wgs

The Sedona Conference

Commentary on the Use of Clean Rooms

A Project of The Sedona Conference Working Group 12
on Trade Secret Law (WG12)

March 2025
Public Comment Version
Submit comments by May 16, 2025,
to comments@sedonaconference.org

The Sedona Conference Commentary on the Use of Clean Rooms

A Project of The Sedona Conference Working Group (WG12) on Trade Secrets

MARCH 2025 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editors-in-Chief

David Almeling Vicki Cundiff

Managing Editor

Casey Mangan

Senior Editor

Lauren Linderman

Contributing Editors

Jeremy Elman
Angelique Kaounis
Teresa Lewi
Lisa Zang
John Gray
Kate Lazarus
Nate McPherson

Staff Editor: Craig Morgan

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the March 2025 Public Comment Version of The Sedona Conference's *Commentary* on the Use of Clean Rooms, a project of The Sedona Conference Working Group 12 on Trade Secret Law (WG12). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG12, formed in February 2018, is "to develop consensus and nonpartisan principles for managing trade secret litigation and well-vetted guidelines for consideration in protecting trade secrets, recognizing that every organization has and uses trade secrets, that trade secret disputes frequently intersect with other important public policies such as employee mobility and international trade, and that trade secret disputes are litigated in both state and federal courts." The Working Group consists of members representing all stakeholders in trade secret law and litigation.

The WG12 Clean Rooms Brainstorming Group was launched in January 2023. Earlier drafts of this publication (including the Brainstorming Group project charter) were a focus of dialogue at the WG12 Annual Meeting in Minneapolis, Minnesota, in September 2023, and the WG12 Annual Meeting in Phoenix, Arizona, in September 2024. The editors have reviewed the comments received through the Working Group Series review and comment process.

This *Commentary* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular David Almeling, the Chair of WG12, and Victoria Cundiff, now Chair Emeritus of WG12, who serve as the Editors-in-Chief of this *Commentary*, and Lauren Linderman who serves as the Senior Editor of this *Commentary*. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including our Contributing Editors Jeremy Elman, John Gray, Angelique Kaounis, Kate Lazarus, Teresa Lewi, Nate McPherson and Lisa Zang.

The drafting process for this *Commentary* has also been supported by the Working Group 12 Steering Committee and WG12's Judicial Advisor for this *Commentary*, the Hon. Hildy Bowbeer (ret.). The statements in this *Commentary* are solely those of the nonjudicial members of the Working Group; they do not represent any judicial endorsement of any recommended practices.

Please note that this version of the *Commentary* is open for public comment through May 16, 2024, and suggestions for improvements are welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please send comments to comments@sedonaconference.org.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG12 and several other Working Groups

in the areas of artificial intelligence, electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, data security and privacy liability, and patent litigation best practices. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Kenneth J. Withers
Executive Director
The Sedona Conference
March 2025

Table of Contents

The Use of Clean Rooms Principles & Guidelines "At a Glance"

I. INTRODUCTION

A "Clean Room" is a development process designed to limit or minimize the risk of legal liability and allegations of unlawful conduct that might otherwise result if the development process were exposed to or influenced by certain information from outside the company to which the company does not have rights. Utilizing a Clean Room development process can be an effective way to develop new proprietary material (whether software, mechanisms, algorithms, business methods, or any other intellectual property) while minimizing concerns about the material's origin. The Clean Room method utilizes an isolated development environment where the possibility that certain information influences the development process is eliminated or significantly mitigated. The Clean Room is intentionally kept free from certain information and influence of third parties, such as confidential or trade secret information, copyrighted materials, licensed materials, or other nonpublic or protected information.

By conducting a development process in a Clean Room, companies take steps to ensure their creations are not the result of copying preexisting works, and that similarities, if any, between the created material and any preexisting material are coincidental. Use of a Clean Room can be an effective tool to avoid or defend against claims for, among other things, breach of a confidentiality agreement or trade secret misappropriation. A Clean Room may also be used as a tool to support (or refute) a defendant's independent development or reverse engineering claim in trade secret litigation by demonstrating that the product or information was independently developed or, alternatively, that it could not have been the result of independent development.

Designing and implementing a Clean Room may, in some situations, be a time-consuming and expensive endeavor, but it can also be critical to minimizing risk and protecting innovations. Whether to implement and how to design the Clean Room should be carefully evaluated by an organization. It is recommended that companies consult with counsel to determine whether, when, and how to implement a Clean Room, and to assist in the design and implementation of the Clean Room.

