BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

# Managing Intellectual Property Issues With The U.S. Government: A User's Guide

*By Steven M. Masiello, Tyson J. Bareis, and Joel M. Pratt**

Commercial organizations often disclose intellectual property (IP) to customers and prospective customers, including the U.S. Government. Whether it is selling a prototype or mature product, licensing software, disclosing specifications to potential customers, developing and managing a supply chain,[1] or acquiring development services from third parties, commercial organizations may find it necessary to submit even the most sensitive IP for review.

Paradoxically, the same IP that may be subject to routine disclosure also may constitute highly sensitive information to the organization that owns the IP. This is due to the central role that IP plays in today's competitive marketplace and the fact that, once an organization loses control of its IP, reestablishing control is challenging.

The question, then, is: How can organizations effectively manage their IP in light of the differing legal regimes surrounding IP relevant to commercial and Government customers, prospective customers, and other third parties?

The short answer is: very carefully. The law affords various protections to organizations that develop and/or disclose IP. However, these protections rely on compliance with complex contractual, statutory, and regulatory regimes, particularly when an organization develops and/or discloses IP in transactions or exchanges with the Government.

This BRIEFING PAPER examines the legal landscape and best practices relevant to managing IP, particularly in the context of business dealings with the U.S. Government. It focuses on the U.S. Government not because the Government necessarily is more likely to use or disclose an

*Steven M. Masiello is a Partner with Dentons where he specializes in Government contracts. Joel Pratt is an associate with Dentons. The views expressed herein do not necessarily reflect the views of Dentons or its clients. Tyson Bareis is in-house counsel at Sierra Nevada Corporation. The content of this Briefing Paper represents Mr. Bareis' personal opinions and not the opinions or position of Sierra Nevada Corporation.

IN THIS ISSUE:

organization's IP improperly. Instead, this PAPER focuses on IP developed or disclosed in transactions or exchanges with the Government because such activities present the most complex environment for effectively managing IP issues. The environment is complex because the U.S. Government is subject to its own set of laws and regulations concerning the collection and distribution of information. Navigating both the standard legal protections for IP and the special Government rules is challenging.

The PAPER begins with a discussion of the fundamentals of IP protection, both generally and in the context of disclosures made to the Government. The PAPER next discusses an organization's options when the Government improperly uses or discloses sensitive IP. Finally, the PAPER identifies best practices for protecting IP in Government procurement and non-procurement contexts.

## Basic Principles Of IP & IP Protection

This BRIEFING PAPER is not intended as a primer on IP. Nevertheless, any discussion of IP protection must necessarily begin with a discussion of the nature of IP and how U.S. law protects IP.

### Patents

U.S. law permits individuals to patent processes, machines, manufacturing methods, or compositions of matter, or any improvement thereof, that are new, useful, and nonobvious.[2] If a patent is granted, the patent holder may prevent others from making, using, or selling the invention in the United States for a set period of time, usually 20 years.[3]

The U.S. Government is authorized to make use of, or have use made of, any U.S. patent, with the sole remedy to the patent owner being the payment of reasonable compensation.[4] Standard Government contract clauses often authorize Government contractors to take such actions on behalf of the U.S. Government.[5] In effect, this means that the U.S. Government and its contractors, in certain circumstances, have the right to use a patented invention, regardless of the patent holder's ability to prevent other individuals from using the invention.

### Copyrights

U.S. law grants copyright protection to original works of authorship, including literary works; musical works; pictorial, graphic, and sculptural works; motion pictures and other audiovisual works; sound recordings; architectural works; and compilations of existing works.[6] Copyright protection also extends to software code.[7] Importantly, a copyright protects only the physical embodiment of a work (i.e., the way in which the author chose to arrange and present the work); it does not protect the concepts or ideas underlying the work.[8]

Unlike patent rights, copyrights attach to a work automatically upon the creation of that work.[9] Subject to some exceptions, a copyright holder has the exclusive right to reproduce, sell, prepare derivative works from, perform, or display the work.[10] If another party infringes on a copyright, the copyright holder is entitled, among other things, to seek an injunction preventing the infringement and to seek damages (actual or statutory) from the infringing party.[11]

Editor: Valerie L. Gross



*Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.*

As in the case of a patent, the Government can infringe upon an entity's copyright, or direct its contractors to do so, and the sole remedy of the copyright holder is a suit for damages against the Government.[12]

### Trade Secrets

While there are many definitions of the term "trade secrets," the concept generally covers nonpublic information that derives economic value from its secrecy.[13] Trade secrets can include many types of information, including internal processes, policies, financial and accounting information, business development information (such as customer lists), technical approaches, nonpublic product information and capabilities, and any other valuable, nonpublic company information.

Unlike the other types of IP discussed in this section of the PAPER, trade secret protections generally arise out of state law. As a result, there is no single legal structure from which to determine the contours of trade secret protections. Nevertheless, there are legal protections in place in state and federal law designed to regulate the unfair use or disclosure of an organization's trade secrets. At the federal level, for example, trade secrets receive protection under the Trade Secrets Act (TSA)[14] and the Freedom of Information Act (FOIA).[15] Moreover, every state has instituted some level of protection for trade secrets maintained in confidence by an organization. Each of these protections is discussed later in this PAPER.

### Trademarks

A trademark is a word, name, symbol, or device (or combination thereof) used to distinguish the source of a particular good or service.[16] Like copyrights, ownership of a trademark is established upon use of the mark.[17] In many jurisdictions, including the United States, trademark holders can register their trademarks as a means of obtaining enhanced protections under the law.[18]

The Government typically does not take ownership in or a license to contractor trademarks, unlike the other categories of IP discussed in this section of the PAPER.[19]

## Statutes & Regulations Applicable To IP Developed With &/Or Submitted To The Government

Information, including IP, that an organization develops with and/or submits to the Government becomes subject to a variety of potentially overlapping statutory and regulatory requirements. At the highest level, these requirements attempt to strike a balance between a private entity's right to restrict the use and further disclosure of IP, the Government's need to use and disclose the IP, and the public's right to access information held by the Government.

These sometimes conflicting goals are implemented through various legal authorities, including FOIA, the TSA, and the Procurement Integrity Act (PIA), as well as Government contracting IP licensing laws and regulations. The application of these authorities, which are discussed in detail in the next two sections of the PAPER, gives management of IP developed with or submitted to the Government a degree of complexity far above ordinary improper use and disclosure issues arising from activities with private entities. Understanding these complexities is essential to managing the IP that an organization develops with and/or submits to the Government.

