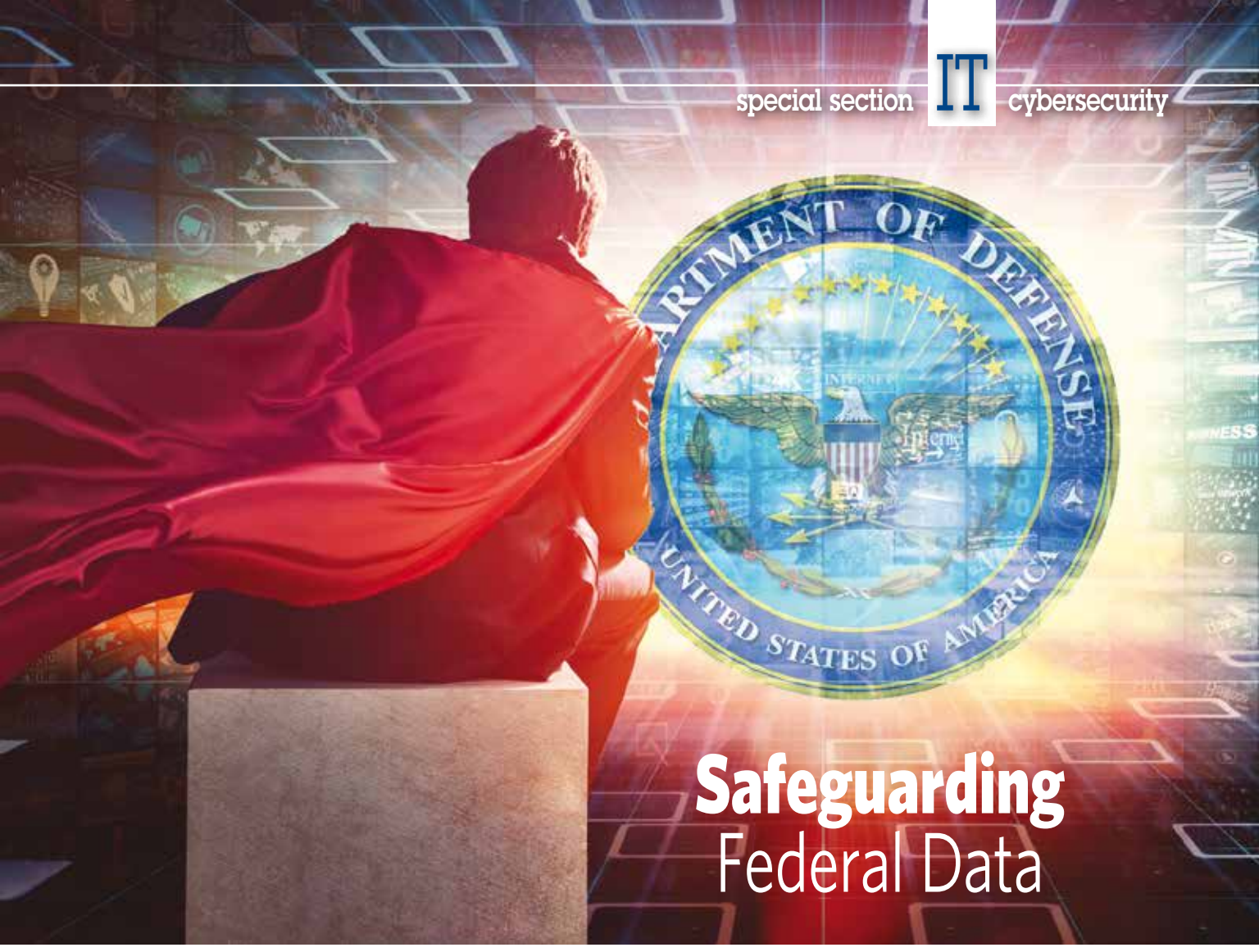


Safeguarding Federal Data

Janel C. Wallace, J.D.

Rules for safeguarding information are increasing in number, as are cyberattacks on federal information. Everyone needs to know about the rules for safeguarding information so their agencies or businesses can comply with them and contracts can continue as planned.

These rules impact everyone, including small businesses, those delivering Federal Acquisition Regulation (FAR) Part 12 supplies and/or services, and contracts below the Simplified Acquisition Threshold (SAT) of $150,000. This article discusses the FAR and other rules instituted to ensure the safeguarding of federal information.

