Trade Secret Seizure Best Practices Under the Defend Trade Secrets Act of 2016

Timothy Lau

Federal Judicial Center
June 2017

These recommended best practices are prepared in accordance with the request of Congress in the Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 6.

CONTENTS

INTRODUCTION

The Defend Trade Secrets Act of 2016 (DTSA), Pub. L. No. 114-153, became law on May 11, 2016. It amends 18 U.S.C. § 1836 to create a private right of action for the misappropriation of trade secrets "for which any act occurs on or after the date of the enactment" and where the trade secrets "[are] related to [] product[s] or service[s] used in, or intended for use in, interstate or foreign commerce."[1] The impetus for the DTSA was Congress's sense that "trade secret theft, wherever it occurs, harms the companies that own the trade secrets and the employees of the companies."[2]

The DTSA uses the definition of "trade secret" that was set forth in the Economic Espionage Act of 1996, codified in 18 U.S.C. § 1839(3), and that broadly encompasses

> all forms and types of financial, business, scientific, technical, economic, or engineering information, . . . , whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing . . . .

In addition, for "information" to qualify as a "trade secret" § 1839(3) requires that

> (A) the owner [of the information] has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means . . . .

The act of "misappropriation" is defined in the newly created §§ 1839(6) and (7).

Sections 1836(b)(2) and (3) govern the remedies for trade secret misappropriation. Section 1836(b)(3) provides that courts may grant the standard remedies of injunctive relief or damages. Section 1836(b)(2) also authorizes a court, upon ex parte application of a plaintiff and "in extraordinary circumstances," to issue "an order providing for the seizure of property necessary to prevent the propagation or dissemination of the [subject] trade secret."

The DTSA tasks the Federal Judicial Center as follows:

> (a) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Federal Judicial Center, using existing resources, shall develop recommended best practices for—
>
> (1) the seizure of information and media storing the information; and
>
> (2) the securing of the information and media once seized.
>
> (b) Updates.—The Federal Judicial Center shall update the recommended best practices developed under subsection (a) from time to time.

1. 18 U.S.C. § 1836(b)(1).

2. DTSA, Pub. L. No. 114-153, § 5(2).

> (c) CONGRESSIONAL SUBMISSIONS.—The Federal Judicial Center shall provide a copy of the recommendations developed under subsection (a), and any updates made under subsection (b), to the—
>
> (1) Committee on the Judiciary of the Senate; and
>
> (2) Committee on the Judiciary of the House of Representatives.[3]

These trade secret seizure best practices were developed in response to the DTSA's mandate and are based on the limited initial experience in the federal courts with 18 U.S.C. § 1836(b)(2). They are being circulated prior to the due date of May 11, 2018, so that courts can benefit from having early guidance on the subject matter. The Center will update these best practices as needed.

Intended Audience of the Trade Secret Seizure Best Practices

These best practices were written for the federal courts and are designed to help them meet their obligations in seizures of misappropriated trade secrets set forth in the DTSA.

Cases involving seizures of trade secrets are inherently challenging. From a practical point of view, because the remedy of seizure may only be granted to prevent "an immediate . . . injury," the courts generally will not have the luxury of time in handling these cases. Also, because 18 U.S.C. § 1836(b)(2) may be invoked "only in extraordinary circumstances," individual judges are unlikely to build up experience with these types of cases through repeated encounters. These factors combine to make these cases difficult to adjudicate.

One judge has suggested that courts would find the development of forms and templates helpful. Accordingly, the best practices are crafted in a way that provides as many standard approaches to the issues presented in these cases as possible. Many of them are drafted in a way that allows them to be incorporated readily into court orders; others are supplemented with illustrative language. In addition, an appendix is provided to give the courts suggestions about how to combine the statutory requirements of 18 U.S.C. § 1836(b)(2) and the best practices in the seizure orders.

Nonetheless, the practices are not intended to displace courts' actual experience with this type of seizure or their consideration of the special circumstances of each particular case. A district may adopt the practices in part, elect to have the practices converted into standing orders issued by individual judges, incorporate the practices within a larger set of local rules governing all trade secret cases, or not adopt any of the practices at all. The best practices are accompanied with narratives that explain the rationale of the practice and describe some of the practical problems the practice is intended to solve. The narratives are intended to assist courts in deciding which, if any, of the best practices they will adopt.

The provisions of 18 U.S.C. § 1836(b)(2) impose practical requirements applicants must fulfill before filing applications for seizure orders, many of which may not be obvious from the language of the statute. While these best practices were not drafted for attorneys, they do give indications about what courts may need from them in order to grant the remedy that they seek. Therefore, attorneys may find the practices helpful as a guide to navigating the various

3. DTSA, Pub. L. No. 114-153, § 6.

requirements of § 1836(b)(2) even when practicing in districts that have not adopted the practices.

Some state courts appear to have issued seizure orders pursuant to 18 U.S.C. § 1836(b)(2), with adaptations to fit the federal remedy within the local context. These best practices are not designed for use in state courts, but they may be useful in guiding state courts that have chosen to adapt elements of the federal practice surrounding § 1836(b)(2).

Scope of the Trade Secret Seizure Best Practices

Section 1836(b)(2) contemplates a multistage process for the seizure of trade secrets, including the following essential steps:

- issuance of a seizure order by the court following an application for the order, governed by §§ 1836(b)(2)(A) and (B);
- seizure of the misappropriated trade secrets by law enforcement officers and the "technical experts," governed by § 1836(b)(2)(E);
- custody of the seized material by the court, governed by §§ 1836(b)(2)(D)(i)–(iii);
- conduct of a seizure hearing by the court, governed by § 1836(b)(2)(F); and
- examination of the seized material by a special master, if one is appointed by the court, governed by § 1836(b)(2)(D)(iv).

This set of trade secret seizure best practices is intended to assist the courts with the stages leading up to the seizure hearing.

Development of the Trade Secret Seizure Best Practices

The Center developed these best practices in consultation with a number of federal judges. The Center also consulted the United States Marshals Service and experienced members of the bar. The best practices take into account the experience of the courts and others in the limited number of cases involving 18 U.S.C. § 1836(b)(2) since the enactment of the DTSA. A particular goal was to ensure that a diversity of opinions and practices are reflected in the development of the best practices.

ACKNOWLEDGMENTS

The Center thanks all who have given their comments and suggestions in the construction of these best practices:

Judge Raymond Clevenger III (Fed. Cir.)

Judge James Dever III (E.D.N.C.)

Judge Jeremy Fogel (N.D. Cal.)

Judge Matthew Leitman (E.D. Mich.)

Judge Loretta Preska (S.D.N.Y.)

Lucille Roberts (United States Marshals Service)

Eugene Kim (United States Marshals Service)

Clifford Krieger (United States Marshals Service)

Professor Eric Goldman (Santa Clara University School of Law)

Professor Mark Lemley (Stanford Law School)

Professor David Levine (Elon University School of Law)

Professor Peter Menell (UC Berkeley School of Law)

Morgan Chu (Irell & Manella LLP)

Elizabeth Laughton (Munger, Tolles & Olson LLPO)

John Marsh (Bailey Cavalieri LLC)

Paul Mersino (Butzel Long)

James Pooley (Orrick)

Gabriel Ramsey (Orrick)

Tina Chappell (Intel Corp.)

Alex Feerst (Medium)

Michael Spillner (Tessera Technologies, Inc.)

Rouz Tabaddor (Core Logic, Inc.)

James Aquilina (Stroz Friedberg LLC)

In addition, the Center held a panel discussion at the 2016 meeting of the American Intellectual Property Law Association. The feedback of each of the members who offered thoughtful suggestions is appreciated even though if he or she cannot be acknowledged by name.

1. GENERAL PROVISIONS OF THE TRADE SECRET SEIZURE BEST PRACTICES[4]

1-1. Scope

These trade secret seizure best practices apply to all civil actions which involve an ex parte application for the seizure of trade secrets under 18 U.S.C. § 1836(b)(2) and for which all the requirements for the issuance of the seizure order set forth under § 1836(b)(2)(A)(ii) have been met.

1-2. Court Discretion

Nothing in these trade secret seizure best practices is intended to limit the discretion of the court to adjust the practices on the basis of the circumstances of any particular case, including, without limitation, the simplicity or complexity of the case as shown by the trade secrets, technology, products, or parties involved.

1-3. Designation and Protection of Certain Disclosures Pending Entry of a Protective Order

The court should provisionally enter a standard protective order or at least provide for the designation and protection of information as "Confidential—Attorneys' Eyes Only" until it enters a protective order.

• • •

The seizure of allegedly misappropriated trade secrets under 18 U.S.C. § 1836(b)(2) generally will take place before the parties to the litigation can agree to a protective order. However, such a seizure necessarily will entail disclosures of trade secrets, which generally should not be made available to the public or even to the parties. It is therefore appropriate that the court at least provide for the designation and appropriate treatment of certain information as "Confidential—Attorneys' Eyes Only" prior to the entry of a protective order.

The court can protect against these disclosures by entering a standard protective order. A number of district courts, such as the Northern District of California, have already promulgated standard protective orders that may be suitable for this purpose. If the court elects not to enter a standard protective order, it should provide for the protection of such disclosures within its seizure order.

4. Recommended best practices are presented in italics at that beginning of each section.

2. CHOICE OF A FEDERAL LAW ENFORCEMENT OFFICER FOR THE SERVICE AND EXECUTION OF THE SEIZURE ORDER

The court should presumptively designate the United States marshal to serve and execute any seizure order issued pursuant to 18 U.S.C. § 1836(b)(2). An applicant for a seizure order who accepts this presumptive choice should be required to ascertain the availability of the marshal to serve and execute the seizure order within seven days of the issuance of the order before filing its application and, if the marshal is not available, to note this on its application. An applicant who requests the designation of a federal law enforcement officer other than the United States marshal to serve and execute the seizure order should be required to accompany such a request with a showing that the service and execution of the order falls within the scope of duties of this officer.

• • •

Section 1836(b)(2)(E) states that

> The court shall order that service of a copy of the order under this paragraph, and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order.

The provision does not specify which federal law enforcement officer must execute a seizure order granted under this authority. However, the United States marshal traditionally has carried out seizure orders authorized under similar provisions, such as 15 U.S.C. § 1116(d)(1)(A). Furthermore, pursuant to 28 U.S.C. § 566(a), "[i]t is the primary role and mission of the United States Marshals Service . . . to obey, execute, and enforce all orders of the United States District Courts . . ., as provided by law." Accordingly, unless the applicant requests otherwise, the Court should presumptively designate the United States marshal to execute the seizure order issued under 18 U.S.C. § 1836(b)(2).

Sections 1836(b)(2)(B)(v) and (b)(2)(F) require that the seizure hearing take place "not later than 7 days after the order has issued." In other words, the seizure must be executed within seven days of the issuance of the seizure order, as computed in accordance with Rule 6 of the Federal Rules of Civil Procedure. Because the United States marshal has other statutory functions, he or she may not be available to execute the seizure order within seven days of issuance. The applicant therefore must contact the marshal ahead of time to ensure that the order can be executed within the statutory time period. The marshal may be able to tentatively schedule the seizure on the basis of the estimated date of issuance of the order. The applicant may find it helpful to provide the marshal with a copy of the draft order, if available, for comments regarding its execution.