A Clean Room's effectiveness depends on its proper implementation and on relevant parties following its requirements. But there is no one-size-fits-all approach for creating and implementing a Clean Room. As such, this *Commentary* makes recommendations regarding Clean Room design that are not intended to be mandatory in any or every situation; the failure to follow the recommendations set forth in this *Commentary* does not necessarily mean the Clean Room was ineffective, just as following every recommendation set forth in this *Commentary* does not necessarily mean the Clean Room was effective. Nor should an organization's following or failure to follow the recommendations set forth in this *Commentary* be dispositive on issues relating to, for example, reasonable efforts to maintain the secrecy of trade secrets. Instead, the goals of the *Commentary* include: (1) providing a foundation for practitioners to understand what a Clean Room is, why one would be used, and when to consider using one; and (2) identifying features that may be incorporated into a Clean Room process, including identifying the key players that may be involved in designing and implementing a Clean Room. To help achieve these goals, we include as Appendix A, a Sample Clean Protocol.

This *Commentary* does not address whether a particular form of Clean Room procedure is certain to withstand scrutiny if challenged in any subsequent litigation because the Clean Room procedures discussed in this *Commentary* are not intended to be used solely for litigation purposes, and because such a conclusion depends on the circumstances at issue and is a question of fact to be determined by a judge, jury, or other fact finder.[1]

[1] Other related Sedona Conference commentaries provide useful guidance regarding Clean Rooms and related topics, including: The Sedona Conference, Commentary on the Governance and Management of Trade Secrets, 24 Sedona Conf. J. 429 (2023), available at https://thesedonaconference.org/publication/Commentary_on_Governance_and_Management_of_Trade_Secrets (discussing trade secret protection programs, including clean rooms).

II. WHAT IS A CLEAN ROOM AND WHEN SHOULD A CLEAN ROOM BE CONSIDERED?

A. Definition of a Clean Room

A "Clean Room" is a development process designed to limit or minimize the risk of legal liability and allegations of unlawful conduct that might otherwise result if the development process were exposed to or influenced by certain information—e.g., confidential or trade secret material from outside the company to which the company does not have—or may be argued not to have—rights (hereinafter "Outside Protected Information").[2] As such, a Clean Room is a deliberate form of an independent development project, often with specific protocols or procedures, designed to restrict or prevent improper or unauthorized reference to or reliance upon Outside Protected Information during development. A Clean Room development process may include, for example, isolating and/or vetting engineers, designers, or developers (the "Development Team") to limit or prevent their access to or use of Outside Protected Information such that the possibility of Outside Protected Information influencing the development process is eliminated or significantly mitigated.

The specific protocols or procedures of a Clean Room development process may differ based on the circumstances, the type of technology, the type of information involved, the capabilities or resources of the parties, the business or litigation reasons for creating the Clean Room, the history of those involved, prior development efforts, the status of general knowledge and skill in the relevant art, the level of acceptable risks given the stakes at hand, and other factors.

As discussed in further detail below, components of Clean Rooms may include: a development team that is screened from and does not have knowledge of Outside Protected Information; a team that defines the specification used by the development team; a monitor, facilitator, or other means to ensure that Outside Protected Information is screened from the development team; and a written instruction protocol for implementing a Clean Room.

The Clean Room development process may also encompass situations where there may be a need for an employee who has had access to Outside Protected Information to be involved in some aspect of the Clean Room development process. In these situations, a company may consider employing additional or alternative safeguards to further mitigate the possibility of Outside Protected Information influencing the development process.

B. Scenarios in which a Clean Room Should be Considered

There are several different scenarios in which a company may utilize a Clean Room, as further discussed in Part III.A, below. Some examples include the following:

---

[2] A Clean Room may also be used in other contexts and for other purposes, including civil and criminal claims at both the state and federal levels. The Sedona Conference Working Group 12 on Trade Secrets, and this *Commentary*, focuses on Clean Rooms in the context of trade secrets liability of allegations.

- When a company has had access to Outside Protected Information—e.g., by virtue of a license agreement, a possible licensing relationship that does not come to fruition, a non-disclosure agreement ("NDA"), a failed collaboration, merger, or joint venture, etc.—and intends to develop a similar or competing product;

- When hiring another company's former employee who had access to that company's Outside Protected Information that might provide, or be perceived to provide, a benefit to the new employer;

- In response to allegations of misconduct or during litigation, to support an independent development or reverse engineering defense to a trade secret misappropriation claim;

- After litigation, as part of a settlement or court-ordered remedy; or

- Other situations where a company or its employees might have had access to Outside Protected Information and the company wishes to take precautions to limit liability and allegations of unlawful conduct based on improper use of that Outside Protected Information in development.