FAR Changes

FAR Subpart 4.19 and FAR Clause 52.204-21 became effective June 15, 2016. FAR Clause 52.204-21 is designed to require a contractor to safeguard some of its information systems as of the date of contract award. FAR Subpart 4.19 and FAR Clause 52.204-21 are attributable both to the changes made in the Federal Information Security Modernization Act of 2014, which provides for additional federal information security requirements, and the Office of Personnel and Management data breach that resulted in the theft of personnel records concerning

Wallace *is a professor of Contract Management at the Defense Acquisition University at Fort Belvoir, Virginia. She is a U.S. Air Force veteran, a former litigation attorney, and a contract specialist. She holds a law degree from the University of North Dakota.*

more than 20 million current and former federal employees and contractors.

The contractor information systems covered ("covered contractor information systems") are defined in FAR Subpart 4.19. They include information systems that a contractor owns or operates that process, store or transmit federal contract information.

What does "federal contract information" mean, specifically? It is summarized as the kind of contract information that the government has no intention of releasing to the public. It is information provided by or generated for the government under a contract to develop a product for or service to the government. It excludes information provided by the government to the public or simple transactional information.

Application of the Rule

FAR 52.204-21 should be added to a solicitation so that offerors are made aware of the safeguarding requirements that could apply to the contract. FAR 4.1903 requires insertion of FAR Clause 52.204-21 when a contractor or subcontractor at any tier may have federal contract information residing in or transiting through its information system. The focus of FAR 52.204-21 is on the information system(s) and not the information itself. That focus makes it unnecessary to specifically identify what information was created or compiled for the government or to decipher specifics about each set of information in a contract to determine its applicability to FAR 52.204-21.

Since the safeguarding requirements apply even in the case of a mere possibility of federal contract information residing in or transiting through a contractor's or subcontractor's information system, it is the responsibility of the government's technical team to assess that possibility in drafting the contract requirements. The government's technical team is relied upon instead of the contracting officer because the government team generally is more familiar with the information and information systems required by the contract.

Pursuant to FAR 7.105(b)(18), the acquisition plan must discuss compliance with FAR 4.19 when addressing the requirement's security considerations if federal contract information may be residing or transiting through the contractor's information systems.

Exceptions to the Rule

Use of FAR 52.204-21 is not required when the procurement involves availale, commercial off-the-shelf (COTS) items; the information has already been made public by the government; or when the information is simple transactional information such as that needed to process payments. COTS items were excluded as COTS is considered unlikely to include even the possibility of federal contract information residing or transiting through a contractor information system. The government inherently does not have an interest in protecting information that is already available to the public. The government also does not have an interest in protecting simple transactional information since doing so may make the rule overbroad.

There are no exceptions to the safeguarding rule when contracts fall below the SAT because many acquisitions below the SAT may still involve a government interest that requires safeguarding. There are no exceptions to contracts falling under FAR Part 12 since information may need to be safeguarded despite the use of Part 12, particularly since Part 12 may utilize policies and procedures from other FAR parts.

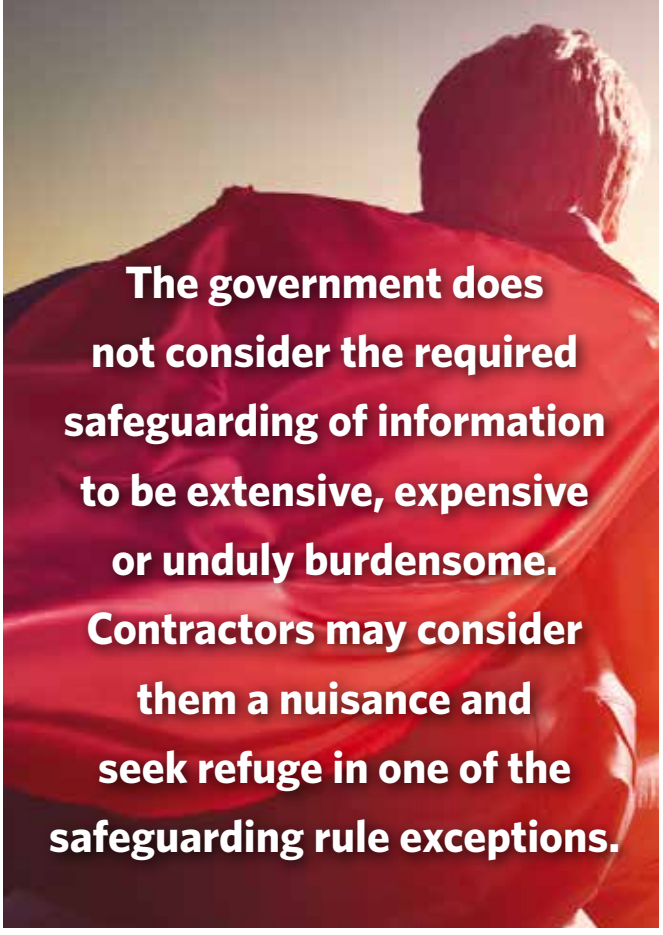
The government does not consider the required safeguarding of information to be extensive, expensive or unduly burdensome. Contractors may consider them a nuisance and seek refuge in one of the safeguarding rule exceptions. For instance, the COTS exception may result in contractors and subcontractors clamoring to categorize their supplies and/or services as COTS items to avoid the safeguard requirements. But contractors and subcontractors should realize that the government expects reduced prices for COTS supplies and services presumed to be sold in sufficiently large market quantities.