### Freedom Of Information Act

The primary law governing how the U.S. Government discloses to the public recorded information in the Government's custody and control is FOIA.[20] FOIA is premised on the concept that Government records must be publicly disclosed so that the general public can determine what its Government is "up to."[21] Thus, FOIA requires federal agencies to (1) disclose automatically certain records to the public, and (2) disclose upon request other agency records to the public.[22]

FOIA's focus is on agency records (i.e., recorded information). FOIA does not require agencies to create or disclose records that do not already exist.[23] FOIA also does not require agencies to obtain or to disclose records that are not within the agency's control at the time of the request.[24]

Certain categories of information are exempt from

 

disclosure under FOIA.[25] Among other things, FOIA exempts from disclosure trade secrets and privileged or confidential commercial or financial information.[26] If a Government record contains such information, FOIA requires the Government to confer with the submitter of the information to determine what can be released.[27] If the Government intends to release information over a submitter's objection, the submitter can appeal the anticipated release through a lawsuit in a federal district court.[28]

Despite the protections that FOIA provides to owners of information submitted to the Government, abuses can occur and may be difficult to correct. First, while most Government employees are aware of FOIA's requirements, individual Government employees may not think of FOIA as prohibiting disclosure of records in response to nontraditional requests (i.e., requests that are not clearly framed as FOIA requests). Thus, Government employees may commit an improper disclosure by informally disclosing certain Government records without going through the exemption processes set forth in FOIA.

Second, if the Government fails to follow FOIA, the rights of the entity owning the improperly disclosed information are limited. For example, in 2010, the U.S. Army released under FOIA certain sensitive contractor information concerning the contractor's trade secrets and unit pricing.[29] Because FOIA does not include a civil right of action against the Government in the event of an improper disclosure, the contractor initiated an action against the Army for violation of the Administrative Procedure Act (APA). This approach handicapped the contractor because the standard for Government wrongdoing under the APA is high (actions must be arbitrary, capricious, or contrary to law)[30] and because the remedies available ordinarily do not include monetary damages.[31] In the referenced case, the contractor and the Government settled; however, the lack of a clear right of action against the Government for improper disclosures under FOIA weakens the overall protections available to submitters of sensitive IP information.

### Trade Secrets Act

The federal TSA prohibits Government employees from disclosing information concerning or relating to a private party's "trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures."[32] The TSA makes such actions a criminal offense and subjects the disclosing individual to removal from office and fines or imprisonment.[33]

While the TSA is a key tool in preventing the inappropriate Government disclosure of non-Government information, it can only be enforced by the Department of Justice.[34] Thus, a private entity that believes the Government has inappropriately disclosed its information cannot bring a suit against the Government or the disclosing Government employee under the TSA. The TSA, therefore, remains more of a deterrent to Government employees inappropriately disclosing IP than an effective remedy for an organization that has had its IP inappropriately disclosed.

### Procurement Integrity Act

The PIA contains various requirements for individuals (including Government officials) participating in the procurement process.[35] The PIA creates criminal and civil penalties for the disclosure of certain potentially sensitive contractor IP, including "contractor bid or proposal information or source selection information before the award of a Federal agency procurement contract to which the information relates."[36] The PIA defines "contractor bid and proposal information" as including nonpublic information relating to (1) cost or pricing information; (2) indirect cost information; (3) proprietary information about manufacturing processes, operations, or techniques marked by the contractor in accordance with applicable law or regulation; or (4) information appropriately marked as "contractor bid or proposal information."[37]

The PIA represents a well-known and well-observed limitation on the Government's ability to disclose information belonging to private parties. As noted above, the restrictions of the PIA are only in place until the award of the procurement to which the information relates.[38] That said, the other statutory and regulatory regimes discussed in this section continue to protect

 

most information covered by the PIA after a contract award.

Like FOIA and the TSA, the PIA does not provide harmed entities with the ability to sue the Government or its employees in the event of a violation.[39] Thus, a private party cannot recover damages or receive an injunction against the Government under the PIA in the event of an improper disclosure of covered information.[40]

## Government Contracting IP Licensing Laws & Regulations

The statutory authorities discussed so far address the Government's ability to disclose information that an organization has submitted or disclosed to the Government. However, the Government has a different set of statutory and regulatory rights in information that it develops with a contractor or otherwise acquires as part of a procurement.

The Government's rights in IP that it has acquired or helped create tend to be broader, reflecting the fact that the Government has aided in some capacity with the development of the IP; it has not simply come into possession of the IP. In some instances, the Government receives a license to contractor IP that is broad enough to enable the Government to use the IP or disclose the IP to the general public. When such a license exists, the contractor IP at issue may no longer be protected by the statutory authorities discussed above. Thus, understanding the Government's rights in IP created or delivered during contract performance is essential to understanding the Government's ability to disclose certain categories of contractor IP.

Standard Government contract clauses set forth the rights that the Government will receive in IP related to a Government procurement. Individual Contracting Officers (COs) generally cannot deviate from these clauses. A contractor or potential contractor must read the contract carefully to understand fully the requirements of a Government contract and the implications of those requirements on the Government's ability to use or disclose contractor IP.

### Rights In Patents

Federal law entitles the Government to take ownership of most patentable inventions first conceived or actually reduced to practice during the performance of a Government contract.[41] Most agencies (with some notable exceptions, such as NASA[42]) waive this right and permit a contractor to retain ownership of a patentable invention, provided that certain conditions are met, including the receipt of a broad Government license to use the invention or have another use the invention on the Government's behalf.[43] Additionally, small businesses or nonprofit organizations may be able to retain title to patentable inventions.[44] Regardless, the Government will have the ability to make use of, and authorize others to make use of, inventions first conceived or actually reduced to practice under a Government contract.

### Rights In Copyrights

Ordinarily, contractors may not copyright works first produced under a Government contract without Government permission.[45] Similarly, contractors may not include copyrighted work in deliverables to the Government unless the contractor receives the Government's permission to do so or obtains an unrestricted license for the Government to use the copyrighted work.[46] As a result, the Government may generally distribute copyrightable works developed or delivered under Government contracts, provided that the Government has a sufficiently broad license in the related data (see discussion below).