In some instances, another federal law enforcement officer may be better situated than the United States marshal to carry out the seizure order sought by the applicant. For example, a United States customs officer may be better placed to intercept material being carried across borders. It is incumbent on the applicant to determine which federal law enforcement officer, if not the United States marshal, is best suited to execute the order.

The applicant must not assume that all federal law enforcement officers will serve and execute process on behalf of civil litigants. If the applicant would like to have the court designate an officer other than the United States marshal to serve and execute the seizure order, the court should require the applicant to show that the officer is authorized by statute to serve and execute the order. For example, an applicant seeking to have a United States customs officer designated should at least point to 19 U.S.C. § 1589a, which states that, "[s]ubject to the direction of the Secretary of the Treasury, an officer of the customs may . . . execute and serve any order . . . or other process issued under the authority of the United States."

3. NOMINATION OF TECHNICAL EXPERTS

3-1. In General

The court should require the applicant, at the time of the filing of the application for a seizure order, to nominate as many technical experts as may be necessary to assist in the execution of the seizure order. It is preferred that the court require that the applicant explain how the nominated technical experts can collectively accomplish all work that must be performed at the locations where the material is to be seized within a period of eight hours, unless the applicant can show that extraordinary circumstances exist or that justice so requires.

• • •

Section 1836(b)(2)(E) states

> The court shall order that service of a copy of the order under this paragraph, and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order. The court may allow State or local law enforcement officials to participate, but may not permit the applicant or any agent of the applicant to participate in the seizure. At the request of law enforcement officials, the court may allow a *technical expert* who is unaffiliated with the applicant and who is bound by a court-approved non-disclosure agreement to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure.

(emphasis added)

The execution of seizure orders issued under 18 U.S.C. § 1836(b)(2) may often require the assistance of technical experts because the law enforcement officers executing the orders may not have the necessary expertise to identify the material targeted for seizure. Even if they have the expertise, the officers may not be authorized to provide such technical assistance, as the assistance may constitute subsidization of private litigation. Furthermore, the officers need the technical experts to provide guidance about the limits of seizure. The officers may not be able to determine if enough material has been seized to accomplish the objective of seizure. Finally, with respect to the United States marshal, the marshal as an officer of the court must remain neutral and therefore avoid participating in any substantive determinations in the case, such as whether a particular object contains misappropriated trade secrets. The court can therefore anticipate that, in many cases, law enforcement officers will request the assistance of the technical experts.

Accordingly, the court should require the applicant to nominate experts at the time of filing of the application, and the court should consider appointing the experts proactively when it issues the seizure order. The court, the applicant, and the officers would be ill served by waiting for the explicit request of the officers for experts and thereby forcing the applicant to return to the court to have experts appointed after the issuance of the seizure order. After all, 18 U.S.C. §§ 1836(b)(2)(B)(v) and (b)(2)(F) require that the seizure hearing take place

"not later than 7 days after the order has issued." In other words, the seizure must be executed within seven days of the issuance of the seizure order, computed in accordance with Rule 6 of the Federal Rules of Civil Procedure. To fit a separate proceeding to appoint technical experts and also the actual execution of the seizure order within those seven days would be costly and burdensome for all involved. Furthermore, § 1836(b)(2)(B)(ii) requires that the seizure order

> provide for the narrowest seizure of property and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret.

In deciding the scope of the seizure order, the court may consider it helpful to understand the work the technical experts are expected to perform while executing the order. Given this overlap between the information the court would need to consider when granting the application and when appointing the experts, there is good reason for the court to consider both issues at the same time.

The technical experts must perform all functions needed for the execution of the seizure order that law enforcement officers are unable to perform. The expertise and staffing needed will vary from case to case. Examples of technical functions include distinguishing between material that should be seized and material that should not be seized; combing through a large area to seize a small piece of material that is difficult to see; tracking down all pertinent material when there is a large volume of material targeted for seizure; and moving material that may be delicate and require special handling. It is incumbent on the applicant to anticipate challenges and identify nominees who can overcome them so that the seizure order can be successfully executed.

The longer the technical experts are present at the locations where the material is to be seized, the greater the interruption to the business operations of others. And because the law enforcement officers who carry out the seizure order generally must stay on site to maintain order and to inventory the seized material, a long seizure may prevent them from performing their other statutory duties and may therefore be contrary to the public interest. To that end, the technical experts that the applicant nominates should be capable of accomplishing their work on site in no more than a workday, that is, a period of eight hours, absent a showing that extraordinary need or circumstances warrant a longer seizure.

3-2. Disclosures

The applicant should be required to submit the following information for each technical expert nominee:

(a) Basic Information About the Nominee. *This at least includes the nominee's name, positions held, and place of business.*

(b) Expertise of the Nominee. *This at least includes a description of the expertise the nominee will provide during the execution of the seizure order, a statement of the nominee's experience, and a summary of the instructions the applicant intends to provide to the nominee.*

(c) Conflict of Interest. *This includes:*

(1) certification to the lack of any ongoing contractual or financial relationship between the nominee and the applicant or the applicant's attorney; and

(2) disclosure of all contractual or financial relationships between the nominee and the applicant or the applicant's attorney in force within two years prior to the date of filing of the application.

(d) Consent and Availability of the Nominee. *This includes*

(1) certification to the nominee's consent to serve as technical expert;

(2) certification that the nominee has been made aware of the provisions of 18 U.S.C. § 1836(b)(2) and these trade secret seizure best practices;

(3) certification to the availability of the nominee to participate in the seizure within seven days of the issuance of the seizure order as required by 18 U.S.C. §§ 1836(b)(2)(B)(v) and (b)(2)(F);

(4) certification that the applicant will pay the compensation required by the nominee; and

(5) certification that the applicant has not disclosed to the nominee the trade secrets and the material targeted for seizure as required by 18 U.S.C. § 1836(b)(2)(A)(ii)(VII).

• • •

The primary purpose of this best practice is to assist the court in making a determination about the fitness of the applicant's nominees to serve as technical experts.

Expertise of the Nominee. The duties to be fulfilled by the technical experts span all seizure-related tasks not performed by the law enforcement officers.

One of these tasks, which is critical to the success of the seizure, is the identification of materials containing misappropriated trade secrets for seizure. This identification may require two different types of technical analysis: searching for the misappropriated trade secrets by their substance and by their form.

Conceptually speaking, trade secrets have two dimensions, substance and form. The term "trade secrets" is set forth in 18 U.S.C. § 1839(3), which states in relevant part:

> the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns,

> plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing . . . .

The first portion of the cited sentence speaks to the substance of trade secrets:

> financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes

In short, the substance of trade secrets is "information."

The second portion of the cited sentence speaks to the form the trade secrets can take:

> all forms and types of . . . information . . . whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing

As can be seen in the broad reference to "all forms and types," there is virtually no limit to the forms that trade secrets may take.

Misappropriated trade secrets are identified fundamentally by a comparison of what was alleged to be misappropriated from the applicant and what is in the possession of the party against whom seizure is ordered. This comparison can be based on either a similarity in the substance or in the form.

It is helpful to consider the distinction through an example. In a somewhat typical fact pattern, a departing employee downloads files from the computers of his or her old employer in order to take the information to the new employer. In this case, the downloaded computer files represent the form of the misappropriated trade secrets, and the contents of the files are the substance. A search for the misappropriated trade secrets by form can be conducted by computational techniques such as an analysis of when or whether USB "thumb drives" have been plugged into the old employer's computer and whether the metadata of the departing employee's files match those of the old employer's. A search for trade secrets by substance, in contrast, requires looking through the contents of the employee's computer files and comparing the contents with the substance of the allegedly misappropriated trade secrets.

It can be readily appreciated that the two types of analyses require entirely different expertise. The technical expertise required for the forms of a trade secret involves the art of forensics and most likely can be found in specialized firms. This skill generally has little overlap with the expertise needed to look for the substance of trade secrets, which is the domain of the technical art associated with the trade secret itself. This substantive expertise can possibly be found in universities or among consultants.

The type of expertise required for the search of materials containing the misappropriated trade secrets during the execution of a seizure order is context-specific. The applicant ought to be prepared to explain how the expertise provided by the nominees can successfully accomplish the goal of seizure, defined explicitly in 18 U.S.C. § 1836(b)(2)(A)(i) as "prevent[ing] the propagation or dissemination of the [misappropriated] trade secret that is the subject of the action."

Conflict of Interest. Section 1836(b)(2)(E) requires that any technical expert appointed to assist in the execution of the seizure order "[be] unaffiliated with the applicant" and not be "any agent of the applicant." This best practice represents the minimum disclosure requirements thought to be necessary for the court to determine whether the nominees for technical experts fulfill that statutory requirement.

A period of two years for the disclosure of a past contractual and financial relationship was chosen based on Rule 7 of the Rules of the Supreme Court of the United States, which sets forth a two-year period of repose before a former employee of the Supreme Court may "participate in any professional capacity in any case pending before this Court or in any case being considered for filing in this Court." The court will most likely have to decide on a case-by-case basis how extensive the contractual or financial relationships must be within this period of time for a nominee to be deemed "affiliated with the applicant" and therefore disqualified from participating in the seizure.

The applicant may have, in accordance with the common practice in trade secret litigation, retained a consultant to assist with its own internal investigation prior to the filing of the suit. The court should remind the applicant that 18 U.S.C. § 1836(b)(2)(E) prohibits such a consultant from serving as a technical expert.

Consent and Availability of the Nominee. Sections 1836(b)(2)(B)(v) and (b)(2)(F) require that the seizure hearing take place "not later than 7 days after the order has issued." In other words, the seizure must be executed within seven days of the issuance of the seizure order, computed in accordance with Rule 6 of the Federal Rules of Civil Procedure. The seizure therefore may take place on short notice. It is of critical importance that the nominees be available to participate in the seizure within this time period.

For a seizure order to issue, 18 U.S.C. § 1836(b)(2)(A)(ii)(VII) requires that "the applicant has not publicized the requested seizure." Practical necessity dictates that the applicant be in direct contact with the nominees prior to the application for the seizure order and that the applicant inform the nominees of the party against whom seizure is sought, so that the nominees can perform their check for potential conflicts. However, the nominees need not and must not be made aware of the subject matter of the seizure before appointment.

The other elements governing the appointment and role of court-appointed expert witnesses are adapted from Rule 706 of the Federal Rules of Evidence.

It must be noted that the applicant bears the cost of hiring the technical experts. The DTSA provides no appropriation for the technical experts, and it implicitly contemplates that the applicant will bear the expense in accordance with former practice. Furthermore, imposing the compensation of the technical experts on the applicant would be consistent with Rule 706(c)(2) of the Federal Rules of Evidence and Rule 53(g)(2) of the Federal Rules of Civil Procedure, which permit the court to direct a party to pay for the compensation of court-appointed expert witnesses and special masters. To that end, it is incumbent on the applicant to determine if it is willing and able to pay the compensation required by the nominees before the Court appoints them as technical experts.