At present, it may not seem worthwhile for contractors to attempt to categorize their products or services as COTS. It may, however, become worthwhile as more stringent safeguarding requirements are developed.

Background

Implementing FAR 4.19 and FAR Clause 52.204-21 are just two steps in a series of coordinated regulatory actions taken to strengthen protection of information systems. In May 2015, the National Archives and Records Administration (NARA), which was designated by Executive Order 13556 to implement the Controlled Unclassified Information (CUI) Program, issued a proposed rule to guide agencies and contractors in designating, safeguarding, disseminating, marking, decontrolling and disposing of CUI that is not classified but also not intended for public disclosure. Only that information requiring safeguarding and dissemination controls pursuant to federal law or regulation and/or government-wide policy can be designated as CUI. Another focus of the CUI program is to prevent inconsistent markings and unnecessary restrictions.

On Sept. 14, 2016, NARA issued its final rule on CUI. NARA explained that the purpose of the program is to establish uniform requirements on how every agency handles each type of CUI. There are two types of CUI, basic and specified, which are now better defined. CUI that doesn't provide specific protections in law, regulation or government-wide policy will fall into the basic category. The basic category provides the minimum controls and is where the majority of CUI will fall. NARA established and now maintains a CUI registry, which is the central location for guidance, policy, instructions and information pertaining to CUI.



NARA and the National Institute of Standards and Technology (NIST) together developed guidelines on how controlled unclassified information should be protected when not under direct federal control. As a result, NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations was created in June 2015. NIST SP 800-171 provides agencies with recommended basic requirements for CUI. The FAR does not have direct references to NIST. However, it does require (in FAR 52.204-21) that contractors consider other safeguarding requirements applicable to the contract.

The Department of Defense (DoD), abiding by NARA's policy, implemented a rule though a revision of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. This revision resulted in a direct reference to the use of NIST SP 800-171 for systems that are not part of an information technology service or system operated on behalf of the government. The contractor is told in 252.204-7012 to implement NIST SP 800-171 no later than Dec. 31, 2017. A nonfederal organization collecting or maintaining information on behalf of the government or operating or using systems on behalf of the government must follow the Federal Information Security Modernization Act, which includes the minimum security requirements of *Federal Information Processing Standards (FIPS) Publication 200* and SP NIST 800-53. Both are viewed as comparatively more burdensome than NIST SP 800-171. NIST SP 800-171 is a blend of NIST SP 800-53 and *FIPS Publication 200.* The use of NIST SP 800-171 may not satisfy the requirements of NIST SP 800-53 and *FIPS Publication 200*, which are more specific and stringent and do not generally apply to contractor systems.

The DoD interim rule also created DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," and DFARS 252.204-7009, "Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information." DFARS 252.204-7008 provides that, by submitting an offer, a contractor represents that it will implement the NIST SP 800-171 in effect at the time of the solicitation. DFARS 252.204-7008 also affords an offeror the opportunity to propose an approach that is different from any of the NIST SP 800-171 security requirements. If the different approach is approved by the DoD Chief Information Officer, it becomes part of the contract.

DFARS 252.204-7009 requires that a contractor agree to limit its use of cyber-incident information received from a third party in assisting or advising the government and not for any other purpose. In signing the contract, the contractor agrees to protect the information against disclosure or release and to ensure that its employees are subject to use and non-disclosure obligations prior to receiving access to the information. Penalties may be assessed against a contractor for violating the agreement. The third party reporter also would be empowered to seek civil damages and other remedies from a contractor that violates the agreement, making this clause exceptional by extending protection to a noncontractual party.