III. HOW TO DESIGN A CLEAN ROOM AND WHO SHOULD BE INVOLVED IN THE PROCESS?

A. Identifying the Purpose of the Clean Room

Principle No. 1 – A Clean Room is an approach to reduce the risk of trade secret misappropriation, document independent development efforts, and/or protect innovation where the development process might otherwise be—or be alleged to have been—exposed to or influenced by Outside Protected Information.

> **Guideline No. 1** – A Clean Room Protocol describes the purpose and operation of the Clean Room. This documentation can take many forms.
>
> **Guideline No. 2** – The Clean Room participants should be aware that the purpose of the Clean Room is to confirm and document independent development; whether to provide further context depends on the specific situation.

Clean Rooms serve different purposes, and how a party implements a Clean Room may depend on the particular purpose. Companies may consider Clean Rooms in several common scenarios.

Litigation-related scenarios

A company may set up a Clean Room when it is in litigation or suspects that litigation is reasonably likely. In this case, one of the primary purposes of the Clean Room is to develop evidence the company could use in litigation. Sometimes, an expert witness could be involved in establishing the Clean Room, and other times the company may do the work alone. Either way, in this scenario, clearly documenting procedures and each step of the Clean Room can help build the record the company may want to use during litigation. (This is not to say that a formal Clean Room is necessary to prove that a company developed a product independently, or that use of a Clean Room will establish independent development.)

Clean Room development can also be part of a litigation settlement or ordered as part of an equitable remedy by a court. For example, a party to a litigation may agree or be ordered to rewrite specific sections of software code in a Clean Room environment where the code has already been determined to contain, to have used in development, or otherwise to misappropriate Outside Protected Information. See, e.g., Oakwood Labs. LLC v. Thanoo, 999 F.3d 892, 910 (3d Cir. 2021) ("The 'use' of a trade secret encompasses all the ways one can take advantage of trade secret information to obtain an economic benefit, competitive advantage, or other commercial value, or to accomplish a similar exploitative purpose, such as 'assist[ing] or accelerat[ing] research or development.").

Non-litigation related scenarios

A company might voluntarily use a Clean Room even where it faces no salient risk of litigation because it wants to reduce the chances that its products contain Outside Protected Information that

the company possesses. For example, a company might receive Outside Protected Information under an NDA as part of joint development work, joint ventures, customer/vendor relationships, merger and acquisition discussions, or any number of business dealings. Sometimes, that information could relate to a product the company wants to develop. Even if the company disclosing the Outside Protected Information has not threatened a claim for trade secret misappropriation or other misuse of the Outside Protected Information, the receiving company might institute a formal Clean Room as a precautionary measure. As another example, a Clean Room may be used to produce a device that can interoperate with another device that contains the Outside Protected Information. In yet another example, a company may want to use a Clean Room to reverse engineer and copy the functionality of some other party's product without using Outside Protected Information incorporated into that product known to the company or incoming employees at the company.

Clean Room development can also be implemented between parties that wish to share and protect limited Outside Protected Information, such as for a joint venture or other joint product development. In this case, one party may give limited Outside Protected Information to the joint developers but withhold other Outside Protected Information from developers in the Clean Room that does not directly relate to the product being jointly developed. This helps ensure that the Clean Room development team has only limited information, which can help protect both participants in the joint development from the misuse (or even the perceived misuse) of Outside Protected Information that should not be used as part of the joint product development. In this way, a Clean Room can be an important and useful development tool in situations where companies share Outside Protected Information pursuant to a written contract that explicitly states which information can be shared and which information cannot be shared or that otherwise places restrictions on the use of Outside Protected Information. For example, Company A and Company B might have technical information about how each of their product components work, and they share that information to help a joint development team combine those components into a single usable product. But Company A and Company B may also have other technical information about other components or about other aspects of product development; that information may be excluded from the Clean Room to ensure that the Clean Room team does not have exposure to the information.

The procedures employed for any given Clean Room project may vary depending on the circumstances and can be described as falling on a spectrum: Some Clean Rooms may have extremely rigorous and well-documented (and more expensive) procedures, others may have less-rigorous procedures that are still sufficient to protect against the unauthorized use of Outside Protected Information, and others may fall anywhere in between. Whether any particular restriction or set of restrictions is appropriate will depend on the situation, including the information, companies, industries, and product development involved, among other things. Therefore, the protocol and procedures described in this Commentary may not be necessary or even appropriate for every product development scenario. While a company may want (or in some cases, need) to use a Clean Room, in general, trade secret law does not mandate the use of Clean Rooms for a company to show that it

has not misappropriated trade secrets,[3] and use of or failure to utilize any of the restrictions described herein is not dispositive of whether an independent development effort was truly "independent" of Outside Protected Information.