### Rights In Trademarks

The standard Government contracts clauses generally do not address trademarks. Unless directed otherwise by the purchasing agency, contractors can include trademarks on delivered goods without risk of the Government acquiring rights in the trademark. Further, given the public nature of an organization's trademarks, the risk associated with an improper Government disclosure of an organization's trademarks is low, though trademark law may have some effect in the procurement context (i.e., an organization may bring suit against the Government to protect

 

trademarks that the organization used during contract performance).[47]

### Rights In Data

The rules for Government access to and use of "data" and "technical data" (types of recorded information that may include contractor trade secrets) relating to Government contracts are complex. The Government will rarely take ownership of data; however, the Government often receives licenses to use and disclose contractor data. The scope of these licenses varies based on a number of factors, including how the data were developed and whether the purchasing agency is a civilian or defense agency.

Standard contract clauses for civilian agencies address "data," which are defined as "recorded information, regardless of form or the media on which it may be recorded" and include computer software and technical data.[48] The standard civilian agency data clause gives the Government an unlimited rights license (defined as the right to "use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so") in data first produced under the contract or data delivered under the contract.[49] As a general matter, the civilian agency data clauses direct contractors to protect data developed at private expense by not delivering the data to the Government and, instead, by delivering "form, fit, or function data," which are defined as "data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements."[50]

Defense agencies have a separate regime for acquiring "technical data," which are defined as "recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation)" and specifically exclude "computer software and data incidental to contract administration, such as financial and/or management information."[51] In contracts with defense agencies, the Government acquires a license to technical data developed under the contract and certain other categories of data relating to contract purchase.[52] The scope of this license varies based on who funded the development of the technical data (the Government or the contractor) and the nature of the data. (The Government always receives broad rights in form, fit, and function data and data necessary for installation, operation, maintenance, or training, regardless of funding.)[53] The broadest standard Department of Defense license to contractor technical data (an "unlimited rights license") enables the Government to use or disclose covered contractor technical data in any manner and for any purpose.[54] Even certain of the more restrictive licenses that the Department of Defense may receive in contractor technical data, such as the "Government purpose license," enable the Government to use the data for dual sourcing and competitive procurements.[55]

The Department of Defense's technical data clauses are complex and contain a number of additional features that affect defense agencies' ability to use and disclose contractor technical data. Such features include (1) a separate and more lenient method for acquiring commercial technical data;[56] (2) the ability to negotiate the Government's technical data rights under certain circumstances (as discussed in greater detail below);[57] (3) the need to identify in the proposal process all technical data that will be furnished with less than unlimited rights;[58] and (4) the ability of the Government to release any technical data to special categories of contractors.[59]

Both the civilian and defense agency data clauses implicitly distinguish between the scope of the Government's rights in contractor data and the data that a contractor actually delivers to the Government under a contract. While Government rights in data attach automatically, the Government must explicitly require the delivery of data, usually through a contract data requirements list (CDRL), to obtain the data. The Government cannot disclose what it does not possess, so the Government's practical ability to release contractor data can still be limited if the contractor does not deliver such data.

### Rights In Computer Software

As a general matter, both civilian and defense agencies treat computer software in a manner similar to data.[60] However, the Government also has special rules for the acquisition of commercial computer software.[61] These rules permit agencies to acquire commercial computer software on terms similar to those that the vendor offers to commercial customers.[62] Even so, the regulations direct COs to review a vendor's standard license and remove terms that are contrary to the Government acquisition process, such as indemnification language (which may create Anti-Deficiency Act issues) and choice of law provisions (which may be inconsistent with the Government's waiver of sovereign immunity).[63]

## When It All Goes Wrong

Many overlapping statutory and regulatory regimes affect an organization's ability to protect IP disclosed to the Government. However, these regimes each have shortcomings that, without more, prevent them from providing an effective and complete remedy for organizations that have suffered from a Government misappropriation or improper disclosure of IP.

This section of the PAPER discusses what happens when something goes wrong. There are many situations in which an IP "wrong" can arise. The Government could inappropriately disclose IP through a response to a FOIA request. Similarly, a Government employee could provide a contractor's IP to a third party (even a competitor), perhaps thinking that it is within his power to do so. Under these and other scenarios, the party owning the misappropriated or improperly disclosed IP should ask two key questions:

(1) How can I regain control of my IP?

(2) Can I be compensated for the loss of value caused by the misappropriation or improper disclosure?

This section of the PAPER addresses these two questions. Specifically, it looks to the potential remedies available to an injured party, including relief under the contract, the Federal Tort Claims Act (FTCA), the APA, the U.S. Constitution, state trade secret laws, and general federal procurement regulations. While each of these actions has its own considerations and complications, a combination of these actions likely provides the most effective means for addressing an inappropriate Government use or disclosure of IP.

### Breach Of Contract Claim

While the standard IP clauses are comprehensive in their coverage, the clauses are less specific regarding a contractor's remedies for improper Government use or disclosure of contractor IP. For copyrights and patents, this is likely due in part to the clearly defined statutory remedy against the Government for damages in the event of Government infringement upon an organization's IP.[64] For data, the lack of specific remedies is likely due in part to the contractor's ability to refrain from delivering certain types of data and in part to the fact that a Government breach (i.e., the use or disclosure of data beyond the scope of its license) may be treated like any other contract breach claim under a Government contract. Under the standard Government contracts disputes clause and relevant contract disputes jurisdiction and forum authority, a contractor may receive an increase in contract price to reflect the added scope associated with an increased license; however, the contractor cannot enjoin the Government's use and disclosure of the IP at issue.[65] Furthermore, a contractor likely cannot stop performance of a Government contract simply because the Government has breached the contract.[66]

The contract may provide a contractor with an avenue to seek declaratory relief and even damages concerning the Government's use of a copyright or data beyond the scope of its license. However, the contract will not provide a mechanism for the contractor to regain control of its IP through equitable remedies. The rest of this section of the PAPER addresses alternative avenues under constitutional, federal, or even state law, both for receiving damages for IP (generally trade secrets) not covered by the contract and for regaining control of that IP through equitable relief.

 

### Federal Tort Claims Act Claim

The FTCA makes the U.S. Government liable for certain torts "in the same manner and to the same extent as a private individual under like circumstances."[67] This waiver of sovereign immunity extends to Government employees acting within the scope of their office or employment.[68] Under the FTCA, an injured party can recover damages against the Government. As with a breach of contract claim, the contractor cannot receive an injunction to stop the damaging activity.[69]

When determining whether the conduct of a Government employee represents an actionable tort, the FTCA directs courts to assess the conduct "in accordance with the law of the place where the act or omission occurred."[70] Thus, state law determines the legal requirements of an FTCA action.