The safeguarding of information is not a new concept, particularly for the DoD, which issued an interim rule in February 2014 that resulted in creation of DFARS 204.74, "Disclosure of Information to Litigation Support Contractors." A final rule was issued on May 10, 2016, making it clear that a litigation support contractor will respond to a contracting officer's request upon completion of the litigation support by destroying or returning to the government all related litigation information in its possession. The final rule also makes it clear in DFARS 252.204-7014, "Limitations on the Use or Disclosure of Information by Litigation Support Contractors," that a contractor will not disclose any litigation information outside the contractor's organization without the contracting officer's written permission. "Sensitive information" is defined by DFARS 204.7401 and includes CUI of a commercial, financial, proprietary or privileged nature. Like the "federal contract information" definition of FAR 4.1901, "sensitive information" does not include information that is otherwise publicly available.

All the aforementioned DFARS clauses contain flow-down language requiring inclusion of each DFARS clause in subcontracts at any tier where required. FAR 52.204-21, although not specific to CUI like the aforementioned DFARS clauses, shares in the required flow-down language so that the

substance of the clause (including the flow-down language) must be inserted in subcontracts when the subcontractor might have federal contract information within or transmitted through its information system(s).

Review of Rule Comments

The government responds to public comments on rule proposals. The responses to the then proposed rule 52.204-21 make it clear that more stringent rules are forthcoming on safeguarding information, particularly for CUI. Sixteen respondents commented on the FAR rule. The Civilian Agency Acquisition Council and Defense Acquisition Regulations Council (hereinafter referred to as "the Councils") reviewed the comments as the councils were developing the final rule. Some of the considerations given to the comments are noteworthy. There were many concerns expressed in the comments about the proposed rule's clarity. In responding, the councils opted for simplification in what apparently was an effort to avoid delay in implementing the rule. The councils opted to make the rule very broad, particularly as compared to its draft version, to avoid regulating in confusing specific terms.

The councils appeared to seek buy-in or acceptance of the idea that they simplified the rule enough to avoid hurting small businesses. The councils indicated their belief that the rule provides the most basic safeguards that a prudent business person would exercise even if the rule did not exist. A review of FAR Clause 52.204-21 appears to indicate that the minimum requirements are far from being egregiously prohibitive.

If the impacts change due to more stringent regulation, there may be an adverse effect not only on small businesses but on the competitive environment. In that case, there would be an increase in both the actual costs that offerors will pass on to the Federal Government and in costs directly attributed to decreased competition. The question then would shift to whether the information-safeguarding rules are worth the government's overall cost of implementing and enforcing them. It may ultimately be left to the contracting officer's discretion to determine whether the federal contract information involved needs the stringent safeguards or instead can be protected by the minimal safeguards of the current FAR 52.204-21.

Other comments on the FAR rule expressed concern that the rule would not be in conformity with the NIST's requirements. One comment suggested that the councils wait pending the final NARA rules pursuant to Executive Order 13556. The councils recognized the validity of the concerns expressed but declined to await the final NARA rule. The Councils instead indicated that they would stipulate through FAR 52.204-21 that contractors are not relieved of the requirement to abide by any other specific safeguarding requirements (i.e., from the NIST), including those for CUI as established by Executive Order 13556.

Other areas of concern regarded the conveying of information via e-mail, voice, fax, text messages and blogs. The councils considered these communication media as being out of scope with the current rule. The focus was intended to be on the information systems as opposed to the information itself. This may be confusing to some, since the type of information conveyed would seem to define what information systems are covered. According to Title 44 U.S. Code Section 3502, an information system is defined in part as including information resources organized for processing, sharing and disseminating information. In considering what constitutes an information system, it would appear that e-mail, fax, text messages and blogs indirectly fall under the requirements of information systems from which they are delivered if the information sent might contain federal contract information. It is important to remember that it is the information system that is regulated rather than the information itself, and that a contractor must put forth a good faith effort to protect its systems.

Conclusion

It is important to know how the rules for safeguarding information affect your agency regardless of whether the rule falls under NIST, DFARS or FAR. The councils made it clear that more stringent rules are on the horizon. The protection of federal information requires that we are neither too relaxed about disclosing our information nor too stringently regulatory. The balance may shift to one side or the other, depending upon the future level of cyberattacks and technology development.

The author can be contacted at **janel.wallace@dau.mil**.