B. Identifying what is Outside Protected Information

Principle No. 2 – The Clean Room should take reasonable measures to avoid the use of Outside Protected Information.

> **Guideline No. 1** – The information that qualifies as Outside Protected Information should be identified.

The particular information that qualifies as Outside Protected Information will vary. Companies should consider at least the following issues.

(1) If the information is subject to an NDA or other contractual confidentiality obligation, carefully review the agreement to assess whether information falls under an NDA. In some cases, not all information that the disclosing company provides to the receiving company will qualify as Outside Protected Information under an NDA. In other cases, documents or information beyond what the disclosing company provided may constitute Outside Protected Information.

(2) Although less common, a company might also possess Outside Protected Information even if that information is not governed by an NDA. In that situation, the Clean Room company should consider whether the information qualifies as a trade secret under the applicable law, as well as whether the information is protectable as non-trade secret proprietary or confidential information.

After the company and/or its counsel, as discussed below, decides what qualifies as Outside Protected Information for purposes of the Clean Room, steps should be taken to ensure that the Clean Room participants understand what is and is not Outside Protected Information, such as by defining that information in a Clean Room Protocol, which can help ensure there is a clear record of what is and is not allowed in the Clean Room.

Depending on the situation, a company may want to exclude more information from the Clean Room than is required under contract or other law. That could be to reduce the company's risk, for business-relationship reasons, or practicality reasons. If that is the case, the company should consider whether to document that it is being over-inclusive so that it does not inadvertently create a record suggesting that more information is protectable than really is.

---

[3] *See, e.g., Adacel, Inc. v. Adsync Tech., Inc*, 2020 WL 4588415, at *3 (M.D. Fla. July 9, 2020) (allowing the plaintiffs' expert to rebut the defendant's expert opinion describing how the defendant could have proceeded without misappropriating the plaintiffs' information "in so far as Defendant failed to use *one accepted method* [a clean room] for ensuring that no trade secrets were used" (emphasis added)).

C. Identifying the people

Principle No. 3 – The Manager(s) of the Clean Room process must be sufficiently familiar with the underlying issues to be able to identify people to be involved or excluded.

As a step in setting up a Clean Room, it is recommended that steps be taken to determine the relevant people who may have some involvement in the Clean Room process. Depending on the circumstances, this can include identifying:

- Who will manage the set-up of the Clean Room ("Manager(s)")?
- Which employees will be involved with the development of the product in the Clean Room?
- Which employees will be involved with the development of any specification the development team will use?
- Which employees, if any, have had exposure to the Outside Protected Information?
- Who, if anyone, will serve as the monitor for the Clean Room development ("Monitor(s)")?
- What will be the role, if any, of inside or outside counsel in the Clean Room process?

1. Individuals who will be involved with the Clean Room development process

Someone or a small group of people—the "Manager(s)"—should be involved in setting up the Clean Room (and the other activities, described below). This often will be legal counsel, but it need not be. The Manager(s) can manage and supervise the entire Clean Room set-up process, such as identifying the individuals who should be involved in the Clean Room development and who should be excluded, developing a Clean Room Protocol, supervising its implementation and progress, and addressing any questions as they may arise. The Manager(s) may or may not also be the Monitor (discussed below).

Although circumstances will differ, the Manager(s) should exercise such control and supervision as is reasonably necessary under the circumstances to make compliance with the Clean Room Protocol reasonably likely. This may include conducting periodic check-ins to, for example, assess the continued need for the Clean Room, confirm no one on the Clean Team has had unauthorized access to Outside Protected Information, and ensure the correct people are involved in the Clean Room development, among other things. The Manager(s) do(es) not necessarily need to be involved with every decision relating to the Clean Room, as many decisions may be handled by the individual employees participating in the Clean Room. However, the Manager's control and oversight should be consistent with the understanding that s/he may be held accountable for the effectiveness of the Clean Room development process.

The Clean Room should usually (though not always, see below) include individuals who are screened from and/or confirmed not to have knowledge of or exposure to Outside Protected Information—the "Clean Team." These are typically product development employees who did not have exposure to the Outside Protected Information, and in some cases depending on the circumstances and the resources available to the company, it may make sense to hire a brand-new team.