All states recognize as a tort some form of trade secret misappropriation. The vast majority of states—all except Massachusetts, New York, and North Carolina—have adopted the Uniform Trade Secrets Act (UTSA).[71] The UTSA defines three elements of trade secret misappropriation: (1) the existence of a valid trade secret, (2) the unconsented disclosure or use of the trade secret, and (3) the knowledge that the trade secret was improperly acquired.[72] Trade secrets include "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value. . .from not being generally known. . .and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[73] Thus, if an organization can show that a Government action met these requirements, it could potentially bring an FTCA claim against the U.S. Government in federal district court.

Some IP-related FTCA claims may face jurisdictional challenges. As noted above, the FTCA provides organizations with a remedy in the federal district courts for torts committed by the U.S. Government, including trade secrets misappropriation claims. A separate federal statute, the Tucker Act, gives a different federal court, the U.S. Court of Federal Claims, *exclusive* jurisdiction over claims arising from an express or implied contract with the United States.[74] The Court of Federal Claims, however, has *no* jurisdiction over tort claims against the U.S. Government.[75] These jurisdictional boundaries result in two separate and exclusive forums for trade secrets claims against the Government: federal district courts, which can hear tort claims but not claims arising from express or implied contracts with the Government; and the Court of Federal Claims, which can hear contract claims but not tort claims. Because trade secrets actions brought under the FTCA are tort claims that often relate to a contract (as discussed above, the Government's ability to use or disclose IP may be defined in a contract between the parties), FTCA claims can cause complicated jurisdictional challenges.

The complex jurisdictional issues that FTCA claims face make the manner in which an organization pleads an IP-related FTCA claim extremely important. For example, in a recent case, the U.S. Court of Appeals for the Fifth Circuit reversed a $1.45 million IP-related award to an organization—U.S. Marine, Inc.—under the FTCA.[76] The Fifth Circuit's rationale was that the case allegedly stemmed from the Government's violation of license rights it received in U.S. Marine's IP and, thus, the case arose from an express or implied contract with the Government and must be heard by the Court of Federal Claims.[77] The Federal Circuit (the appellate court for the Court of Federal Claims) recognized that U.S. Marine had no privity of contract with the Government (no actual contract existed licensing the IP to the Government) and that U.S. Marine could lose its ability to recover under the FTCA if the case were transferred to the Court of Federal Claims (because FTCA claims necessarily are tort claims).[78] Despite the potential lack of a meaningful recovery at the Court of Federal Claims, the Federal Circuit agreed with the Fifth Circuit and determined that the claim should have been brought in the Court of Federal Claims.[79]

Jurisdictional issues can make an IP-related FTCA action more complicated (and expensive) to pursue and may deprive an organization of a remedy for Government misuse of an organization's trade secret. Thus, jurisdictional issues are important initial consider-

ations when contemplating an FTCA action, particularly if the underlying conduct can be characterized as relating to a contract with the Government (even if the organization bringing the claim is not a party to the relevant contract).

### Administrative Procedure Act Action

If the Government threatens improperly to use or disclose an organization's IP, the organization may consider an APA claim against the Government. Under the APA, an organization can seek injunctive relief against a Government agency to prevent it from taking actions that are arbitrary, capricious, or against the law.[80] As explained above, APA claims can be expensive to prosecute and difficult to win because of the high standard that must be shown to reverse Government action under the APA.[81]

The APA permits injunctive relief against the Government but does not allow for the recovery of monetary damages.[82] This makes the APA an imperfect remedy for improper IP use and disclosure. The organization owning the IP must know of the potential improper use or disclosure ahead of time in order for the injunction to provide any benefit; an injunction preventing the Government from disclosing IP after it has already done so is of little use. Such advanced knowledge of an inappropriate Government use or disclosure is not often possible.

In addition to the substantive challenges of an APA claim, an organization bringing an APA action in the context of an IP disclosure may face procedural challenges. The APA only provides for equitable remedies.[83] Many inappropriate Government disclosures of IP occur in the context of Government contracts, so the Court of Federal Claims will have exclusive jurisdiction over related disputes.[84] Because the Court of Federal Claims does not have authority to issue equitable relief,[85] an injured party may find itself in a similar situation to that discussed above in the context of FTCA: the Tucker Act could force an APA claim to the Court of Federal Claims because the claim relates to a contract, but at the Court of Federal Claims, an organization may have no remedy under the APA because the Court has no authority to award the only relief available under the APA.

### Takings Claim

A more clear-cut option for organizations with a potential IP-related claim against the Government is a takings claim under the Fifth Amendment of the U.S. Constitution.[86] The basic theory of such a claim is that the Government has "taken" an organization's IP and diminished its value by its unauthorized use or by disclosing it to competitors or the public. Accordingly, under this theory, the Government owes the organization just compensation for its taking in the same way that the owner of physical property is due compensation if the Government takes or destroys that property.

The legal requirements for a takings claim are relatively straightforward: a claimant must show "Governmental action short of acquisition of title or occupancy [that] deprive[s] the owner of all or most of his interest in the subject matter."[87] Whether a takings claim has occurred, however, is a factually dependent determination.[88] In making this determination, courts look to "[t]he economic impact of the regulation on the claimant and, particularly, the extent to which the [Government] has interfered with distinct investment-backed expectations."[89] Courts will also look to the character of the Government action, with physical invasions being more likely to result in successful takings actions than "when interference arises from some public program adjusting the benefits and burdens of economic life to promote the common good."[90]

An organization must have a valid property interest before it can allege that the Government has taken its property.[91] The trade secret protections identified above can provide such an interest and, therefore, can serve as the basis for a takings claim.[92] An organization must show that all of the above-discussed requirements of a trade secret are present. Thus, an organization will need to show that it has sought to keep the information at issue secret through organizational safeguards on the storage, transmission, and distribution of the information.[93]

The ability of the organization to obtain complete relief through a takings claim is a second key factor to determining whether a takings claim is appropriate. An organization cannot actually stop the misuse or

 

improper disclosure of its IP under a takings claim because equitable remedies, such as injunctions, are not available.[94] Furthermore, while an organization is entitled to monetary damages under a successful takings claim, to do so, an organization must show the difference in market value of the IP before and after the taking.[95] Meeting this standard in the context of an IP-related takings claim can be challenging because establishing the value of the IP is difficult and identifying the reduction in such value caused by the Government's misuse or public release may require speculation.