3-3. Locksmith Expertise

The court should require the applicant to inform the court to explicitly authorize the federal law enforcement officer designated to execute the seizure order to use force to access locked areas. The applicant should also be required to include a locksmith among the technical expert nominees if the applicant has reason to believe that such force may be needed to successfully execute the seizure order.

• • •

Section 1836(b)(2)(A)(iv) states that a seizure order must

> provide guidance to the law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including . . . whether force may be used to access locked areas . . . .

The United States marshal does not use force to break into property without explicit authorization of the Court. Furthermore, he or she does not necessarily provide the expertise to do so even if authorized to do so. Other law enforcement officers may act differently, according to the policies of their agencies.

It is incumbent on the applicant to arrange and pay for the necessary expertise if the applicant believes that it will be necessary to break into locked areas to successfully execute the seizure order. It must be noted that if locksmith expertise is used to access locked areas, the same expertise must be made available to secure the areas at the conclusion of the seizure.

3-4. Transportation Expertise

When appropriate, the court should require the applicant to include among the technical expert nominees as many transportation vendors as may be necessary to assist in the transportation of material seized pursuant to the seizure order. If special expertise is necessary to preserve and maintain the seized material during transportation, the applicant must provide a statement about the pertinent capabilities of the nominee.

• • •

The seized material naturally has to be moved away from the locations where it is seized. However, it is reasonable to expect in most instances that law enforcement officials will not participate in the transportation of seized material. The purpose of this best practice is to ensure that the necessary transportation will be arranged to facilitate the execution of the seizure order.

In most cases, special expertise will not be necessary to protect the seized material during transportation. However, when the preservation of the seized material requires special expertise, such as animal care or refrigeration, the applicant must assure the court of the pertinent expertise of the nominee.

4. NOMINATION OF SUBSTITUTE CUSTODIANS

4-1. In General

At the time of the filing of the application for a seizure order, the applicant should be required to nominate as many vendors as may be necessary to serve the court as substitute custodians of the material seized pursuant to the seizure order.

• • •

Section 1836(b)(2)(D) requires that:

> Any materials seized under this paragraph shall be taken into the custody of the court. The court shall secure the seized material from physical and electronic access during the seizure and while in the custody of the court.

The court may not always have the capability to store the seized material.

The purpose of this best practice is to ensure that the court can appoint an appropriate substitute custodian to store the seized material.

4-2. Disclosures

The applicant should be required to submit the following information for each substitute custodian nominee:

(a) Basic Information About the Nominee. *This at least includes the nominee's name, positions held, and place of business.*

(b) Expertise of the Nominee. *This at least includes*

(1) a chart comparing the measures the applicant alleges to have taken to keep secret the information to be protected by the seizure order against the corresponding measures the nominee will take to protect the seized material, justifying any deficiency in the nominee's capabilities;

(2) certification to the ability of nominee to store all seized electronic devices in Faraday enclosures; and

(3) if special expertise is necessary to preserve and maintain the seized material during storage, a statement about the pertinent capabilities of the nominee.

(c) Conflict of Interest. *This includes*

(1) certification to the lack of any ongoing contractual or financial relationship between the nominee and the applicant or the applicant's attorney; and

(2) disclosure of all contractual or financial relationships between the nominee and the applicant or the applicant's attorney in force within two years prior to the date of filing of the application.

(d) Consent and Availability of the Nominee. *This includes*

(1) certification to the nominee's consent to serve as substitute custodian;

(2) certification that the nominee has been made aware of the provisions of 18 U.S.C. § 1836(b)(2) and these Trade Secret Seizure Best Practices;

(3) certification to the availability of the nominee to store the seized material for at least three months from the date of the issuance of the seizure order;

(4) certification that the applicant will pay the compensation required by the nominee; and

(5) certification that the applicant has not disclosed to the nominee the trade secrets and the material targeted for seizure as required by 18 U.S.C. § 1836(b)(2)(A)(ii)(VII).

• • •

The disclosure requirements enumerated here mirror those of Best Practice 3-2 concerning the nomination of technical experts.

Several additional requirements should be noted.

Expertise of the Nominee. Section 1836(b)(2)(D)(i) requires that

> The court shall secure the seized material from physical and electronic access during the seizure and while in the custody of the court.

The necessary level of protection, such as surveillance cameras and ID checks for access to the seized material, is context-specific.

However, according to 18 U.S.C. § 1839(3)(A), for information to qualify as a trade secret, the owner of the information must have "taken reasonable measures to keep such information secret." The applicant for a seizure order must allege what "reasonable measures" he or she has taken to keep the information secret in order to meet the requirement of § 1836(b)(2)(A)(IV)(aa).

These "reasonable measures" are a fair and convenient metric for assessing the fitness of the nominee to serve as a substitute custodian for the seized material. The applicant should nominate and pay for a vendor who can provide at least the same level of protection given to the trade secrets prior to the alleged misappropriation. The court should require the applicant to justify any discrepancy in the level of protection the nominee will provide for the seized material.

With respect to the storage of electronic devices, 18 U.S.C. § 1836(b)(2)(D)(i) specifically directs that

> The court shall secure the seized material from physical and *electronic access* during the seizure and while in the custody of the court.

(emphasis added)

Section 1836(b)(2)(D)(ii) further requires the following

> If the seized material includes a storage medium, or if the seized material is stored on a storage medium, *the court shall prohibit the medium from being connected to a network or the Internet* without the consent of both parties,

> until the hearing required under subparagraph (B)(v) and described in subparagraph (F).

(emphasis added)

The scope of the requirement's language—"[i]f the seized material includes a storage medium"—is broad. It not only includes "traditional" computing devices, such as hard disks, laptops, and desktop computers; it also extends beyond "newer" devices, such as smart phones, digital cameras, and USB thumb drives. Devices that incorporate some sort of storage medium now include drones, cars, thermostats, and wearable technologies such as watches. More and more devices are made "smart," that is, they are computers and generally make use of information stored on storage media. It seems appropriate to presume that all electronic devices have some form of storage media; the presumption will only hold more force in the future.

Technological advances can also be observed in the wireless network connection capabilities of electronic devices. Traditionally, devices connected to "a network or the Internet" through wires and only when in their "on" state; to prevent them from connecting to the Internet a user simply kept them unplugged or turned "off." However, more and more electronic devices have the capability to connect to networks wirelessly. A large range of devices—from key fobs to household appliances to mobile phones to cars—connect to networks wirelessly. Furthermore, an increasing number of devices wirelessly connect to networks or can be electronically accessed whether or not the device is in its "on" state. Finally, from a digital forensics point of view, it may be beneficial in some cases that devices be kept "on," for example, to prevent a device from encrypting itself and destroying access to the data within.

Accordingly, a reasonable presumption for the court may be that all electronic devices have storage media and have to be prevented from wirelessly connecting to networks. The standard technique for preventing devices from wirelessly connecting to networks is to put such devices in Faraday enclosures, which act as barriers against the transmission of radio signals into and out of the enclosures and which may take various forms, such as a cage, a box, or a bag. Requiring all electronic devices to be stored in Faraday enclosures may be an expedient measure that saves the substitute custodians from having to discern which of the seized electronic devices may wirelessly connect with networks, require special protection from electronic access, or may be safely turned "off" without destruction of data.

In most cases, special expertise will not be necessary to protect the seized material in storage. However, when the preservation of the seized material does require special expertise, such as animal care, refrigeration, or humidity control, the applicant must assure the court of the pertinent expertise of the nominee.

Consent and Availability of the Nominee. Ideally, the storage services of the substitute custodians will only be needed for a short amount of time. Unrelated material should be returned as quickly as possible to the person against whom seizure was ordered. The remaining material should be of a sufficiently small quantity that the parties should be able to easily arrange for its disposition.

In practice, however, it may take time to arrange for the separation of the unrelated material and to clear it for return. This best practice therefore requires the applicant to certify to the ability of the substitute custodian to store the seized material for at least three months. Three months should be sufficient time for the parties to arrive at a workable solution about the disposition of the seized material, with or without the intervention of the court.

5. APPOINTMENT OF TECHNICAL EXPERTS AND SUBSTITUTE CUSTODIANS

5-1. In General

The court should provide a formal appointment order for each technical expert or substitute custodian.

• • •

Traditionally, when a court issues a seizure order pursuant to an ex parte application in a civil action, the applicant's attorney personally conducts the act of seizure and stores the seized material in his or her office on behalf of the court. The attorney hires contractors to assist where needed. All expenses, naturally, are borne by the applicant.

This old practice is strictly prohibited by the DTSA. Section 1836(b)(2)(E) states that

> The court shall order that service of a copy of the order under this paragraph, and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order. The court may allow State or local law enforcement officials to participate, but may not permit the applicant or any agent of the applicant to participate in the seizure. At the request of law enforcement officials, the court may allow a *technical expert* who is *unaffiliated with the applicant* and who is *bound by a court-approved non-disclosure agreement* to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure.

(emphasis added). By any definition, the applicant's attorney is not "unaffiliated with the applicant" and is an "agent of the applicant." Accordingly, the applicant's attorney is disqualified from participating in the seizure. Section 1836(b)(2)(D) further requires that

> Any materials seized under this paragraph shall be taken into the custody of the court. The court shall *secure the seized material from physical and electronic access during the seizure and while in the custody of the court*.

(emphasis added). Presumably, the "secur[ing] [of] the seized material from physical and electronic access" includes denying the applicant's attorney access to the seized material, at least until the seizure hearing described in § 1836(b)(2)(F).

This provision presents a practical puzzle. Because the DTSA provides no appropriation for the technical experts and the substitute custodians, it appears to contemplate that the applicant will bear the expense in accordance with former practice. However, the requirements that the technical experts "[be] unaffiliated with the applicant" and not be "any agent of the applicant" appear to indicate that the primary allegiance of the technical experts and the substitute custodians must reside with the court, not with the applicant who pays for their services.

Accordingly, this best practice suggests that the court provide a formal appointment order which makes clear that the applicant is not the actual client of the technical experts and the substitute custodians.

There are multiple benefits to this approach. First, an order of appointment formalizes the act of appointment as a judicial act. It eliminates disputes about whether the court itself is liable by appointing the technical experts and the substitute custodians.

Second, formal appointment of the technical experts and the substitute custodians provides them with some measure of immunity. This eliminates any claim to contract rights over the performance of the services that the applicant may have gained by paying for their services. This is particularly important with regard to the technical experts, because there is always a possibility that, when executing the seizure order, the technical experts may fail to find and seize all material that falls within the scope of the order. This danger is particularly great because of the short amount of time the experts have to familiarize themselves with the trade secrets they are tasked to find. It is contrary to the public policy underlying 18 U.S.C. § 1836(b)(2) for qualified persons to be deterred from serving as experts by the possibility of contract liability, and it is proper to vest them with some amount of immunity.

Third, the technical experts may be governed by the codes of conduct and state law governing their professions, under which they owe certain duties to their clients. A formal order of appointment ensures that such professionals know that they do not owe such legal duties to the applicant.