2. Individuals who may have had exposure to Outside Protected Information

In some situations, there may be individuals at the company who have had or may have had exposure to Outside Protected Information, whether by virtue of prior employment, authorized disclosure as part of the ordinary course of their job duties, or some other reason. It is often advisable to identify such individuals at the outset of the Clean Room development project. In most cases, individuals who have had exposure to Outside Protected Information will be screened from being on the Clean Team or otherwise participating in the development taking place in the Clean Room; out of an abundance of caution, individuals who may have had exposure to Outside Protected Information may also be screened out. In short, and to the extent practicable under the circumstances, anyone who may reasonably be thought to have had exposure to or familiarity with the Outside Protected Information ordinarily should not be on the development team.

In certain situations, however, it may not be possible or practical for a company to completely screen individuals who were exposed to Outside Protected Information from a Clean Room development project, e.g., when a certain employee has a unique skill set required for a development project or is a key decision-maker whose input and/or involvement in a development project is necessary. In these situations, additional safeguards may be employed to eliminate or at least significantly mitigate the possibility of Outside Protected Information influencing a Clean Room development process.

a. Screening employees who may have had exposure to Outside Protected Information from a Clean Room development project

As previewed above, if a company employee had access to Outside Protected Information, that employee will frequently be screened from a Clean Room development process. In such situations, that employee may be instructed not to communicate with the Clean Team or, at least, not to convey any Outside Protected Information to any member of the Clean Team. The Clean Team may similarly be instructed not to communicate with that employee about the Clean Room development process.

If a Clean Room development process is subject to subsequent evaluation (such as by a court or other outside party), the evaluator may closely scrutinize whether and to what extent there were communications between the Clean Team and any individuals who may have had access to Outside Protected Information, along with the content of any such communications. Where this scrutiny is likely or foreseeable, it may be advisable to block or limit direct communication between these two groups. This may not be practical in every situation, however, as the two groups may need to

communicate, for example, on unrelated subject matter or on subject matter related to the product being developed that does not implicate Outside Protected Information.

Ultimately, if employees who had or may have had access to Outside Protected Information are screened from a Clean Room development project, the design of the Clean Room should give careful attention to whether there can be any direct communications between those employees and members of the Clean Team and, if so, what procedures or protections should be put in place relating to those communications. Such procedures or protections could include instructions to keep such communications minimized, a prohibition on direct communications relating to the Clean Room development, and/or the use of a monitor to screen or be copied on all such communications, as discussed in the next section. A company may also consider having the employees with access to Outside Protected Information sign assurances saying that they have not provided Outside Protected Information to the Clean Team.

b. Use of a "Dirty Room" / "Dirty Team" and other safeguards for situations when individuals who previously had access to Outside Protected Information have some role in a Clean Room development project

As already discussed, in view of business realities, technical and geographic limitations, or for other reasons, persons who had access to Outside Protected Information may be necessary to a development project. For example, an executive who was previously involved in due diligence may need to be involved in a subsequent development project to supervise the overall development and approve the final product. As another example, an employee with a certain unique skill set may need to be involved in both the evaluation of third-party technology and the subsequent development of a company's own home-grown technology. In these situations, a company may still use various components of a Clean Room process but may wish to employ additional or alternative safeguards and processes to eliminate or at least mitigate the possibility of Outside Protected Information influencing the development process.

As one example, a Clean Room development project may include a team of individuals separate from the Clean Team who have access to information about an existing product that is available to them, regardless of whether that information constitutes Outside Protected Information—referred to as a "Dirty Team" operating in a "Dirty Room." The Dirty Room can contain documents, data, and other information, including Outside Protected Information (assuming the inclusion of such information is not barred by any applicable agreements or law) to understand the product's functionality and how to interface with it. The Dirty Team may then be tasked with preparing a functional specification to be given to the Clean Team that describes the required features of the product that will be developed in the Clean Room, but that does not include or reference any Outside Protected Information and that is not derived from and does not otherwise make use of Outside Protected Information.

In situations where a Dirty Room or Dirty Team is utilized, the purpose of the Dirty Room, how the Dirty Room and/or Dirty Team interacts with the Clean Room, the Clean Team or the Monitor (if

used) should be specified in the Clean Room Protocol. That Protocol may also describe what additional safeguards a company may employ to ensure that Outside Protected Information does not inadvertently get transferred from the Dirty Room to the Clean Room, such as, for example, requiring that all communications and documentation sent by the Dirty Room to the Clean Room first be reviewed by the Monitor, or requiring that any specification prepared in the Dirty Room must directly link any product requirement to public information or the Company's previously documented know-how. A separate Dirty Room Protocol may also be prepared.