### State Trade Secrets Action Against The Recipient Of IP

While both FTCA and takings claims permit a potential monetary recovery against the Government, neither allows for an injunction forcing the Government to stop the unauthorized use or disclosure of the IP. Further, while the APA provides for injunctive relief, the standard for relief is high[96] and the likelihood that a contractor will have advanced knowledge of a Government disclosure is low. In fact, as discussed above, the Government has the inherent right to use certain types of IP, such as patents, as long as compensation is paid to the IP owner. In the event of an improper Government disclosure of a trade secret, however, IP owners may wish to do everything possible to actually cease the unauthorized use and disclosure of their IP.

One potential way to stop the use of improperly disclosed IP is to seek an injunction against the recipient of the IP through a state trade secret action. As explained above, the UTSA prohibits trade secret misappropriation.[97] The UTSA defines trade secret misappropriation in a way that covers both individuals that inappropriately take trade secrets and individuals that disclose or use a trade secret of another when that individual, among other things, (1) prior to use, knew or had reason to know that the information was a trade secret and that knowledge of it had been acquired by accident or mistake, or (2) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use.[98] Both of the above circumstances, which represent only some of the actionable circumstances under the UTSA, cover an instance where a Government employee incorrectly discloses IP that is marked as proprietary, or other IP that is obviously proprietary, to a third party.

Unlike some other remedies discussed in this Paper, the UTSA expressly allows a party to obtain injunctive relief.[99] This means that an injured organization could bring a UTSA action against a party receiving inappropriately disclosed IP (assuming that the disclosure and receiving party is known) to prevent that other party from using or disclosing the IP. The availability of such a remedy outside of the APA context makes a UTSA action against the recipient of improperly disclosed IP an important option to consider for an organization that has had critical IP improperly disclosed by the Government.

### Bid Protest

Finally, if an unauthorized disclosure occurs that affects a procurement, an injured bidder may consider protesting a future award that may have been affected by the disclosure. The two most likely grounds for a protest under these circumstances arise from a potential organizational conflict of interest (OCI) or a PIA violation.

The Government limits participation in procurement actions by contractors that have an OCI.[100] An OCI occurs when "a firm has access to non-public information as part of its performance of a government contract and where that information may provide the firm a competitive advantage in a later competition for a government contract."[101] If the Government awards a contract to an entity with an unmitigated OCI, a disappointed bidder could potentially protest the award as improper.

Winning a protest on OCI grounds may not be easy.[102] The Government agency conducting the procurement has considerable discretion in deciding whether and how a company should be excluded from a procurement if an OCI exists.[103] Moreover, a protester must present "hard facts," as opposed to a mere inference, to show that an OCI exists.[104]

 

PIA violations, as discussed earlier in this PAPER, can also give rise to actionable bid protest grounds.[105] If a PIA violation occurs, a disappointed bidder will have to show that the violation affected the award of a contract to have appropriate grounds for a protest.[106]

Even a bid protest victory may be an incomplete remedy for a disappointed bidder. A bid protest would not be able to give the injured organization long-term relief in the form of damages caused by the disclosure, nor can the action result in an injunction against any third party from further disclosing the proprietary information. At best, the successful protester is permitted a fair opportunity for award of the contract, most likely after a recompetition or other remedial action by the agency. If the danger is the further use or disclosure of its proprietary information, however, these remedies offer little comfort, and the injured organization will need to look to the other remedies referenced in this section of the PAPER to obtain further relief.

## Best Practices When Disclosing IP To The Government

There are steps that an organization can take to protect itself from misuse and inappropriate Government disclosures of IP and position itself for a complete remedy if such a disclosure occurs. This section of the PAPER discusses some of these best practices.

### General Best Practices

The only information that is protected fully from Government misuse or disclosure is information that the Government does not possess. While there are several overlapping regimes related to protection of IP submitted to the Government, those regimes each have their shortcomings. Neither absolute protection nor entirely adequate remedies are assured if the Government misuses or improperly discloses an organization's IP.

For organizations looking for IP security, the best practice is to limit disclosures of IP to the Government or any other unaffiliated party. In practical terms, this does not mean ceasing all IP disclosures. Instead, organizations should identify the IP that matters most to them and attempt to avoid any disclosure of such IP, even when legal protections are in place for the disclosed IP.

Organizations can mitigate the impacts of this approach by identifying substitute IP that is less sensitive and can be disclosed with the appropriate protections. Executable code can be provided instead of source code; "other than certified cost or pricing data" can be provided instead of cost data; technical capabilities can be provided instead of technical data; and basic product information can be provided instead of detailed product schematics. The goal should be getting the customer the information that it needs without compromising an organization's "crown jewels."

The disclosure or nondisclosure of critical IP will have strategic implications for an organization. Nondisclosure may involve not immediately giving customers, potential customers, and other Government entities exactly what they are requesting. This may create customer relation issues or misunderstandings that will need to be managed. Furthermore, there may be times when nondisclosure is simply not an option. Nevertheless, shifting from a presumption of submitting IP whenever asked to a presumption that at least certain IP is never disclosed is a first step to protecting an organization's most valuable IP from inappropriate use or disclosure.

### Disclosing Information Outside Of A Contractual Setting

Within Government contractors, IP protection efforts tend to focus on Government contracts. This attention is warranted because of the complex terms at issue and implications of improper disclosure. That said, organizations routinely disclose substantial IP outside of the contract setting. Such disclosures can occur in the context of Government product evaluation efforts, prototype demonstrations, and the general interactions between the Government and industry technical or program personnel.

Disclosure of IP outside of the contractual setting is dangerous. These disclosures occur outside of the IP protection structures with which many Government employees and contractors are most familiar (i.e., protections during the proposal process and contractual

 

data licensing and protection provisions). Further, the informal nature of these disclosures may not emphasize to Government employees the sensitivity of the information communicated.

The best practice when disclosing IP to the Government outside of the contractual setting is similar to the general best practice discussed above: only disclose what is necessary to achieve your goal. Often, organizations can achieve the purpose of noncontractual disclosures by communicating limited and high-level technical information (which presumably is less sensitive), rather than disclosing truly sensitive information. When an organization only discloses such high-level information, the existing protections discussed above likely are sufficient to protect the information at issue.

