary plan.
- Requirement 03.05.07—Password Management: Contractors must decide or adjust how often passwords need to be checked and how complex they should be. Again, existing acceptable use policies and fundamental network access protocols will undoubtedly be impacted.
- Requirements 03.13.10 and 03.13.11—Cryptographic Key Establishment and Management/Cryptographic Protection: Contractors are on their own to determine the best practices for key generation and storage, although FIPS-validated is "recommended." However, variance in acceptable or directed cryptologic regiments could wreak havoc on contractor networks.

Notably, as if written with the keenest absurdist humor, out of all the families, the only one without any ODPs is "Maintenance." Ironically, it is the one area that remains constant amidst a sea of variables.

While ODPs are intended to provide flexibility, contractors may get a comedy of errors: trying to guess what the agency wants while keeping their systems secure. It's a heavy lift and feels like performing stand-up with no script—improv at its most chaotic.

Peripeteia—Plot Twist!—For those unfamiliar with the term (as the author was), peripeteia is an abrupt and surprising reversal of fortune or change in circumstances that occurs to the protagonist of a story leading into the denouement. And, as with any well-told tale or joke, contractors are also faced with peripeteia in their efforts to safeguard CUI when, on May 2, 2024, the DOD introduced a class deviation delaying the enforcement of Revision 3 for DOD contracts. Instead of jumping into the latest version, contractors must follow SP 800-171 Revision 2. This deviation to DFARS 252.204-7012 dictates that adherence to the older version is required despite Revision 3 being on the horizon. This plot twist gives the industry more time for a gradual and deliberate transition to the new standards.

For contractors, this deviation period is both a reprieve and a call to action. While immediate compliance with Revision 3 is not yet mandatory, staying ahead of the curve is critical. Reviewing and fortifying compliance with Revision 2 should be the current focus. Simultaneously, preparing for the eventual enactment of Revision 3 is prudent. Understanding and anticipating these future requirements will ensure a seamless transition when the curtain eventually rises on the new standards.

Dénouement—The End-*ish*—Like any hero's journey, the labyrinth of federal cybersecurity regulations has brought contractors to this pivotal moment. Whether or not a contractor views it as the main plot or a simple twist, cybersecurity regulations are no joke. All federal agencies recognize the importance of cybersecurity and are trying to address it, especially concerning CUI. And while the ins and outs of how well each agency is doing in that effort can be comical, it really is no laughing matter for contractors with significant risk and liability on the line. Despite the challenges, NIST 800-171 Rev. 3 aims to make things more straightforward and flexible. While the ODPs may seem like curveballs now, they are intended to help agencies and contractors tailor their security needs. Whether this flexibility will work in harmony or dissonance with contractors remains to be seen. Still, it may be worth the agency's extra effort to define or standardize its ODPs before issuing solicitations. If they do not, or if contractors do not see them, those contractors would be wise to add ODP-related questions in advance of responding to any solicitations promising the presence of CUI but failing to clarify the ODPs it will accept. Contractors cannot and should afford to "wait and see." If they do, they may find the punchline that hits them more than just a little offensive.

Fortunately, DOD's temporary deviation allows time for contractors to solidify current compliance and strategically plan for the future. Contractors who navigate these changes with diligence and foresight will be well-prepared to meet present and future challenges in safeguarding CUI. As this chapter closes, the focus shifts to readiness and resilience, setting the stage for a secure and compliant future.

This Feature Comment was written for The Government Contractor by* Alexander Major. *Mr. Major is a partner and co-leader of the Government Contracts & Global Trade Practice Group at McCarter & English, LLP. He can be reached at amajor@mccarter.com.