In addition, a company may employ other safeguards to eliminate or at least mitigate the risk that Outside Protected Information will influence a Clean Room development project, where an employee who was exposed to Outside Protected Information is a necessary participant in the development project. Such additional safeguards include, for example:

- Limiting that employee's involvement to an area unrelated to Outside Protected Information or where that employee's expertise is necessary for the development project.

- Conducting an audit of the work performed by, or contributions of, that employee to confirm no Outside Protected Information was used.

- Limiting the involvement of that employee to providing high-level guidance, e.g. regarding desired product attributes, or to approving or rejecting the end product of the development project.

- Requiring that employees who had access to Outside Protected Information sign assurances saying that they have not provided Outside Protected Information to the Clean Team.

A company may also consider alternatives to the Clean Room development process to mitigate the possibility that Outside Protected Information may be used. For example, a company may choose to preemptively instruct employees involved in a development project not to use any third-party information in the course of the development project, or to only utilize information from publicly available sources. A company may also remind its employees that are participating in a development project that those employees have a legal obligation not to use the Outside Protected Information of another company in general or a specific company (e.g., if the employees were previously used in a due diligence project on a particular company). A company may also include provisions in employment agreements informing employees that they are prohibited from using or disclosing any third-party confidential or trade secret information and that they may be subject to repercussions, up to and including termination, for any violations.

Ultimately, a company has a wide variety of safeguards it may choose to employ to either eliminate or at least mitigate the possibility that Outside Protected Information is used in a development project.

3. Individuals who may be involved with monitoring the Clean Room development process

Clean Room development may or may not utilize an entity or person whose job it is to ensure that Outside Protected Information does not enter the Clean Room and/or that the ultimate product of the Clean Room development process did not utilize Outside Protected Information. When used, the "Monitor" will typically have access to all materials in the Clean Room, and among the Monitor's primary responsibilities will be to ensure that the Clean Room does not become contaminated with Outside Protected Information.

In Clean Rooms where a Monitor is used, a subsequent evaluation of that Clean Room development process will likely scrutinize the Monitor, including who served as the Monitor, what the Monitor's role was in the Clean Room development project, and more generally the effectiveness of the Monitor. Where a Monitor is used, in certain circumstances, it may be advisable to hire an independent, third-party Monitor from outside the company who has not had access to the Outside Protected Information and does not have a vested interest in the product that is the subject of the Clean Room development.[4] But in other situations where a Monitor is used, this may not be practical or necessary.[5]

Where a Monitor is used, the Monitor may screen all communications regarding the Clean Room development going into the Clean Room to ensure they do not contain or reflect Outside Protected Information and/or the Monitor may be copied on all such communications. In situations where the Monitor has received or had access to all communications going into the Clean Room, the Monitor may then be able to attest that no Outside Protected Information was communicated to the Clean Room in any of those communications.[6]

---

[4] *Resman, LLC v. Karya Prop. Mgmt., LLC,* Case No. 4:19-cv-00402, 2021 U.S. Dist. LEXIS 146422, *34 (E.D. Tex. Aug. 5, 2021) (appointing Magistrate Judge as independent monitor); *Hologic, Inc. v. Direct Digital Imaging Tech. (Beijing)*, 2018 Mass. Super. LEXIS 542, *3 (Mass. Superior Court) (appointing Magistrate Judge, who also was tasked with resolving disputes regarding clean room); *Bridgetree, Inc. v. Red F Mktg. LLC*, No. 3:10-CV-00228-FDW, 2013 WL 443698, at *23 (W.D.N.C. Feb. 5, 2013) (requiring "[a] third party 'gatekeeper,' who is an independent, third party forensic examiner with expertise in source code development and analysis, to be mutually selected by the parties").

[5] *Nordstrom Consulting, Inc. v. M & S Techs., Inc.*, Case No. 06 C 3234, 2008 U.S. Dist. LEXIS 17259, at *21-23 (N.D. Ill. Mar. 4, 2008) (not requiring independent monitor, and dismissing concern that the clean room was infected by those with knowledge of the source code at issue stating, "[e]ven if Plaintiffs could establish that the developers of the new software had access to the NCI Software, they would still need to prove that the new software is substantially similar to the NCI Software"); *ECIMOS LLC v. Carrier Corp.*, Case No. 2:15-cv-2726-JPM-cgc, 2019 U.S. Dist. LEXIS 199746, *13 (W.D. Tenn. Aug 15, 2019) (allowing company employee to serve as monitor, under direction of Special Master).