5-2. Elements of Appointment Orders

The appointment orders for the technical experts and the substitute custodians should contain the following elements:

(a) Statement of Duties. *This includes a statement of any investigation or enforcement duties and any limits on the authority of the technical experts and the substitute custodians. The court should direct the technical experts to jointly file a report on the tasks they performed during the seizure with the Court and the parties' counsel of record, marked "Confidential—Attorneys' Eyes Only," prior to the seizure hearing described in 18 U.S.C. § 1836(b)(2)(F). The court should also direct the substitute custodians to jointly file an explanation of the status of the seized material with the court and the parties' counsel of record, marked "Confidential—Attorneys' Eyes Only," prior to the seizure hearing. The court should additionally require the substitute custodians to await further instructions from the court about the disposition of the material.*

(b) Prohibition Against Ex Parte Communications. *This includes a prohibition on any ex parte communication with the parties relating to the seizure order outside of the Pre-seizure Briefing described in Best Practice 6 and a requirement that the technical experts or substitute custodians promptly inform the court of any attempt by the parties to initiate ex parte communication.*

(c) Compensation. *This includes the basis, terms, and procedure for fixing the compensation.*

> *(d)* Non-Disclosure Agreement. *The appointment order should incorporate by reference the non-disclosure agreement required by 18 U.S.C. § 1836(b)(2)(E). The non-disclosure agreement should at least include the following elements:*
>
> *(1) a statement that the agreement is between the court and the nominee;*
>
> *(2) a statement that the agreement is for the benefit of the parties to the litigation, their successors, and their assigns.*
>
> • • •

The elements above are largely adapted from Rule 53(b)(2) of the Federal Rules of Civil Procedure, which sets forth the elements of appointment orders for special masters. While the roles of the technical experts and the substitute custodians differ greatly from those of special masters, the rule nonetheless is instructive about what ought to be included in the appointment orders.

Several additional features should be noted.

Statement of Duties. The court can implement this best practice in part by incorporating the seizure order by reference. In addition, the court should consider requiring the technical experts and the substitute custodians to file letters with the court and the parties' counsel of record to ensure that the court and the litigants are aware of what the technical experts have done during the seizure and how the substitute custodians have handled the seized material ahead of the seizure hearing described in 18 U.S.C. § 1836(b)(2)(F).

This best practice recognizes that the letters may involve the disclosure of trade secrets belonging to the parties that are unrelated to the subject trade secret of the litigation. Consistent with 18 U.S.C. § 1836(b)(2)(D)(iii), which directs the court to "take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized," the letters should be made available to the parties' attorneys but not to the parties themselves.

Prohibition Against Ex Parte Communications. This best practice is in keeping with the spirit of 18 U.S.C. § 1836(b)(2) that neither the applicant nor the party against whom seizure is ordered may have access to the trade secrets of the other party except for the subject trade secret of the litigation. It ensures that the court will be notified in the event of a breach of the non-disclosure agreements between the court and the technical experts and the substitute custodians, while the litigation is still pending.

Non-Disclosure Agreement for Court Approval. Section 1836(b)(2)(E) requires that the technical experts appointed by the court be "bound by a court-approved non-disclosure agreement." Non-disclosure agreements are contracts. It is highly unusual that the law contemplates a contract remedy for a breach of confidence by the technical experts when the court has the inherent power to punish contempt of its orders. However, 18 U.S.C. § 1836(b)(2)(E) can be understood in view of the fact that, if a technical expert were to disclose trade secrets that it learned during the litigation, the court itself would not suffer actual, economic harm. After all, the court is not the owner of the trade secrets. Rather, it would be one or both of the parties to the litigation that would suffer economic loss. The provision therefore can be understood as giving the parties to the litigation a contract cause of action against the technical experts for

disclosure. It represents a carve-out from the immunity that the technical experts enjoy as appointees of the court.

Accordingly, the agreements required by 18 U.S.C. § 1836(b)(2)(E) is for the benefit of all parties to the litigation. So while the non-disclosure agreement necessarily is between the court and the technical experts it appoints, the agreement should make clear whom the agreement benefits.

With regard to the substitute custodians, 18 U.S.C. § 1836(b)(2)(D)(iii) specifically directs that

> The court shall take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized pursuant to this paragraph unless the person against whom the order is entered consents to disclosure of the material.

It is appropriate for the court to require substitute custodians to execute non-disclosure agreements similar to those required of the technical experts by § 1836(b)(2)(E).

Appendix to Best Practice 5.
Illustrative Appointment Orders and Non-Disclosure Agreements

The court may consider the following illustrative appointment orders and non-disclosure agreement, which implement Best Practice 5-2. It should be noted that the templates provided here were drafted to function with the illustrative language provided in the Appendix A (see page 35, *infra*) concerning the elements of the seizure order. The illustrative appointment order for the substitute custodians also implements the protections set forth in 18 U.S.C. § 1836(b)(2)(C)–(D) for the party against whom seizure is ordered and for the seized material.

ILLUSTRATIVE APPOINTMENT ORDER FOR TECHNICAL EXPERTS

Upon consideration of the ex parte application for seizure submitted by _____ (the "Applicant") and having issued a Seizure Order, hereby incorporated by reference, this Court additionally finds that the participation of a Technical Expert will aid the efficient execution and minimize the burden of the seizure.

Pursuant to 18 U.S.C. § 1836(b)(2), it is hereby ordered that:

(1) _____ is appointed as a Technical Expert to participate in the seizure. Specifically, the Technical Expert must perform the following tasks:

  (A) be briefed in a Pre-seizure Briefing by the Applicant about the material targeted for seizure and about its role in the seizure;

  (B) coordinate about the execution of the Seizure Order with the federal law enforcement officer designated by this Court to execute the Seizure Order and with the other Technical Experts and the Substitute Custodians appointed by this Court;

  (C) participate in the seizure subject to the directions of the Seizure Order and to all instructions of the federal law enforcement officer designated by this Court to execute the Seizure Order.

  The Technical Expert is directed to proceed with all reasonable diligence to complete these tasks.

(2) The Technical Expert must not publicize this Order or disclose, confirm, or deny any details relating to this Order without prior approval of this Court.

(3) The Technical Expert must not request or knowingly entertain any ex parte communication relating to the seizure order or its execution or engage in any such communication with any party, counsel, agent of a party, or person reasonably expected to transmit the communication to a party or party's agent outside of the Pre-seizure Briefing without the prior approval of this Court. Upon receiving such ex parte communication, the Technical Expert must promptly transmit to this court either

the written communication or a written summary of the oral communication with an outline of the surrounding circumstances to this Court.

(4) The Technical Expert must comply with the Non-Disclosure Agreement approved by this Court and included with this order as an appendix.

(5) The Technical Expert must be paid $_____ per hour for work done pursuant to this Order and must be reimbursed for all reasonable expenses incurred. The Applicant must pay the Technical Expert a reasonable estimate of the fees at the Pre-seizure Briefing. The Technical Expert must file a bill with this Court and the parties' counsel of record, marked "Confidential—Attorneys' Eyes Only," for any overage upon completing the tasks assigned in Section 1 of this Order, which the Applicant must promptly pay.

This Order takes effect upon the execution of the Non-Disclosure Agreement by the Technical Expert.

ILLUSTRATIVE APPOINTMENT ORDER FOR SUBSTITUTE CUSTODIANS

Upon consideration of the ex parte application for seizure submitted by _____ (the "Applicant") and having issued a Seizure Order, hereby incorporated by reference, this Court additionally finds that it is necessary to delegate custody of the seized material pursuant to 18 U.S.C. § 1836(b)(2).

Accordingly, it is hereby ordered that

(1) _____ is appointed as a Substitute Custodian to serve as custodian of the seized material on behalf of this Court. Specifically, the Substitute Custodian must perform the following tasks:

(A) be briefed in a Pre-seizure Briefing by the Applicant about the material targeted for seizure and about its role in the seizure;

(B) coordinate with the federal law enforcement officer designated by this Court to execute the Seizure Order and with the Technical Experts and the other Substitute Custodians appointed by this Court about the execution of the Seizure Order;

(C) itemize and take possession of the seized material from the Technical Experts;

(D) store the seized material under the following security measures:

(i) all physical and electronic access to the seized material must be prohibited, unless this Court explicitly orders otherwise;

(ii) all electronic devices must be stored within Faraday enclosures, although, when necessary to preserve data, they can be connected to a power source; and

(iii) _____;

(E) with the other Substitute Custodians, jointly file a letter with this Court and the parties' counsel of record, marked "Confidential—Attorneys' Eyes Only," providing an inventory of the seized material and explaining the status of the seized material, prior to the date of the seizure hearing set forth in the Seizure Order; and

(F) obey all pertinent directions of the Seizure Order.

The Substitute Custodian is directed to proceed with all reasonable diligence to complete these tasks.

(2) The Substitute Custodian must not investigate, search, or make copies of the seized material without prior approval of this Court.

(3) The Substitute Custodian must not publicize this Order or disclose, confirm, or deny any details relating to this Order without prior approval of this Court.

(4) The Substitute Custodian must not request or knowingly entertain any ex parte communication relating to the seizure order or its execution or engage in any such communication with any party, counsel, agent of a party, or person reasonably expected to transmit the communication to a party or party's agent outside of the Pre-seizure Briefing without the prior approval of this Court. Upon receiving such ex parte communication, the Substitute Custodian must promptly transmit to this Court either the written communication or a written summary of the oral communication with an outline of the surrounding circumstances.

(5) The Substitute Custodian must comply with the Non-Disclosure Agreement approved by this Court and included with this order as an appendix.

(6) The Substitute Custodian must be paid $_____ per day for work done pursuant to this Order and must be reimbursed for all reasonable expenses incurred. The Applicant must pay the Substitute Custodian a reasonable estimate of the fees at the Pre-seizure Briefing. The Substitute Custodian must file a bill with this Court and the parties' counsel of record, marked "Confidential—Attorneys' Eyes Only," for any overage upon completing the tasks assigned in Section 1 of this Order, which the Applicant must promptly pay.

This Order takes effect upon the execution of the Non-Disclosure Agreement by the Substitute Custodian.

The following illustrative language is geared toward the technical experts, and can be modified easily to refer to the substitute custodians.

It should be noted that the illustrative agreement also includes numerous other clauses, beyond those suggested in Best Practice 5-2, which the court may find useful or desirable. In particular, the illustrative agreement includes a liquidated damages provision, which may not always be appropriate. The clauses that generally should be included within non-disclosure agreements are the subject of a large body of literature; a full discussion of this subject matter is beyond the scope of this document.

ILLUSTRATIVE NON-DISCLOSURE AGREEMENT

This Non-Disclosure agreement (the "Agreement") is entered into by and between the United States District Court for the _____ District of _____ (the "Court") and _____, located at _____, its directors, officers, employees, and agents (the "Technical Expert").