If an organization must disclose more sensitive information, it should consider whether it is appropriate to seek a nondisclosure agreement (NDA) from the Government officials receiving the information. Seeking an NDA from Government employees, either in their own capacity or on the part of the Government, is not yet a wide-spread and accepted practice, and many Government entities will take the position that such documents may not be executed or are void. That said, case law supports the enforceability of an NDA when the individual signing the NDA has actual or implied authority to do so or when a Government employee with contracting authority later ratifies an unauthorized NDA.[107]

There is always the possibility that sensitive IP must be disclosed outside of a contractual setting to a recipient that is unwilling to sign an NDA. Organizations should assess such situations on a case-by-case basis. If the organization determines that the disclosure is worth the risk, the best practice is to conspicuously mark the information as proprietary to remind those with access to the information to treat the IP appropriately. Emphasizing the proprietary nature of the IP in a cover letter or other documented communication and again when discussing the information is also appropriate under such circumstances.

### Disclosing Information In A Contractual Setting

IP disclosures in a contractual setting present an especially complex challenge to an organization looking to maintain control of its IP. After a contract is in place, there may be little that an organization can do to avoid the need to disclose certain IP to a Government customer if that IP is identified as a deliverable under the contract. Moreover, the Government will receive greater rights in IP that it procures under a contract (including sometimes the right to disclose that IP) than IP that an organization discloses for other reasons. There are, however, actions that an organization can take to protect itself and its IP in a contractual setting.

First, at the start of the procurement process, organizations should communicate with Government customers about the nature of the products or services acquired under the contract. The rights that the Government receives in IP related to a product or service will vary significantly based on how the organization developed the product (i.e., with Government or private funds) and whether the product is a commercial item. While these details may seem obvious to business development personnel within an organization, Government customers may not be as familiar with the product and may make assumptions that are incorrect or negatively affect an organization's ability to protect its IP.

A companion to this approach is the contractor development of support in advance for key assertions of commerciality and privately funded development. Whenever possible, contractors should provide Government purchasing personnel with this support so that the purchasing personnel can take it into account when shaping and conducting the acquisition. Having prepackaged support on hand for commerciality and private development determinations and communicating that information to Government purchasing personnel will help prevent the Government from procuring items in a way that gives the Government more IP rights than it requires or is legally permitted to obtain.

Second, when possible, organizations should structure contract proposals and contract terms in a way that protects their IP. Deliverables should be scrutinized; IP deliverables (most likely CDRLs) should be limited to information needed by the customer and should avoid delivery of the most sensitive product in-

 

formation when possible. Statements of work should also be closely reviewed because clarifying whether a product is being developed or simply delivered under a contract can dramatically affect the scope of the Government's rights in associated IP. Finally, standard contract clauses included in the proposed contract should be reviewed for applicability because eliminating unnecessary or inapplicable clauses will avoid confusion and make it easier to determine the intent of the parties in the event a dispute later arises. Contractors should be cautious, however, as objections to data rights terms in a competitive setting may invalidate a contractor's bid and prevent the contractor from obtaining a contract at all.[108]

Third, if a contract must be structured in a way that gives the Government rights in critical contractor data, contractors should consider specifically negotiated license rights. Within the Department of Defense, COs are permitted to negotiate the scope of license rights to certain categories of technical data.[109] While COs cannot waive all Government license rights in technical data delivered or created under a contract, they can agree to restrict the Government's rights to disclose data publicly or use that data for future competitive acquisitions.[110] COs are not required to negotiate technical data rights but, when available, specifically negotiated license rights provide an avenue for avoiding many of the most significant contractor concerns over Government use and disclosure of contractor IP.

Fourth, organizations *must* comply with proposal and contract terms regarding IP marking, disclosure, and administration. Many solicitations will require organizations to disclose as part of the proposal process IP that is developed at private expense; failure to do so could cause the Government to treat the IP as developed at Government expense.[111] Similarly, most contracts will require organizations to disclose patentable inventions (not just patented inventions) created in the course of performance; failure to do so could result in the contractor losing *all* rights in the invention.[112] Finally, most contracts require that data delivered with less than unlimited rights be marked with specific legends; failure to do so may result in inappropriate disclosure of the information or the Government receiving unlimited rights in the data.[113] Because of the critical role that contract language plays in the protection of an organization's IP, it is essential that an organization's contracts and program personnel understand and effectively implement the specific requirements of its contracts concerning the organization's IP.

Fifth, organizations performing Government contracts must recognize the potential significance of the Government's ability to demand delivery of IP. As discussed previously in this Paper, Government agencies will receive rights in IP developed with Government funds or relating to products delivered under a Government contract. However, the mere existence of these rights does not require a contractor to deliver the IP to the Government. Instead, to demand delivery, a contract must identify IP as a deliverable or contain a deferred ordering/delivery clause.[114] This is a second reason why contractors must closely review CDRLs and standard contract clauses, as discussed above. Even without a delivery requirement or a deferred ordering/delivery clause, the Government sometimes asserts that it is entitled to the delivery of IP simply by virtue of rights that it may have received in that IP. Knowledgeable contracts and program personnel can potentially avoid such disagreements by focusing on the delivery requirements of the contract.

Finally, an organization's contract and program personnel should be comfortable engaging with internal legal personnel early and often regarding IP issues. IP issues are complex and generally not part of a program's daily activities. While a threshold understanding of IP at the program level is essential, program personnel must also be comfortable routinely engaging legal personnel as a matter evolves.

## Guidelines

These *Guidelines* are intended to assist you in understanding how organizations can effectively manage their IP in light of the differing legal regimes surrounding IP relevant to commercial and Government customers, prospective customers, and other third parties. They are not, however, a substitute for professional representation in any specific situation.

 

**1.** Organizations should know and understand the basic rules for the development and protection of IP, both in general and in the context of transactions or exchanges with the U.S. Government.

**2.** Organizations should know the protections offered under federal patent, copyright, and trademark laws and under state trade secret laws.

**3.** When submitting information to the Government, organizations should be aware of the various legal regimes, like FOIA, the TSA, and the PIA, that protect their information from further use and disclosure.

**4.** Organizations should carefully read solicitations and contracts, looking for (a) IP delivery requirements, including for deferred delivery clauses, (b) IP disclosure requirements, and (c) IP rights and licensure provisions.

**5.** Organizations should identify alternate IP in situations where they might otherwise need to deliver to the Government sensitive IP.

**6.** Organizations should request that Government officials sign a nondisclosure agreement in situations where sensitive IP will be disclosed outside of a contractual setting.

**7.** Organizations should request specifically negotiated data rights in situations where the Government would receive broad rights in sensitive contractor IP.