[6] *Epic Sys Corp v. Tata*, Case No. 14-cv-748-wmc, 2016 U.S. Dist. LEXIS 60344. *5 (W.D. Wis. Apr. 27, 2016) ("While plaintiff will be allowed to direct the monitor's activities, consistent with those outlined in the permanent injunction, plaintiff will not be privy to the outcome of that review, except for disclosure of any evidence of a violation of the permanent injunction itself, and defendants may seek relief from the court if they believe the monitor's activities exceed the parameters of the injunction.").

If the Monitor discovers that a communication contains the Outside Protected Information or could be reasonably construed to contain the Outside Protected Information, the Monitor should inform the Manager(s) and/or Clean Team and take steps to ensure that that information is not used or otherwise incorporated into the product being developed in the Clean Room.

When a Monitor is used, the Clean Room Protocol should consider including an instruction requiring any communications to the Clean Team to first be screened by the Monitor to verify that the communication does not contain Outside Protected Information before it is sent to the Clean Team. Alternatively, the Protocol may include an instruction that the Monitor be copied on all communications to the Clean Team, as well as an instruction that any inadvertent communication from outside the Clean Room related to development issues will be reported to the monitor. In either instance, the Monitor may examine the communication to either verify that no Outside Protected Information was shared or, if possible and as necessary, take steps to remediate any sharing of Outside Protected Information.

In situations involving the use of both a Monitor and a Dirty Team to prepare a functional specification that describes the required features of the product that will be developed in the Clean Room, the Monitor may be utilized to review the specification for any Outside Protected Information before it is provided to the Clean Team. If the Monitor determines that the specification does not contain any Outside Protected Information, the Monitor can then transfer it to the Clean Room.

When used to review the specification, if the Monitor finds Outside Protected Information, the Monitor sends the specification back to the Dirty Team to resolve the issue and eliminate any reference to, or disclosure of Outside Protected Information. The Dirty Team will rework the specification and transfer it back to the Monitor until the Monitor verifies it as containing no Outside Protected Information and transfers it to the Clean Room. If the Clean Team has questions, those questions may be routed through the Monitor first, and the Monitor may be used to review the response from the Dirty Team before it is provided to the Clean Team to ensure it does not divulge any Outside Protected Information.

A Monitor may also be utilized to verify that the final product created in the Clean Room does not contain the Outside Protected Information.

4. Involvement of counsel in the development process

Principle No. 4 – Counsel may be uniquely positioned to consult on the design of the Clean Room and whether the processes for the Clean Room are appropriate in view of the legal landscape, litigation concerns, or other legal concerns the company may have.

> **Guideline No. 1** – It is often, but not always, necessary for counsel to participate in the Clean Room process. Counsel, both inside and outside, will often play a crucial role in developing and implementing a Clean Room process and may be involved in one or more of the following functions:

- Identification of what information constitutes Outside Protected Information and what information is not Outside Protected Information.

- Identification of individuals who may have had exposure to Outside Protected Information, those individuals who did not have exposure to Outside Protected Information, and, relatedly, those individuals who should or should not have access to the Clean Room.

- Consultation regarding, or the design, preparation and set up of a Clean Room Protocol as well as other legal requirements and considerations for the Clean Room.

- Consultation regarding the product development in the Clean Room itself, *e.g.*, intellectual property counsel may provide freedom to operate advice to the members of the Clean Room in view of public intellectual property rights.

- Consultation regarding, or the implementation of, a Clean Room Protocol.

- Consulting and/or conducting periodic check-ins regarding the progress of Clean Room development and continued need for the Clean Room.

- Serving as, or consulting with the Monitor for the Clean Room, if a Monitor is used, ensuring Outside Protected Information does not go into the Clean Room.

- Consultation regarding, or the implementation of, procedures regarding the Dirty Team.

Counsel also may have responsibilities at the company, such as ethics and addressing potential legal liabilities, which require their involvement in the set up or implementation of a Clean Room. Alternatively, if a Clean Room commences during litigation, litigation counsel may need to be involved, or a court may mandate counsel involvement.

Counsel may also need to be involved in Clean Room development or implementation to ensure that applicable rules and regulations are adhered to during the Clean Room process.

Counsel may also have possession of Outside Protected Information, e.g., part of a team negotiating a failed deal during which Outside Protected Information was exchanged that the company now wants to avoid using, and therefore may need to be screened from the Clean Room development process.

Principle No. 5 – When legal counsel is involved in a Clean Room development process, care should be taken to avoid inadvertent and unintended waiver of privilege or work product protections connected to the involvement of counsel or, if waiver is reasonably foreseeable, take measures to plan and define the scope of the intentional waiver.