WHEREAS the Technical Expert is appointed by the Court for the purpose of assisting the United States Marshal in the execution of the Seizure Order issued in the case captioned _____, __-CV-_____ (the "Litigation"), for which it will be compensated by _____ (the "Applicant");

WHEREAS the Technical Expert shall learn of information or receive material in the performance of its service for the Court (the "Confidential Information");

NOW THEREFORE, in consideration of the premises and the mutual undertakings of the Court and the Technical Expert, the Technical Expert consents to the following terms:

(1) The Technical Expert agrees

(A) to hold and maintain the Confidential Information in the strictest confidence;

(B) not to use the Confidential Information in any way, or to copy, reverse engineer, or test any product embodying the Confidential Information, except for the purpose of assisting the execution of the Seizure Order;

(C) to take all steps reasonably necessary to protect the secrecy of the Confidential Information, and to prevent the Confidential Information from falling into the public domain or into the possession of unauthorized persons, including the Applicant; and

(D) to carefully restrict access to the Confidential Information to employees, contractors, and third parties as is reasonably required, who must sign non-disclosure restrictions at least as protective as those in this Agreement.

(2) To the extent the Confidential Information is otherwise publicly available, it is public information and is not restricted by operation of this Agreement. However, if public information is provided to the Technical Expert for use in assisting the execution of the Seizure Order in a media, format, or otherwise in a manner in which it is not available to the public, such information may not be used for any other purpose by the Technical Expert except with the permission of the Court.

(3) This Agreement is made and intended for the benefit of the parties to the Litigation, their successors, and assigns (the "Beneficiaries") and may be enforced by the Beneficiaries. The Beneficiaries may seek any remedy available to them to enforce this Agreement including, but not limited to, application for a court order prohibiting the use or disclosure of the Confidential Information in breach of this Agreement. The Technical Expert further acknowledges that actual damages that are likely to result from breach of this Agreement are difficult to estimate on the date of this Agreement and would be difficult for the Beneficiaries to prove. Each Beneficiary enforcing the non-disclosure restrictions of this Agreement is entitled to liquidated damages in the amount of _____, in place of actual damages, for each unauthorized use or disclosure of the Confidential Information by the Technical Expert.

(4) This Agreement is governed by and will be construed in accordance with the laws of the state of _____. The Technical Expert hereby expressly consents to the personal jurisdiction of the state and federal courts located in _____ District of _____ for any lawsuit filed arising out of or related to this Agreement.

(5) The non-disclosure restrictions of this Agreement run from the date of this Agreement, survive the termination of this Agreement, and remain in effect until otherwise directed by court order or by agreement of the parties to the litigation.

(6) This Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

IN WITNESS WHEREOF, the Technical Expert has executed this Agreement on the date shown below.

6. SEIZURE INSTRUCTIONS

6-1. "Actual Possession" Limitation to the Scope of Seizure

The court should clearly identify the party against whom seizure is ordered. The court should also explicitly direct the law enforcement officers executing the seizure order to limit seizure to material that is in the actual possession of such party and provide detailed guidance on the meaning of "actual possession."

• • •

This best practice facilitates the efforts of the law enforcement officers executing the seizure order. It also helps the court protect the Fourth Amendment rights of persons who may be related by family or business ties to the party against whom seizure is ordered but who have not been alleged by the applicant to have misappropriated trade secrets.

The "party against whom seizure is ordered" and its variant forms, including "person against whom seizure would be ordered," "person against whom the order is directed," "party against whom the order has issued," are terms of great significance within the context of 18 U.S.C. § 1836(b)(2). The law relies heavily on these terms to set forth the boundaries of the actions that may be taken when the seizure is ordered.

In particular, 18 U.S.C. § 1836(b)(2)(IV) limits the "person against whom seizure would be ordered" to one who most likely has "misappropriated the trade secret of the applicant by improper means; or . . . conspired to use improper means to misappropriate the trade secret of the applicant." At the same time, § 1836(b)(2)(V) sets forth that an order may not be granted unless it "clearly appears" that "any property to be seized" is in the "actual possession" of the "the person against whom seizure would be ordered."

In conjunction, the two provisions limit the material targeted for seizure to "property" that is in the "actual possession" of the party whom the court has found to likely have "misappropriated the trade secret of the applicant by improper means; or . . . conspired to use improper means to misappropriate the trade secret of the applicant." The provisions also, by effect, exempt from seizure property that is merely in the "constructive possession" of the party against whom seizure is ordered. The legislative history supports this construction; Senate Report 114-220 states in relevant part:

> The requirement of actual possession contained in clause (V) serves to protect third-parties from seizure. For instance, the operator of a server on which another party has stored a misappropriated trade secret, or an online intermediary such as an Internet service provider, would not be subject to seizure because their servers, and the data stored upon them, would not be in the actual possession of the defendant against whom seizure was ordered.

The court should not assume that law enforcement officers will be sufficiently familiar with the structure and legislative history of 18 U.S.C. § 1836(b)(2) to infer this substantive limitation on the scope of the seizure authority. A clear identification of who exactly is the party against whom seizure is ordered and a clear statement that seizure is limited to material in the "actual possession" of such a party increase the likelihood that seizure will be conducted in a way that both complies with the statutory strictures of 18 U.S.C. § 1836(b)(2) and respects the substantive and procedural rights of others who are not the subject of the seizure order.

To that end, the court should not assume that law enforcement officers will generally know the legal significance of the term "actual possession" and the distinction between "actual possession" and "constructive possession." The court may consider providing guidance about the terms based on this succinct definition provided by the Supreme Court in *Henderson v. United States*:

> Actual possession exists when a person has direct physical control over a thing. See Black's Law Dictionary 1047 (5th ed. 1979) (hereinafter Black's); 2A O'Malley § 39.12, at 55. Constructive possession is established when a person, though lacking such physical custody, still has the power and intent to exercise control over the object. See Black's 1047; 2A O'Malley § 39.12, at 55.

135 S. Ct. 1780, 1784 (2015).

Furthermore, the court should be sensitive to the practical difficulties that questions of joint possession may present to the law enforcement officers executing a seizure order. Material may well be under the joint physical control of multiple parties. For example, a laptop can be shared by family members and a server can be maintained by a number of business partners. Indeed, the law recognizes this practical reality; the usage of the term "joint possession" is well-settled.

However, even when material is legally and practically in the actual possession of multiple parties, it may from a visual point of view appear to be in the actual possession of only a single party. For example, the laptop shared by family members will very likely be held or used by only one of the members at any given moment, and it will look as if it is in the sole actual possession of that member.

The possibility therefore exists that material targeted for seizure whose actual possession is shared by the party against whom seizure is ordered and a third party may appear at the time of seizure to be in the sole actual possession of the third party. And, unless given additional instructions by the court, the law enforcement officers may find no reason to think that the material is in the actual possession of the party against whom seizure is ordered and subject to seizure.

It is incumbent on the applicant to anticipate and inform the court about all foreseeable joint possession issues with regard to each piece of material that it requests to have seized. The applicant should supply all the pertinent facts, including details of the relationships between the party against whom seizure is ordered and the third parties who reasonably may be expected to be seen with direct physical control of the material targeted for seizure. Providing the court with this information will enable it to properly formulate guidance within the seizure order about the specific situations when material should be seized even when the law enforcement officers find that the material is in the direct physical control of a third party during execution of the order.

6-2. Investigation and Search

The court should instruct the technical experts not to perform any investigation or search at the locations where the material is to be seized beyond the minimum needed to identify the material targeted for seizure. The court should further order that doors and containers only be opened if there is reason to believe that the misappropriated trade secrets may be found within.

• • •

This best practice gives direction to the technical experts in their investigation or search for the material targeted for seizure.

The court generally will authorize the use of "all reasonable force in conducting the seizure" and the opening of doors and containers to locate and identify the material targeted for seizure. But experience has shown that an open-ended authorization may not help the technical experts with the practical problem of knowing how much investigation or search they should perform before concluding the seizure. After all, in most business premises and homes, there will generally be too many doors and containers for them to all be opened, investigated, and searched. The court should therefore consider providing guidance about the limits of the investigation or search the technical experts are required to do.

Section 1836(b)(2)(B)(ii) requires that a seizure order

> direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret.

Accordingly, the court should order that the technical experts perform the minimum amount of investigation or search needed to identify the material targeted for seizure. The court should further explain that doors and containers may be opened only if there is reason to believe that the misappropriated trade secrets may be found within.

Such instructions should help the technical experts understand that, for example, they may look through closets and dressers under the direction of the law enforcement officers, but they may not or need not do so unless there is reason for the investigation or search.

6-3. Electronic Storage Media

The court should authorize the seizure of an electronic storage medium or an electronic device containing an electronic storage medium only when the technical experts determine, after examination of the storage medium, that:

(a) there is reason to believe that the storage medium actually contains the misappropriated trade secrets; and

(b) it is impractical to extract the misappropriated trade secrets from the storage medium at the locations where material is to be seized.

• • •

This best practice addresses the same problem that Rule 41(e)(2) of the Federal Rules of Criminal Procedure is designed to solve in the context of warrants seeking electronically stored information. The Advisory Committee on the Federal Rules of Criminal Procedure provides the following explanation:

> *Subdivision (e)(2).* Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.
>
> The term "electronically stored information" is drawn from Rule 34(a) of the Federal Rules of Civil Procedure, which states that it includes "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained." The 2006 Committee Note to Rule 34(a) explains that the description is intended to cover all current types of computer-based information and to encompass future changes and developments. The same broad and flexible description is intended under Rule 41.
>
> In addition to addressing the two-step process inherent in searches for electronically stored information, the Rule limits the . . . [14] day execution period to the actual execution of the warrant and the on-site activity. While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a "one size fits all" presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.

Nonetheless, this best practice does not directly adopt the solution presented in Rule 41(e)(2) because 18 U.S.C. § 1836(b)(2)(B)(iii)(I) explicitly requires the court to order

> [the] protecti[on] of the seized property from disclosure by . . . prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court . . . .

Rule 41(e)(2) is built around the concept of "forensic imaging" of electronic storage media, which is, essentially, the making of a copy of storage media. The prohibition against the making of "copies, in whole or in part, of the seized property" set forth in 18 U.S.C. § 1836(b)(2)(B)(iii)(I) may have foreclosed the possibility of "forensic imaging" of storage media and may compel actual, physical seizure of storage media or electronic devices containing storage media.

The court should permit some room for independent judgment by the technical experts about the seizure of electronic storage media. As explained with regard to Best Practice 4-2, there are now many "smart" electronic devices that contain some sort of storage medium. A seizure order issued under 18 U.S.C. § 1836(b)(2) that leaves no discretion concerning the seizure of electronic storage media may require televisions to be stripped from the wall, home alarm systems to be detached from the house, cars to be driven away, and even bathroom scales to be taken. The actual seizure of all electronic devices with a storage medium in the actual possession of the party against whom seizure is ordered, even if it were feasible from a physical or practical point of view, may not be reasonable from the perspective of the Fourth Amendment.

Accordingly, the court should instruct that the technical experts first determine whether an electronic storage medium may reasonably contain the misappropriated trade secrets. If they believe it may, but they do not believe it is practical to extract the misappropriated trade secrets at the locations where material is to be seized, they may decide to physically seize the storage medium or the electronic device containing the storage medium.