**8.** Organizations should clearly identify and mark all IP. In a contractual context, organizations should make sure all disclosed IP carries the markings required by the contract.

**9.** Organization employees should engage early and often both with legal counsel and the Government to determine expectations for the use and disclosure of IP.

**ENDNOTES:**

[1]See generally Mutek, Geldon & Aylmer, "Supply Chain Risk Management & Compliance," Briefing Papers No. 15-13 (Dec. 2015).

[2]35 U.S.C.A. §§ 101, 103.

[3]35 U.S.C.A. §§ 154, 271.

[4]28 U.S.C.A. § 1498(a); 35 U.S.C.A. § 183.

[5]E.g., 48 C.F.R. 52.227-1.

[6]17 U.S.C.A. §§ 102, 103.

[7]17 U.S.C.A. § 101; Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240 (3d Cir. 1983).

[8]17 U.S.C.A. § 102.

[9]17 U.S.C.A. § 302(a).

[10]17 U.S.C.A. § 106.

[11]17 U.S.C.A. §§ 502, 504.

[12]28 U.S.C.A. § 1498(b).

[13]See Unif. Trade Secrets Act § 1, ULA Trade Secrets § 1 (Unif. Law Comm'n 1985).

[14]18 U.S.C.A. § 1905.

[15]5 U.S.C.A. § 552.

[16]15 U.S.C.A. § 1127.

[17]Gen. Healthcare Ltd. v. Qashat, 364 F.3d 332, 335 (1st Cir. 2004).

[18]15 U.S.C.A. § 1051.

[19]But see Complaint, DNC Parks & Resorts at Yosemite, Inc. v. United States, No. 1:15-cv-01034 (Fed. Cl. Sept. 17, 2015) (suit by previous contractor forces Yosemite National Park to change some established hotel and concession names); see also Whitcomb, "Yosemite Landmarks Set To Lose Famous Names in 'Ugly Divorce,' " Reuters (Feb. 29, 2016), http://www.reuters.com/article/us-yosemite-trademarks-idUSKCN0W35T6.

[20]5 U.S.C.A. § 552. See generally Meagher & Bareis, "The Freedom Of Information Act," Briefing Papers No. 10-12 (Nov. 2010).

[21]See, e.g., Renegotiation Bd. v. Bannercraft Clothing Co., 415 U.S. 1, 17 (1974).

[22]5 U.S.C.A. § 552(a)(1)–(3).

[23]See, e.g., NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 161–62 (1975); http://www.gsa.gov/portal/mediaId/188991/fileName/GSA__PUBLIC__INFORMATION__HANDBOOK (last visited Feb. 1, 2016); http://www.nro.gov/foia/faqs.html (last visited Feb. 1, 2016).

[24]See, e.g., Anderson v. U.S. Dep't of Justice, 518 F. Supp. 2d 1, 10 (D.D.C. 2007).

[25]5 U.S.C.A. § 552(b).

[26]5 U.S.C.A. § 552(b)(4).

[27]Exec. Order No. 12,600, 52 Fed. Reg. 23,781 (June 23, 1987).

[28]CNA Fin. Corp. v. Donovan, 830 F.2d 1132, 1133 n.1 (D.C. Cir. 1987).

[29]Complaint, Battelle Mem'l Inst. v. U.S. Dep't of the Army, No. 2:14-cv-00445 (S.D. Ohio May 14, 2014).

[30]5 U.S.C.A. § 706.

[31]5 U.S.C.A. § 702.

[32]18 U.S.C.A. § 1905.

[33]18 U.S.C.A. § 1905.

[34]See, e.g., Chrysler Corp. v. Brown, 441 U.S. 281, 316–17 (1979).

[35]41 U.S.C.A. §§ 2101–2107.

[36]41 U.S.C.A. §§ 2102(a), 2105.

[37]41 U.S.C.A. § 2101.

[38]41 U.S.C.A. §§ 2102(a), 2105.

[39]41 U.S.C.A. § 2105.

[40]41 U.S.C.A. § 2105.

[41]35 U.S.C.A. §§ 201, 202. See generally DeVecchio, "Patent Rights Under Government Contracts," Briefing Papers No. 07-7 (June 2007).

[42]See 48 C.F.R. § 1852.227-70(b).

[43]E.g., 48 C.F.R. § 52.227-11.

[44]See 37 C.F.R. § 401.14.

[45]48 C.F.R. § 27.404-3(a). See generally DeVecchio, "Copyright Protection Under Government Contracts," Briefing Papers No. 05-6 (May 2005).

[46]48 C.F.R. § 27.404-3(b); see also 48 C.F.R. § 27.404-3(b)(2) (requiring that the Government receive in all copyrighted work contained in a deliverable a paid-up, nonexclusive, irrevocable, worldwide license to reproduce, prepare derivative works, distribute to the public, perform publicly, and display publicly by or on behalf of the Government).

[47]See Complaint, DNC Parks & Resorts at Yosemite, Inc. v. United States, No. 1:15-cv-01034 (Fed. Cl. Sept. 17, 2015).

[48]48 C.F.R. § 52.227-14(a).

[49]48 C.F.R. § 52.227-14(a), (b).

[50]48 C.F.R. § 52.227-14(a), (g).

[51]48 C.F.R. § 252.227-7013(a)(15).

[52]48 C.F.R. § 252.227-7013(b).

[53]48 C.F.R. § 252.227-7013(a), (b).

[54]48 C.F.R. § 252.227-7013(a), (b).

[55]48 C.F.R. § 252.227-7013(a), (b).

[56]See 48 C.F.R. § 252.227-7015(b) (providing the Government with unrestricted rights in (1) form, fit, and function data; (2) data that are produced to the Government without restrictive markings; (3) data that are necessary for operation, maintenance, installation, or training (other than detailed manufacturing or process data); and (4) corrections or changes to Government-furnished data).

[57]48 C.F.R. § 252.227-7013(b)(4).

[58]48 C.F.R. § 252.227-7013(e) (setting forth format for disclosure of technical data to be provided to the Government with less than unlimited rights and noting that the Government may treat data not disclosed through this process as being covered by an unlimited rights license).

[59]48 C.F.R. § 252.227-7013(a)(5), (b)(3)(iv) (permitting disclosure of limited rights technical data to "covered government support contractors," defined as contractors that "furnish independent and impartial advice or technical assistance directly to the Government in support of the Government's management and oversight of a program or effort (rather than to directly furnish an end item or service to accomplish a program or effort)," but requiring contractor notice of such disclosure and permitting the contractor to require the Government support contractor to execute an nondisclosure agreement).

