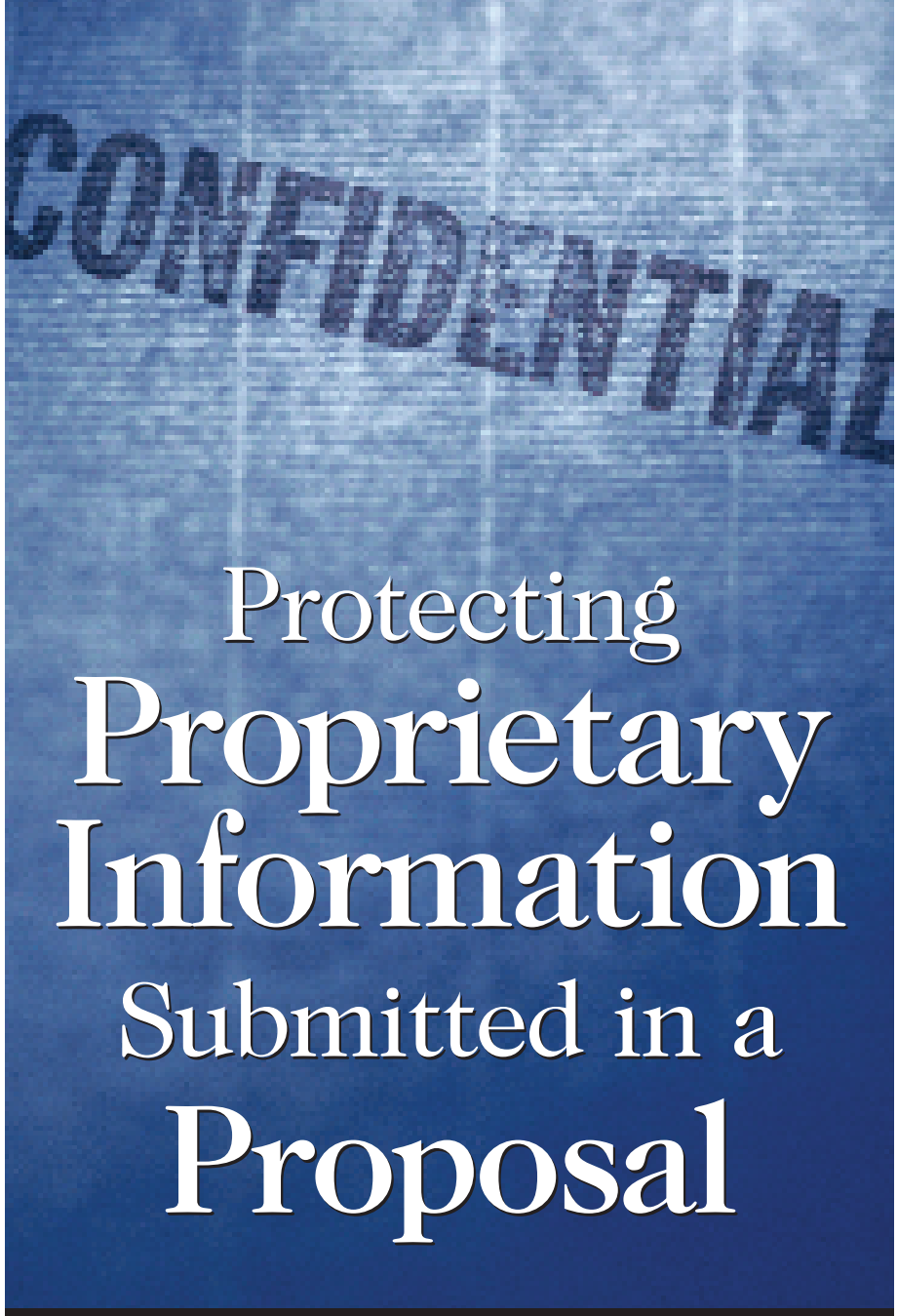


# Protecting Proprietary Information Submitted in a Proposal

**Explore the methods available to prospective contractors to protect proprietary information submitted to the government from unauthorized use or disclosure.**

BY PATRICIA A. MEAGHER AND MARK A. KAHN

In proposing to do business in the commercial world, companies frequently find themselves in the position of having to disclose confidential information and proprietary data in order to win business. Companies may be requested, for example, to turn over mission-critical data to potential customers—the disclosure of which to competitors or the general public might severely impact the company's competitive edge, as well as hamper its efforts to succeed in the marketplace.

Fortunately, in the commercial environment, the parties are free to negotiate whatever contractual arrangements are necessary and appropriate to protect confidential information and proprietary data. Commercial entities are also provided with access to the courts to enforce such agreements, to prevent the disclosure of proprietary data, and to collect damages in the event of unauthorized use or disclosure.