6-4. Power- and Data-Related Accessories of Electronic Devices

The court should authorize the seizure of the power- and data-related accessories of seized electronic devices.

• • •

It is standard practice in the seizure of electronic devices in the criminal law enforcement context to also seize the accessories, such as power converter/adapters, sync cradles, and cables. This best practice mirrors this law enforcement practice.

Furthermore, this best practice enables the connection of the electronic devices to power sources where necessary to preserve data and also facilitates the post-seizure examination of the devices by the special master described in 18 U.S.C. § 1836(b)(2)(D)(iv).

6-5. Storage of Electronic Devices in Faraday Enclosures

The court should direct the technical experts to keep seized electronic devices in Faraday enclosures as soon as they take possession of the devices. However, the court should allow the technical experts to exercise their judgment about whether the preservation of data justifies keeping the devices in their "on" state and connecting the devices to a power source within the Faraday enclosures.

• • •

Best Practice 4-2 provides that the substitute custodians maintain seized electronic devices in Faraday enclosures. This best practice ensures that the technical experts will do so as well at the time of seizure.

With respect to the seizure of electronic devices, 18 U.S.C. § 1836(b)(2)(D)(i) specifically directs that

> [t]he court shall secure the seized material from physical and *electronic access* during the seizure and while in the custody of the court.

(emphasis added). Section 1836(b)(2)(D)(ii) further requires that

> [i]f the seized material includes a storage medium, or if the seized material is stored on a storage medium, *the court shall prohibit the medium from being connected to a network or the Internet* without the consent of both parties, until the hearing required under subparagraph (B)(v) and described in subparagraph (F).

The standard technique for preventing devices from wirelessly connecting to networks is to put such devices in Faraday bags or Faraday cages. Requiring all electronic devices to be stored in Faraday enclosures may be an expedient measure, as it saves the technical experts from having to discern which of the seized electronic devices may wirelessly connect with networks or require special protection from electronic access.

From a digital forensics point of view, it may be beneficial in some cases that devices be kept "on," for example, to prevent a device from encrypting itself and destroying access to the data within. To maintain such devices in their "on" state, it may be necessary to connect the devices to a power source, such as a portable battery. However, the connection of the devices inside a Faraday enclosure to power sources may compromise the usefulness of the Faraday enclosure, as charging wires may be able to serve as an antenna for the devices.

Thus, the decision whether to maintain a device in an "on" condition within a Faraday enclosure requires a balance of practical considerations that the court should not settle with a bright-line rule. It is appropriate to allow the technical experts to exercise discretion on this issue.

6-6. Documentation of Seizure

The court should order that the technical experts take sufficient technical notes about the seizure so that, if necessary, the material targeted for seizure can be restored to its original condition.

• • •

It is standard practice in the seizure of electronic devices in the criminal law enforcement context to take extensive documentation in order to prove both that the seizure was reasonable and proper and that the seizure was conducted in a reasonable manner. This best practice mirrors this practice.

To that end, this best practice provides a minimum standard of the sufficiency of the technical notes to be taken by the technical experts. Fairness dictates that the party against whom seizure is ordered, if it prevails, should be allowed to restore the seized material to its condition prior to seizure. The technical notes taken by the technical experts should therefore be sufficiently detailed to permit this to happen.

The court, however, should be mindful of the requirement of 18 U.S.C. § 1836(b)(2)(B)(iii)(I) that it order

> [the] protecti[on] of the seized property from disclosure by . . . prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court . . . .

The technical experts should take technical notes but should not collect documentation through the making of "copies."

7. PRE-SEIZURE BRIEFINGS

7-1. In General

The court should require the applicant, as soon as is practical after the issuance of a seizure order and prior to the execution of the seizure order, to conduct a Pre-seizure Briefing with the technical experts and the substitute custodians appointed by the court, either individually or collectively. When a corporate entity is appointed to serve as a technical expert or a substitute custodian, the corporate entity should be represented by an agent with the authority to execute agreements binding on the entity. At the Pre-seizure Briefing, the applicant should be required to instruct these appointees, answer their questions about their respective roles in the seizure, and address all potential seizure and custody issues.

• • •

Section 1836(b)(2)(A)(ii)(VII) requires, for a seizure order to issue, that "the applicant has not publicized the requested seizure." As a practical matter, the applicant for a seizure order must at least have made some indirect suggestions or inquiries in order to arrive at nominees for technical experts and substitute custodians. Still, strictly according to the letter of the law, the technical expert and the substitute custodian nominees cannot know the exact role they are to play in the execution of the seizure order prior to their appointment by the court. Accordingly, after the appointments are made, the court should formally direct that there be a briefing at which the applicant can tell the appointees what they are to do in the execution of the seizure order.

A Pre-seizure Briefing at which potential logistical issues are addressed and discussed is also important from a practical point of view. The *Asset Forfeiture Manual* of the United States Department of Justice specifically recognizes intellectual property as an asset that "creat[es] difficult and unusual problems" during seizure, and it mandates "pre-seizure planning discussions" whenever intellectual property is targeted for forfeiture. Given that trade secrets are a form of intellectual property, the reasoning that compels a "pre-seizure planning discussion" in forfeiture cases applies with equal force to cases involving seizures of misappropriated trade secrets under 18 U.S.C. § 1836(b)(2), therefore requiring a Pre-seizure Briefing.

7-2. Service of Appointment Orders, Execution of Non-Disclosure Agreements, and Payment

The court should require the applicant to begin the Pre-seizure Briefing with the following tasks:

(a) serve the appointment orders, including all documents incorporated by reference, on the technical experts and the substitute custodians;

(b) provide the non-disclosure agreements approved by the court to be executed by the technical experts and the substitute custodians; and

(c) tender a reasonable estimate of the fees to the technical experts and the substitute custodians.

The applicant should be required to promptly file a copy of the executed agreements at the end of the Pre-seizure Briefing.

• • •

The Pre-seizure Briefing is a good opportunity to take care of these important housekeeping matters.

7-3. Need for New Appointments for Technical Experts or Substitute Custodians

If, at the Pre-seizure Briefing, any of the technical experts or the substitute custodians appointed by the court inform the applicants of their inability to perform the role for which they were appointed, the court should require the applicant to immediately move the court to dissolve or modify the seizure order and nominate replacements in accordance with Best Practices 3-2 and 4-2.

7-4. Search Tools, Search Protocols, and Equipment

The court should require the applicant to provide to the technical experts at the Pre-seizure Briefing any search tool or search protocol that is to be used to identify the material targeted for seizure. The court should also require the applicant to furnish or ensure that the technical experts have all the equipment necessary to execute the seizure order, including as many Faraday enclosures as may be needed to transport electronic devices.

7-5. Record of the Pre-seizure Briefing

The court should require that the Pre-seizure Briefing be recorded by audio, audiovisual, or stenographic means. The court should ensure that the applicant bear the recording costs and that any party may arrange to transcribe the briefing. The court should order that all documents and tangible things provided by the applicant to the technical experts and the substitute custodians at the briefing be marked for identification and be made available for inspection by any party to the litigation. The court additionally should require that information disclosed at the briefing and the record of the briefing be designated as "Confidential—Attorneys' Eyes Only."

• • •

The purpose of this best practice is to ensure that there is a record of the instructions given by the applicant to the technical experts and the substitute custodians.

It is highly likely that the material that must be searched to identify misappropriated trade secrets for seizure will contain trade secrets unrelated to the litigation. There may be a strong incentive for the applicant to find ways to learn about such unrelated trade secrets even though it is not entitled to do so, and the party against whom seizure is ordered may be very suspicious of a search through this unrelated material in the execution of the seizure order. This best practice therefore aims to prevent disputes about what exactly the applicant told the persons and entities who actually executed the seizure order to look for during the seizure.

This best practice recognizes that the Pre-seizure Briefing necessarily involves disclosures of trade secrets and that the record of the briefing ought to be appropriately protected.

The court can adapt Rule 30 of the Federal Rules of Civil Procedure governing depositions when formulating its requirements about the record of the Pre-seizure Briefing.

8. APPOINTMENT OF A SPECIAL MASTER

8-1. Suggestion of a Special Master Candidate at the Filing of the Application

At the time of the filing of the application for a seizure order, the court should permit the applicant to suggest a candidate for appointment by the court as a special master for purposes of 18 U.S.C. § 1836(b)(2)(D)(iv) in accordance with Rule 53 of the Federal Rules of Civil Procedure.

• • •

In some cases, it may be impractical to perform the task of separating out the misappropriated trade secrets from unrelated material at the locations where material is to be seized. For example, the misappropriated trade secret may be distributed across too many files within a computer for the court to order the seizure of specific files from the computer. As provided for under Best Practice 6-2, the court should grant discretion to seize electronic storage media containing the electronically stored information targeted for seizure, even if the media contain clearly unrelated information.

However, the quick return of unrelated material is important, in view of this explicit statement within the Defend Trade Secrets Act of 2016 (DTSA):

> It is the sense of Congress that . . .
>
> it is important when seizing information to balance the need to prevent or remedy appropriation with the need to avoid interrupting the—
>
> (A) business of third parties; and
>
> (B) legitimate interests of the party accused of wrongdoing.

Pub. L. No. 114-153, § 5(2). To that end, 18 U.S.C. § 1836(b)(2)(D)(iv) specifically provides that

> [t]he court may appoint a special master to locate and isolate all misappropriated trade secret information and to facilitate the return of unrelated property and data to the person from whom the property was seized. The special master appointed by the court shall agree to be bound by a non-disclosure agreement approved by the court.

In other words, the DTSA contemplates that the court may appoint a special master to facilitate the return of unrelated material, even if the court retains custody of a portion of the seized material for further analysis.

The quick return of unrelated material may require a quick appointment of the special master. The purpose of this best practice is to increase the possibility that a special master can be appointed at the earliest opportunity. Rule 53 of the Federal Rules of Civil Procedure states that:

> Before appointing a master, the court must give the parties notice and an opportunity to be heard.

The earliest opportunity for the court to appoint the special master will likely be the seizure hearing described in 18 U.S.C. § 1836(b)(2)(F).

Given the short statutory time period between the issuance of the seizure order and the seizure hearing set forth in 18 U.S.C. §§ 1836(b)(2)(B)(v) and (b)(2)(F), it may be difficult for the party against whom seizure is ordered to research and suggest a candidate for appointment as the special master. Permitting the applicant to suggest, where appropriate, a candidate for the special master at the time of the filing of the ex parte application helps increase the possibility that there will be a candidate for the court's consideration by the time of the seizure hearing. It also gives some time for the party against whom seizure is ordered to research the background of the proposed special master and ascertain his or her fitness to serve as such.

In addition, it is appropriate to allow the applicant to have the first opportunity to suggest a candidate for appointment as the special master. It is important to note that the special master does not make substantive findings as to whether or not the seized material contains misappropriated trade secrets. Those findings are the province of the court. The special master's duty is to clear for return that portion of the seized material not alleged to contain misappropriated trade secrets. As a result, every decision the special master makes to clear material for return is for the benefit of the party against whom seizure is ordered and may be against the interests of the applicant. Because the special master does not and cannot make decisions adverse to its interests, the party against whom seizure is ordered may find few grounds for objecting to the appointment of a special master candidate suggested by the applicant.