[60]See 48 C.F.R. §§ 52.227-14(a) (defining for civilian acquisitions "data" as including computer software), 252.227-7014 (setting forth similar rights in noncommercial computer software as the Government receives in technical data).

[61]See 48 C.F.R. §§ 12.212, 227.7202-3.

[62]See 48 C.F.R. § 12.212(a) ("Commercial computer software or commercial computer software documentation shall be acquired under licenses customarily provided to the public. . . ."); 48 C.F.R. § 227.7202-3(a) ("The Government shall have only the rights specified in the license under which the commercial computer software or commercial computer software documentation was obtained.")

[63]48 C.F.R. § 12.212(a) (requiring use of commercial licenses only "to the extent such licenses are consistent with Federal law and otherwise satisfy the Government's needs"); 48 C.F.R. § 227.7202-1(a) ("Commercial computer software or commercial computer software documentation shall be acquired under the licenses customarily provided to the public unless such licenses are inconsistent with Federal procurement law or do not otherwise satisfy user needs.")

[64]See 28 U.S.C.A. § 1498(a), (b); 35 U.S.C.A. § 183.

[65]See 48 C.F.R. § 52.233-1.

[66]See 48 C.F.R. § 52.233-1.

[67]28 U.S.C.A. § 2674.

[68]28 U.S.C.A. § 1346(b).

 

[69]28 U.S.C.A. § 1346(b); Talbert v. United States, 932 F.2d 1064, 1065–66 (4th Cir. 1991).

[70]28 U.S.C.A. 1346(b).

[71] http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (last visited Feb. 1, 2016).

[72]Unif. Trade Secrets Act § 1, ULA Trade Secrets § 1 (Unif. Law Comm'n 1985).

[73]Unif. Trade Secrets Act § 1(4), ULA Trade Secrets § 1(4) (Unif. Law Comm'n 1985).

[74]28 U.S.C.A. § 1491(a).

[75]28 U.S.C.A. § 1491(a)(1).

[76]U.S. Marine, Inc. v. United States, 478 F. App'x 106 (5th Cir. 2012).

[77]U.S. Marine, Inc. v. United States, 478 F. App'x 106 (5th Cir. 2012).

[78]U.S. Marine, Inc. v. United States, 722 F.3d 1360 (Fed. Cir. 2013), 55 GC ¶ 228.

[79]U.S. Marine, Inc. v. United States, 722 F.3d 1360 (Fed. Cir. 2013), 55 GC ¶ 228; see also Nash, "Stealing Subcontractor Limited Rights Data: Tort, Breach of Contract, or Taking?," 27 No. 9 NASHCIBINIC-NL ¶ 44 (Sept. 2013).

[80]5 U.S.C.A. § 706.

[81]5 U.S.C.A. § 706.

[82]5 U.S.C.A. § 702.

[83]5 U.S.C.A. § 702.

[84]28 U.S.C.A. § 1491(a).

[85]28 U.S.C.A. § 1491(a).

[86]See, e.g., Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984); see also 28 U.S.C.A. § 1491(a) (providing the Court of Federal Claims jurisdiction to hear claims based on the Constitution and, therefore, avoiding the jurisdictional issues presented by FTCA and APA actions).

[87]Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1005 (1984); see U.S. Marine, Inc. v. United States, 722 F.3d 1360, 1373–74 (Fed. Cir. 2013), 55 GC ¶ 228; Gal-Or v. United States, 470 F. App'x 879, 884 (Fed. Cir. 2012).

[88]Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 124 (1978).

[89]Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 124 (1978).

[90]Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 124 (1978).

[91]See, e.g., Chancellor Manor v. United States, 331 F.3d 891, 901 (Fed. Cir. 2003).

[92]Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984).

[93]Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984).

[94]Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1016 (1984) ("[e]quitable relief is not available to enjoin an alleged taking of private property for a public use").

[95]See, e.g., Dugan v. Rank, 372 U.S. 609, 624-25 (1963).

[96]5 U.S.C.A. § 706.

[97]Unif. Trade Secrets Act § 1(2), ULA Trade Secrets § 1(2) (Unif. Law Comm'n 1985).

[98]Unif. Trade Secrets Act § 1(2), ULA Trade Secrets § 1(2) (Unif. Law Comm'n 1985).

[99]Unif. Trade Secrets Act § 2(a), ULA Trade Secrets § 2(a) (Unif. Law Comm'n 1985).

[100]48 C.F.R. § 9.505.

[101]Trandes Corp., Comp. Gen. Dec. B-411742 et al., 2015 CPD ¶ 317, 57 GC ¶ 356.

[102]But see 48 C.F.R. § 9.505-4(b) (contemplating confidentiality agreements between organizations that submit data to the U.S. Government and Government support contractors that receive and use the data to provide services to the Government; these confidentiality agreements may provide the basis for a breach action directly against an organization that has an OCI).

[103]Trandes Corp., Comp. Gen. Dec. B-411742 et al., 2015 CPD ¶ 317, 57 GC ¶ 356.

[104]See, e.g., North Wind, Inc., Comp. Gen. Dec. B-404880.7, 2012 CPD ¶ 314.

[105]See Eng'g Support Personnel, Inc., Comp. Gen. Dec. B-410448, 2015 CPD ¶ 89.

[106]See Eng'g Support Personnel, Inc., Comp. Gen. Dec. B-410448, 2015 CPD ¶ 89.

[107]Demodulation, Inc. v. United States, 103 Fed. Cl. 794, 804 (2012); Liberty Ammunition, Inc. v. United States, 119 Fed. Cl. 368 (2014), 57 GC ¶ 26.

[108]See, e.g., Deloitte Consulting, LLP, Comp. Gen. Dec. B-411884 et al., 2016 CPD ¶ 2, 58 GC ¶ 63.

[109]48 C.F.R. § 252.227-7013(b)(4).

[110]48 C.F.R. § 252.227-7013(b)(4).

[111]See, e.g., 48 C.F.R. §§ 252.227-7017, 252.227-7013(e).

[112]48 C.F.R. § 52.227-11(b)(2)(i).

[113]See, e.g., 48 C.F.R. §§ 227.7103-10(c), 252.227-7013(e).

[114]See, e.g., 48 C.F.R. §§ 52.227-16, 252.227-7026, 252.227-7027.

 