In contrast, when a company is seeking to do business with the federal government, the rules of engagement are, for the most part, laid out in statutes and regulations rather than negotiated. As a result, companies are put on notice from the outset as to what is, and is not, acceptable to the government. Moreover, since these rules are in large part non-negotiable, a company seeking government business must either assume some level of risk or decide to forgo opportunities to contract with the government.

This article explores the methods available to prospective contractors to protect proprietary information submitted to the government from unauthorized use or disclosure.

In addition, the article discusses the inherent risks associated with submitting proposals (whether solicited or unsolicited) to the government.

**About the Authors**

**PATRICIA A. MEAGHER, ESQ.,** and **MARK A. KAHN, ESQ.,** are attorneys with Rogers Joseph O'Donnell and Phillips in San Francisco, California. Send comments on this article to **cm@ncmahq.org**.

## Government Obligations

Federal statutes and agency regulations provide the first layer of protection for proprietary data contained in technical, management, or cost proposals (referred to collectively as "proposals") by regulating the conduct of government officials and employees who receive such information from prospective contractors.

Under the Trade Secrets Act,[1] it is a criminal offense for a federal government official or employee to disclose trade secret or confidential commercial or financial data "to any extent not authorized by law."[2] A "trade secret" under this statute is defined as

> any formula, pattern, device, or compilation of information that is used in one's business, and gives him an opportunity to obtain an advantage over competitors who do not know or use it.[3]

This act applies to proprietary information contained in proposals.

Although there have been few prosecutions of government officials or employees for violations of the act, the severe sanctions provided for in the statute, including fines and imprisonment, operate as a deterrent to wrongful conduct. The Economic Espionage Act of 1996[4] also protects proprietary information by imposing criminal sanctions for misappropriation or theft of trade secrets by any person (not limited to government officials and employees).

Further, the Procurement Integrity Act prohibits federal procurement officials from disclosing bid or proposal information to any person other than those persons authorized to receive such information. Bid or proposal information includes cost or pricing data, indirect costs, direct labor rates, and properly marked proprietary information concerning manufacturing process, operations, or techniques.[6] The prohibitions of the Procurement Integrity Act, however, apply only during the procurement process and do not continue after contract award or cancellation of the procurement.

In addition, the *FAR* requires that government officials secure all bids—including modifications—until bid opening,[7] and safeguard all proposals from unauthorized disclosure throughout the source selection process.[8]

While these provisions guard against the unauthorized use or disclosure of proposal information by government officials and employees, offerors and other prospective contractors should take additional steps (described on page 22) to protect more fully proprietary data submitted with a proposal.

## Protecting Data in an RFP

Offerors responding to a competitive solicitation are permitted to mark data included in their proposals with a restrictive legend. The legend restricts the disclosure and use of the data by government personnel to the evaluation of the proposal. Specifically, paragraph (e) of the standard request for proposal (RFP) provision "Instructions to Offerors—Competitive Acquisitions" (Jan 2004), FAR 52.215-1, provides that offerors seeking such a restriction on the disclosure and use of their data

should take two steps. First, the offeror should mark the title page of its proposal with the following legend.

. . . . . .

This proposal includes data that shall not be disclosed outside the government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets [*insert numbers or other identification of sheets*].

. . . . . .

Second, the offeror should mark each sheet in its proposal containing data it wishes to restrict with the following legend:

. . . . . .

Use or disclose the data contained on this sheet is subject to the restriction on the title page of this proposal.

. . . . . .

Note that the *FAR* legends do not acknowledge that the information marked by the offeror is proprietary. Rather, the legends simply limit the disclosure and use of the data by government officials and employees to proposal evaluation. In addition, as noted in the *FAR* legend itself, the government's right to use or disclose the data *after contract award* is governed by the clauses incorporated into the contract rather than the legend.

Offerors submitting proposals to the Department of Defense (DOD) should also be aware of DOD's policy governing disclosure and use of proprietary proposal data. Specifically, DOD regulations provide that, by submitting the proposal, the offeror agrees that DOD may reproduce and use proposal information for evaluation purposes.[9] The regulations also advise that subsequent to contract award, the government shall have the right to disclose and use proposal information within the government, and outside the government with the contractor's written permission.[10]

Additionally, NASA has its own policy with regard to proposals submitted in response to NASA Research Announcements.[11] This policy provides that a proposal will be used for evaluation purposes only and will be protected by NASA "to the extent permitted by law." NASA also instructs offerors to insert the following notice on the title page of the proposal.

. . . . . .

NOTICE—RESTRICTION ON USE AND DISCLOSURE OF PROPOSAL INFORMATION

The information (data) contained in [*insert page numbers or other identification*] of this proposal constitutes a trade secret and/or information that is commercial or financial and confidential or privileged.