Because of the possibility that the special master may erroneously return material containing misappropriated trade secrets, which would render the seizure meaningless, or may clear for return all of the seized material, which may in effect terminate the suit, the applicant has a strong interest in carefully selecting a candidate who will be capable of and competent in the special master role.

8-2. Prohibited Suggestions

The special master appointed by the court for purposes of 18 U.S.C. § 1836(b)(2)(D)(iv) should not be the technical expert appointed by the court for purposes of § 1836(b)(2)(E).

• • •

It is important that the special master not be a person or entity who participated in the seizure, so the court can ensure a second, independent review of the seized material.

9. CALCULATION OF SECURITY

The court should require that the applicant propose an amount of security to be posted for purposes of 18 U.S.C. § 1836(b)(2)(B)(vi) based on the number of hours each person is expected to be present to execute the seizure order at the locations where the material is to be seized, including the technical experts, their employees, and their contractors. The court retains the ultimate discretion to set the exact amount of security that the applicant must post, which may be higher or lower than the proposed amount, but should require the applicant to justify any request for a downward adjustment from the proposed amount.

• • •

The Defend Trade Secrets Act of 2016 states:

> It is the sense of Congress that . . .
>
> it is important when seizing information to balance the need to prevent or remedy appropriation with the need to avoid interrupting the—
>
> (A) business of third parties; and
>
> (B) legitimate interests of the party accused of wrongdoing.

Pub. L. No. 114-153, § 5(2).

The more complicated the seizure sought, the greater is the likelihood of such interruption. It is therefore appropriate that the applicant be required to propose an amount of security that is in some way tied to the complexity of the seizure. The calculating the number of hours needed by the persons participating in the seizure at the locations where the material is to be seized is a rough but useable way to estimate the amount of security required.

The court can set the amount of security the applicant must propose using the following illustrative formula:

> The proposed amount of security is set at $10,000, adjusted as follows: add $500 for each person expected to be present to execute the seizure order at the locations where the material is to be seized (including the technical experts, their employees, and their contractors, but excluding the law enforcement officers); multiply that figure by the number of hours each person is expected to be at the locations.

The illustrative formula excludes the law enforcement officers from the number of persons expected to be present to execute the seizure order because federal law enforcement officers, such as the United States marshal, will generally require the applicant to pay a separate indemnity bond and advance deposit to cover their expenses.

Requiring the applicant to perform this calculation is helpful for two additional reasons. First, to arrive at the amount of the proposed security, the applicant must carefully calculate the number of individuals and hours needed to conduct the seizure before applying for the seizure order. Second, the dollar figure gives the court a rough, but objective, indication of the technical complexity of the seizure as contemplated by the applicant.

APPENDIX A. SEIZURE ORDER

This appendix is *not* a best practice. It is a guide to assist the court in deciding how to implement the statutory requirements of 18 U.S.C. § 1836(b)(2) and the trade secret seizure best practices in the seizure order. The first two sections provide a summary of the elements that must be or should be incorporated in the seizure order; the third section provides illustrative language.

A-1. Statutory Requirements Pertinent to the Seizure Order

At the outset, 18 U.S.C. § 1836(b)(2)(B) sets forth the required elements of a seizure order. It reads, in full:

> (B) ELEMENTS OF ORDER.—If an order is issued under subparagraph (A), it shall—
>
> (i) set forth findings of fact and conclusions of law required for the order;
>
> (ii) provide for the narrowest seizure of property necessary to achieve the purpose of this paragraph and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;
>
> (iii)
>
> (I) be accompanied by an order protecting the seized property from disclosure by prohibiting access by the applicant or the person against whom the order is directed, and prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court; and
>
> (II) provide that if access is granted by the court to the applicant or the person against whom the order is directed, the access shall be consistent with subparagraph (D);
>
> (iv) provide guidance to the law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including—
>
> (I) the hours during which the seizure may be executed; and
>
> (II) whether force may be used to access locked areas;
>
> (v) set a date for a hearing described in subparagraph (F) at the earliest possible time, and not later than 7 days after the order has issued, unless the party against whom the order is directed and others harmed by the order consent to another date for the hearing, except that a party against whom the order has issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the applicant who obtained the order; and

> (vi) require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or wrongful or excessive attempted seizure under this paragraph.

Section 1836(b)(2)(B)(i) of title 18 of the U.S. Code, by referring to the "findings of fact and conclusions of law required for the order," implicitly incorporates 18 U.S.C. § 1836(b)(2)(A)(ii) by reference. Section 1836(b)(2)(A)(ii) is here duplicated in full:

> (ii) REQUIREMENTS FOR ISSUING ORDER.—The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that—
>
> (I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order;
>
> (II) an immediate and irreparable injury will occur if such seizure is not ordered;
>
> (III) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;
>
> (IV) the applicant is likely to succeed in showing that—
>
> (aa) the information is a trade secret; and
>
> (bb) the person against whom seizure would be ordered—
>
> (AA) misappropriated the trade secret of the applicant by improper means; or
>
> (BB) conspired to use improper means to misappropriate the trade secret of the applicant;
>
> (V) the person against whom seizure would be ordered has actual possession of—
>
> (aa) the trade secret; and
>
> (bb) any property to be seized;
>
> (VI) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;
>
> (VII) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and
>
> (VIII) the applicant has not publicized the requested seizure.

The court should note that other provisions of 18 U.S.C. § 1836 also apply to the seizure order. Specifically:

> (C) PROTECTION FROM PUBLICITY.—
>
> The court shall take appropriate action to protect the person against whom an order . . . is directed from publicity, by or at the behest of the person obtaining the order, about such order and any seizure under such order.
>
> (D) MATERIALS IN CUSTODY OF COURT.—
>
> (i) IN GENERAL.—
>
> Any materials seized under this paragraph shall be taken into the custody of the court. The court shall secure the seized material from physical and electronic access during the seizure and while in the custody of the court.
>
> (ii) STORAGE MEDIUM.—
>
> If the seized material includes a storage medium, or if the seized material is stored on a storage medium, the court shall prohibit the medium from being connected to a network or the Internet without the consent of both parties, until the hearing required under subparagraph (B)(v) and described in subparagraph (F).
>
> (iii) PROTECTION OF CONFIDENTIALITY.—
>
> The court shall take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized pursuant to this paragraph unless the person against whom the order is entered consents to disclosure of the material.
>
> . . . .
>
> (E) SERVICE OF ORDER.—
>
> The court shall order that service of a copy of the order . . ., and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order. The court may allow State or local law enforcement officials to participate, but may not permit the applicant or any agent of the applicant to participate in the seizure. At the request of law enforcement officials, the court may allow a technical expert who is unaffiliated with the applicant and who is bound by a court-approved non-disclosure agreement to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure.

Finally, the following provision of 18 U.S.C. § 1836 may also apply.

> (H) MOTION FOR ENCRYPTION.—
>
> A party or a person who claims to have an interest in the subject matter seized may make a motion at any time, which may be heard ex parte, to encrypt any material seized or to be seized under this paragraph that is stored on a storage medium. The motion shall include, when possible, the desired encryption method.

A-2. Best Practices Pertinent to the Seizure Order

Outside of the statutory elements, the court may consider implementing Best Practices 1, 2, 3, 6, and 7 in the seizure order.

Best Practice 5-2 suggests that the court prohibit the technical experts and the substitute custodians from engaging in ex parte communications with the parties. However, the court may consider adding an additional requirement within the seizure order forbidding the parties from initiating ex parte communications with the technical experts and the substitute custodians.

A-3. Suggestions for Implementing the Statutory Requirements and the Best Practices

The court may consider the following suggestions about the elements of the seizure order and the illustrative language implementing the requirements and practices described in the preceding two sections. It should be noted that the illustrative language is based on the assumption that the court provided separate appointment orders for the technical experts and the substitute custodians in accordance with Best Practice 5. Also, the flow of this section adheres to the logical order of the seizure order, and therefore simultaneously addresses the various statutory requirements and the trade secret seizure best practices.

At the outset, the court should consider whether it needs to issue the seizure order under seal, pursuant to the requirement of 18 U.S.C. § 1836(b)(2)(C) that the court "take appropriate action to protect the person against whom an order . . . is directed from publicity."

Section 1836(b)(2)(B)(i) and (ii) concerns why the seizure order should be granted and what the seizure is about. The parts of the seizure order that address these provisions necessarily must be tailored to the specific facts of the case. In crafting this section of the order, the court should be aware that the seizure order itself, even though arising in the context of civil litigation, is subject to Fourth Amendment scrutiny because the seizure involves some intrusion on the security of the party against whom seizure is ordered from governmental interference. The order must therefore be made to comply with the protections of the Fourth Amendment, which likely can be accomplished if the order is drafted to fully conform to the strictures of 18 U.S.C. § 1836(b)(2). Accordingly, the court should note then that § 1836(b)(2)(i) requires that the order "set forth findings of fact and conclusions of law required for the order," which, in accordance with § 1836(b)(2)(A)(ii), must be sufficiently "specific" so that "it clearly appears" that the requirements for granting seizure are met.

Sections 1836(b)(2)(E), (b)(2)(B)(iv), (b)(2)(A)(ii)(V), and (b)(2)(D)(i)–(ii) concern who may execute the seizure order, where seizure may occur, and how seizure may be conducted.

Some of the considerations are also covered in Best Practices 2, 3, 4, 5, 6, and 7. The court may consider the following illustrative language to implement the requirements and the practices:

(1) The material targeted for seizure, set forth in Appendix A, must be seized by _____ [federal law enforcement officer], assisted by the Technical Experts appointed by this Court and, if necessary, by state or local law enforcement officials, at _____. _____ [federal law enforcement officer] has discretion as to the choice of the day of the seizure; however, the seizure must occur between the hours of ____ and _____ and before the day of _____.

(2) All reasonable force may be used in conducting the seizure and doors, locks, boxes, briefcases, and containers of any type or nature may be opened to locate and identify the material targeted for seizure.

(3) In the execution of this Order, the _____ [federal law enforcement officer]must limit seizure to material that is in the "actual possession" of the party against whom seizure is ordered, identified in Appendix B. "Actual possession" means that a person has direct physical control over an object. It is to be distinguished from "constructive possession," when a person, though lacking such physical custody, still has the power and intent to exercise control over the object.

(4) Prior to the execution of this Order, the Applicant must conduct a Pre-seizure Briefing with the Technical Experts and the Substitute Custodians, either individually or collectively. When a corporate entity has been appointed to serve as a Technical Expert or the Substitute Custodian, the corporate entity should be represented by an agent with the authority to execute agreements binding on the entity.