It is furnished to the government in confidence with the understanding that it will not, without permission of the offeror, be used or disclosed other than for evaluation purposes; provided, however, that in the event a contract (or other agreement) is awarded on the basis of this proposal the government shall have the right to use and disclose this information (data) to the extent provided in the contract (or other agreement). This restriction does not limit the government's right to use or disclose this information (data) if obtained from another source without restriction.

. . . . . .

Similar protection is afforded proposals submitted in response to a NASA Announcement of Opportunity.[12]

## Protecting Data in an Unsolicited Proposal

Government agencies also receive unsolicited proposals from potential contractors setting forth new and innovative ideas that have not been the subject of a government-initiated solicitation. Agencies are required to establish procedures for the evaluation of unsolicited proposals and for the control and protection of material submitted in conjunction with the unsolicited proposals.

The *FAR* recognizes that, like responses to an RFP, unsolicited proposals may include data that should not be disclosed to the public or used by the government for any purpose other than proposal evaluation.[13] Further, the *FAR* provides an offeror submitting an unsolicited proposal the same opportunity to limit the use or disclosure of data as provided to an offeror responding to an RFP.

Specifically, offerors submitting unsolicited proposals can mark the title page of the proposal and each sheet of the proposal that it wishes to have protected with the same legends noted earlier.[14]

If the offeror includes a legend that differs from the legends set forth in the *FAR*, the agency point of contact is directed to return the unsolicited proposal to the offeror without evaluation.[15]

## Protecting Data from Release Under FOIA

The *FAR* legends noted earlier impose restrictions on the government's use or disclosure of proposal data. But, the *FAR* legends do not protect information or data submitted with a proposal from release or disclosure under the Freedom of Information Act (FOIA), 5 U.S.C. § 552. Enacted in 1966, FOIA gives *any person,* including a competitor, the right to request access to company documents in the possession of a federal agency.

Since 1997, civilian agencies and DOD have been prohibited by statute from releasing under FOIA proposals submitted in response to a competitive procurement.[16] While this statute affords great protection, its application

is limited. For example, the statute does not apply to NASA. The statute also does not apply to any proposal that is set forth or incorporated by reference into a contract between the government and the party submitting the information. In addition, the statute does not apply to unsolicited proposals. It is therefore recommended that, notwithstanding this statute, all offerors continue to mark their proposals in the manner discussed below to invoke the applicable FOIA exemption and protect proprietary information from disclosure to the public.

### *Trade Secrets and Confidential Information*

In order to be protected from disclosure in response to a FOIA request, the information or data submitted with a proposal must fall within one of the exceptions set forth in the statute. The most common exemption relied on by offerors and government officials seeking to protect proposal data from public disclosure is the FOIA's exemption for "trade secret" and "privileged or confidential commercial or financial information." This exemption is commonly referred to as "Exemption 4."

Under this provision, trade secret is defined as "a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort."[17] Further, commercial or financial information is within the FOIA exemption if it is confidential. In this regard, confidential means that the information is not customarily released to the public and the release would cause competitive harm or would impact the government's ability to obtain such information in the future.

In its application, Exemption 4 does not protect the total price of the contract from public disclosure, but it has been applied to preclude the release of overhead factors, cost figures, and profit and line-item pricing information, where the release of information would likely cause substantial competitive harm.[18]

Since the government disfavors any modification or change to the *FAR* legends for marking the proposal title page and proposed sheets, the best practice is for an offeror to mark its proposal with the *exact* legend proscribed in the *FAR* and then mark the proposal separately and distinctly with the FOIA legend. A suggested additional legend is:

. . . . . .

This proposal contains trade secret and confidential business or financial information exempt from disclosure under the Freedom of Information Act.

. . . . . .

### *Exemption for Critical Infrastructure Information*

In 2002, Congress passed the Homeland Security Act, which, among other things, created a new FOIA exemption. In particular, the act exempts from disclosure.

> Critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose….[19]

When Congress created this exemption, a number of critics contended that the exemption has the potential to shut down public access to vast amounts of information. In this regard, 42 U.S.C. § 5195c(e) defines "critical infrastructure" quite broadly:

> The term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The definition leaves open to argument what systems and assets are so crucial that their destruction would have a debilitating impact on the security of the country.

Because the statute is less than two years old it remains to be seen how broad the exemption truly is. In this regard, the Department of Homeland Security (DHS) is in the process of implementing regulations relating to the critical infrastructure exemption. Notably, in an interim rule published earlier this year, DHS acknowledged and justified the breadth of the definition of "critical infrastructure," stating that it "provides the appropriate degree of flexibility necessary to further promote information-sharing by providing submitters with an opportunity to provide the information they believe meets the definition and should be protected."[21]

As discussed earlier, it is important that the offeror mark proprietary information appropriately. In the case of proposals submitted to DHS, the offeror must include the following legend (for written information):

. . . . . .

This information is voluntarily submitted to the federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.

. . . . . .

For information submitted verbally, the submitter must provide a written statement regarding the expectation of nondisclosure within a reasonable period following the verbal communication.[22]

## Exemption for CRADA Information

Another exemption relevant to protecting proprietary information relates to Cooperative Research and Development Agreements, or CRADAs. A CRADA is an agreement

between a federal laboratory (e.g., Los Alamos or Lawrence Livermore) and a private party to engage in joint research and development efforts.

The exemption does not specifically protect information submitted in a proposal, but rather precludes the disclosure of trade secrets or commercial or financial information that is privileged or confidential that is obtained by the government pursuant to a CRADA.[23] It also provides that trade secret/confidential information that is developed through the performance of a CRADA may be withheld for up to five years.

## Nondisclosure Agreements

On occasion, a prospective contractor may request that a government agency, before the submission of information or an unsolicited proposal, enter into a nondisclosure agreement. This agreement typically sets forth the specific purpose for which the proprietary information is provided, prohibits the use of the information for any other purpose, and sets other conditions such as limited circulation of the data, a restriction on the number of copies that can be made, and procedures for the return or destruction of the data within a set time.

A prospective contractor's success in negotiating such an agreement with a government agency will depend, of course, on the agency's interest in receiving the information or evaluating the unsolicited proposal. It is not uncommon for government officials to simply refuse to enter into a nondisclosure agreement, claiming that federal statutes and regulations adequately protect proprietary information from unauthorized use or disclosure.

The only regulation addressing nondisclosure agreements is DFARS 227.7103-7, which requires the execution of a "Use and Non-Disclosure Agreement" before any disclosure of technical data or computer software delivered to the government with restrictive markings to a third-party recipient.

## Debriefings

Another event in the competitive bidding process that poses some risk for the disclosure of an offeror's proposal data is the post-award debriefing of offerors. By law, any successful offeror that has received notification of a contract award may request a debriefing by the agency.[24] The debriefing provides the offeror information, including the overall evaluated cost and technical ranking of awardees, and a summary of the rationale for the award decision. The debriefing is *not* to reveal information protected from disclosure under FOIA including trade secrets, privilege or confidential manufacturing processes and techniques, and commercial and financial information that is privileged or confidential including cost breakdowns, profit, indirect cost rate, and similar information.

## Enforcing Your Right

On occasion, a federal government agency and an offeror may disagree as to the portions of the offeror's proposal that are releasable to competitors and other members of the public, or as to the timing of the release.

In those instances where the agency and the offeror are unable to reach agreement on the timing and extent of the release of an offeror's proposal, the offeror's legal remedy is to file an action in federal district court seeking an injunction against the release of its proprietary data by the federal agency.

In such an action, the offeror must establish that release of the information would be in violation of a statutory or regulatory provision, such as the Trade Secrets Act, the Procurement Integrity Act, or the FOIA exemption for the trade secret and confidential commercial and financial information. Assuming the offeror makes such a showing to the court's satisfaction, the agency will likely be enjoined from disclosing the information.

## Conclusion

Offering to do business with the government frequently involves the submission of proprietary information to the government. It is critical that prospective contractors be cognizant of what the government's rights and obligations are with respect to that information, as well as the steps that offerors must take to protect that information. Of course, protecting information at the proposal stage is only the beginning—once a company actually contracts with the government, a whole different set of rules apply. ***CM***

### Endnotes

1. 18 U.S.C. § 1905.
2. Ibid.
3. *Kewanee Oil Co. v. Bicron Corp.,* 416 U.S. 470 (1974).
4. 18 U.S.C. § 1831.
5. 41 U.S.C. § 423; FAR 3.104.
6. FAR 3.104-1.
7. FAR 14.401(a).
8. FAR 15.207.
9. DFARS 252.227 – 7016(b).
10. DFARS 252.227 – 7016(c).
11. NASA FAR Supplement 1852.235-72.
12. Ibid., 1872.705-1.
13. FAR 15.608(b).
14. FAR 15.609(a) – (b).
15. FAR 15.609(c).
16. 41 U.S.C. § 253b(m); 10 U.S.C. § 2305(g).
17. *Public Citizen Health Research Group v. FDA,* 704 F.2d 1280, 1288 (D.C. Cir. 1983).
18. *McDonnell Douglas Corp. v. NASA,* 180 F.3d 303 (D.C. Cir. 1999).
19. 6 U.S.C. § 133(a)(1)(A).
20. 69 Fed. Reg. 8073 (Feb. 20, 2004).
21. Ibid., 8076.
22. 6 U.S.C. § 133(a)(2).
23. 15 U.S.C. § 3710a(c)(7).
24. 41 U.S.C. § 253b(e).