(5) At the Pre-seizure Briefing, the Applicant must instruct the Technical Experts and the Substitute Custodians, answer their questions about their respective roles in the seizure, and address all potential seizure and custody issues. The Applicant must also perform the following tasks:

   (A) serve the Appointment Orders, including all documents incorporated by reference, on the Technical Experts and the Substitute Custodians;

   (B) provide the Non-Disclosure Agreements approved by this Court to be executed by the Technical Experts and the Substitute Custodians;

   (C) tender a reasonable estimate of the fees to the Technical Experts and the Substitute Custodians;

   (D) provide to the Technical Experts any search tool or search protocol that is to be used to identify the material targeted for seizure;

   (E) furnish or see that the Technical Experts have all equipment which they may need in the execution of the seizure order, including as

many Faraday enclosures as may be necessary for the transportation of electronic devices.

The Applicant must promptly file a copy of the executed agreements at the end of the Pre-seizure Briefing. Should any Technical Expert or Substitute Custodian appointed by this Court inform the Applicant of its inability to perform the role for which it was appointed, the Applicant must immediately move the Court to dissolve or modify the seizure order and nominate a replacement.

(6) The Pre-seizure Briefing must be recorded by audio, audiovisual, or stenographic means. The Applicant bears the recording costs, and any party may arrange to transcribe the Pre-seizure Briefing. Information disclosed at the Pre-seizure Briefing and the record of the Pre-seizure Briefing must be designated as "Confidential—Attorneys' Eyes Only."

(7) The record of the Pre-seizure Briefing must be made in accordance with the following procedure:

(A) Officer's Duties

(i) *Before the Pre-seizure Briefing.* The Pre-seizure Briefing must be conducted before an officer appointed or designated under Rule 28 of the Federal Rules of Civil Procedure. The officer must begin the Pre-seizure Briefing with an on-the-record statement that includes

(a) the officer's name and business address;

(b) the date, time, and place of the briefing;

(c) the names of the Technical Experts and the Substitute Custodians at the Pre-seizure Briefing; and

(d) the identity of all persons present.

(B) *Conducting the Pre-seizure Briefing; Avoiding Distortion.* If the Pre-seizure Briefing is recorded nonstenographically, the officer must repeat the items in section (i)(a)–(c) at the beginning of each unit of the recording medium. The appointees' and attorneys' appearance or demeanor must not be distorted through recording techniques.

(C) *After the Pre-seizure Briefing.* At the end of the Pre-seizure Briefing, the officer must state on the record that the Pre-seizure Briefing is complete and must set out any stipulations made by the attorneys about custody of the transcript or recording and of the exhibits, or about any other pertinent matters.

(D) Review by the Technical Experts and the Substitute Custodians; Changes

(i) *Review; Statement of Changes.* On request by the Technical Experts, the Substitute Custodians, or the Applicant before the Pre-seizure Briefing is completed, the Technical Experts and the Substitute Custodians must be allowed 30 days after being notified by the officer that the transcript or recording is available in which:

(a) to review the transcript or recording; and

(b) if there are changes in form or substance, to sign a statement listing the changes and the reasons for making them.

(ii) *Changes Indicated in the Officer's Certificate.* The officer must note in the certificate prescribed by section (E)(i), below, whether a review was requested and, if so, must attach any changes the appointees make during the 30-day period.

(E) Certification and Delivery; Exhibits; Copies of the Transcript or Recording; Filing

(i) *Certification and Delivery.* The officer must certify in writing that the record of the Pre-seizure Briefing accurately reflects the proceedings of the Pre-seizure Briefing. The certificate must accompany the record of the Pre-seizure Briefing. Unless this Court orders otherwise, the officer must seal the record of the Pre-seizure Briefing in an envelope or package bearing the title of the action and marked "Pre-seizure Briefing of [name of the Technical Experts and the Substitute Custodians present at the briefing]" and must promptly send it to the attorney who arranged for the transcript or recording. The attorney must store it under conditions that will protect it against loss, destruction, tampering, or deterioration.

(ii) *Documents and Tangible Things.*

(a) *Originals.* Documents and tangible things provided by the applicant to the Technical Experts and the Substitute Custodians at the Pre-seizure Briefing must be marked for identification. Any party to the litigation may inspect and copy them. The Technical Experts and the Substitute Custodians must store the originals received from the Applicant under conditions that will protect them against loss, destruction, tampering, or deterioration pending disposition at the Seizure Hearing.

(b) *Order Regarding the Originals.* Any party may move for an order that the originals be attached to the record of the Pre-seizure Briefing pending final disposition of the case.

(F) *Copies of the Transcript or Recording.* Unless otherwise stipulated or ordered by this Court, the officer must retain the stenographic notes of a Pre-seizure Briefing taken stenographically or a copy of the recording of a Pre-seizure Briefing taken by another method. When paid reasonable charges, the officer must furnish a copy of the transcript or recording to any party to the litigation, the Technical Experts, or the Substitute Custodians.

(G) *Notice of Filing.* A party who files the record of the Pre-seizure Briefing must promptly notify all other parties of the filing.

(8) The Technical Experts must accompany the _____ [federal law enforcement officer] during the seizure to identify the material targeted for seizure. The Technical Experts must itemize and take possession of the seized material, provide a copy of the inventory to the _____ [federal law enforcement officer], and deliver the seized material to the Substitute Custodians. In the performance of this task, the Technical Experts must not perform any investigation or search at the locations where the material is to be seized beyond the minimum needed to identify the material targeted for seizure. Doors and containers may only be opened if there is reason to believe that the misappropriated trade secrets may be found within. The Technical Experts must not make any copies of the material targeted for seizure, but must take sufficient technical notes about the seizure so that, if necessary, the seized material can be restored to its original condition.

(9) The seizure of an electronic storage medium or an electronic device with an electronic storage medium is permitted only when the Technical Experts determine, after examination of the storage medium, that

(A) there is reason to believe that the storage medium actually contains the misappropriated trade secrets; and

(B) it is impractical to extract the misappropriated trade secrets from the storage medium at the locations where material is to be seized.

(10) With regard to the seizure of electronic devices, the Technical Experts must seize the power- and data-related accessories of electronic devices, including sync cradles, cables, and power converter/adapters. The Technical Experts must keep the devices in Faraday enclosures as soon as they take possession of the devices. However, they may exercise their judgment about whether the preservation of data justifies keeping the devices in their "on" state and connecting the devices to a power source within the Faraday enclosures.

(11) When the seizure is completed, the Technical Experts must jointly file the following documents with the Court, all of which must be marked "Confidential—Attorneys' Eyes Only," prior to the date of the seizure hearing set forth in this Order:

(A) the inventory of seized material;

(B) a letter to the Court and the parties' counsel of record reporting on the tasks they performed during the seizure.

The Technical Experts must store the technical notes under conditions that will protect them against loss, destruction, tampering, or deterioration pending disposition at the Seizure Hearing.

Section 1836(b)(2)(H) allows the parties to request that seized computer files be encrypted. If the applicant invokes this provision at the filing of the application, the court may consider including the following illustrative language within the seizure order:

(12) The Technical Experts must encrypt, using _____ encryption method, the following seized computer files: _____. The Technical Experts must not encrypt the entire storage medium containing these computer files and must not encrypt any file not otherwise specified. The Technical Experts must store the encryption key under conditions that will protect it against loss, destruction, tampering, or deterioration pending disposition at the Seizure Hearing.

Sections 1836(b)(2)(B)(iii) and (b)(2)(D)(i)–(iii) are concerned with the protection of the seized material. The illustrative appointment order of the substitute custodians, provided in the Appendix to Best Practice 5, implements these provisions. However, as discussed in Appendix A-2, the Court may consider further restricting the parties from initiating ex parte contact with the Technical Experts and the Substitute Custodians. The Court therefore may consider inserting the following language into the seizure order:

(13) No party, counsel, or agent of a party shall engage in or knowingly cause any ex parte communication relating to this Order or its execution with any technical expert or substitute custodian appointed by the Court outside of the Pre-seizure Briefing without prior approval of this Court.

Section 1836(b)(2)(C) is concerned with the protection of the party against whom seizure is ordered. The Court may consider including the following illustrative language within the seizure order:

(14) The Applicant must not publicize this Order or disclose, confirm, or deny any details relating to this Order without prior approval of this Court.

If the court elects to implement Best Practice 1-3 without entering a standard protective order, it can insert the following illustrative language in the seizure order:

(15) Until the entry of a protective order, information designated as "Confidential—Attorneys' Eyes Only" must be treated as follows:

(A) Access to the information must be limited to the Court and its officers, the counsel of record of the parties and their office associates, legal assistants, and stenographic and clerical em-

ployees, and persons shown on the face of a document containing the information to have authored or received the information.

(B) The information may be used only for purposes of preparation, trial, and appeal of this action and may not be used under any circumstances for any other purpose.

All information must be treated in accord with the terms of the protective order upon entry.

Section 1836(b)(2)(B)(vi) requires the Court to set a security that the applicant must pay. The court can consider including the following illustrative language in the seizure order after calculating the amount of security in accordance with Best Practice 8:

(16) The Applicant must deposit with the Clerk of this Court the amount of $_____ pursuant to 18 U.S.C. § 1836(b)(2)(B)(vi) to serve as sufficient security for the payment of any damages the Defendant may be able to recover as a result of a wrongful seizure. To the extent the Defendant believes that additional security is necessary, the Defendant must file an application to the Court at the Seizure Hearing.

Section 1836(b)(2)(B)(v) states that the seizure order must set a date for the seizure hearing. The court could use standard language for this purpose, and may also consider adding a provision within the seizure order stating how the order, the summons for the seizure hearing, and related papers should be served on the party against whom seizure is ordered.

The court can include two separate appendices to the seizure order. The first, in accordance with the illustrative language provided above, setting forth a list or description of the material targeted for seizure. The second appendix, implementing Best Practice 6-1, identifying the party against whom seizure is ordered. In simple cases, this appendix can take the form of a list. The court should provide additional guidance when the material targeted for seizure will potentially be in the direct physical control of a party who is not the party against whom seizure is ordered at the time of seizure.

The Federal Judicial Center

About the Federal Judicial Center

The Federal Judicial Center is the research and education agency of the federal judicial system. It was established by Congress in 1967 (28 U.S.C. §§ 620–629), on the recommendation of the Judicial Conference of the United States.

By statute, the Chief Justice of the United States chairs the Center's Board, which also includes the director of the Administrative Office of the U.S. Courts and seven judges elected by the Judicial Conference.

The organization of the Center reflects its primary statutory mandates. The Education Division plans and produces education and training for judges and court staff, including in-person programs, video programs, publications, curriculum packages for in-district training, and Web-based programs and resources. The Research Division examines and evaluates current and alternative federal court practices and policies. This research assists Judicial Conference committees, who request most Center research, in developing policy recommendations. The Center's research also contributes substantially to its educational programs. The Federal Judicial History Office helps courts and others study and preserve federal judicial history. The International Judicial Relations Office provides information to judicial and legal officials from foreign countries and informs federal judicial personnel of developments in international law and other court systems that may affect their work. Two units of the Director's Office—the Information Technology Office and the Editorial & Information Services Office—support Center missions through technology, editorial and design assistance, and organization and dissemination of Center resources.