Guideline No. 1 – To avoid inadvertent waiver or intentional waiver with an unintended scope, consider whether the role of counsel and what aspects of Clean Room development counsel is working on should be clearly defined and memorialized.

Guideline No. 2 – To avoid inadvertent waiver or intentional waiver with an unintended scope, consider whether to divide responsibilities among separate legal counsel, such as by having one counsel advise on issues where waiver is foreseeable and a separate counsel advise on issues where waiver is not foreseeable.

Since it is often necessary to disclose various details concerning the Clean Room process employed by a company to a tribunal or third party, a company may intentionally or unintentionally waive attorney-client privilege or work product protections where counsel is involved in the Clean Room process.[7] Therefore, parties seeking to utilize a Clean Room must exercise care and consider whether and how to structure attorney involvement in the Clean Room process from the outset to avoid unintentional waiver or limit the scope of an intentional waiver.

Certain courts have held that where an attorney has communications with employees in a "Clean Room" during a development process, those communications may be "at issue" and therefore discoverable. Indeed, the communications may be determined to be "at issue" if the party challenging the Clean Room can show that it needs those communications to evaluate the effectiveness of the Clean Room.8

Similarly, other courts have indicated that where an attorney with knowledge of the Outside Protected Information is the Monitor, that attorney's communications with the Clean Room are not protected by attorney-client privilege.[9]

Courts may also reach different conclusions on whether legal advice related to the design of a Clean Room and product development in a Clean Room is protected or at issue, which may depend on what happens during litigation. For example, earlier drafts of a Clean Room Protocol reflecting legal advice may be protected from disclosure where a party challenging the Clean Room is unable to show a need for those earlier privileged drafts of the Clean Room Protocol. On the other hand, if counsel advises on freedom to operate or noninfringement of patent rights during the Clean Room development process, and if a company later affirmatively relies on that advice in a subsequent proceeding, privilege as to that advice will likely be found waived and the extent of that waiver may be hard to anticipate in advance.

---

[7] *See, e.g., Cargill Inc. v. Budine,* No. CV-F-07-349- LJO-SMS, 2008 U.S. Dist. LEXIS 72809, at *10 (E.D. Cal. July 21, 2008) (finding subject matter waiver for communications regarding clean room).

[8] See Computer Associates Intern. v. Quest Software, Inc., 333 F.Supp.2d 688, 701 (N.D. Ill. 2004).

[9] *See Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc.*, Case No. 10–CV–03428–LHK, 2013 U.S. Dist. LEXIS 18870, at *38-39 (N.D. Cal. Feb. 12, 2013) (attorneys with knowledge of the trade secrets can be appointed as monitor, even though it may waive privilege in certain circumstances).

To mitigate the risk of inadvertent waiver or intentional waiver with an unintended scope, companies should clearly define and memorialize in writing the role and responsibilities of counsel in the Clean Room development process. Companies may also consider structuring counsel involvement in a Clean Room development process, e.g., by using different counsel to perform different functions, based on how they intend to use the Clean Room and based on whether they may need to place certain communications involving counsel at issue to the extent the Clean Room is later the subject of litigation. For example, if the Monitor for the Clean Room is an in-house attorney, a company may wish to have a different in-house attorney or any outside attorney advise the development team on freedom to operate related to patent rights held by third parties.

D. Involvement of Artificial Intelligence Tools

Clean Room development may be aided by using artificial intelligence (AI) tools. Depending on how such tools are used, this could have the benefit of accumulating all available information to the Clean Room participants without human involvement or intervention, potentially lowering the possibility of human-created issues such as contamination between the Clean Room and the Outside Protected Information, bias or error. This assumes, however, that the AI tools are properly developed and customized, and that they were not themselves trained with any Outside Protected Information.

E. Preparing a Clean Room Protocol

Principle No. 6 – A Clean Room Protocol should clearly describe the restrictions put in place to prevent the Clean Team from using or incorporating Outside Protected Information in product development.

In implementing a Clean Room, it is recommended that the Clean Room procedures be documented in a Clean Room Protocol. The Protocol is designed to ensure that (1) exposure to Outside Protected Information by those in the Clean Room is extremely unlikely if not impossible and (2) a subsequent evaluator (e.g., judge or jury) would understand that from reviewing the protocol. The Clean Room Protocol is to be shared with everyone involved in the Clean Room project: the Clean Team, the Dirty Team (if any), the Monitor (if any), and any other relevant employees as necessary or appropriate for the particular Clean Room project (e.g., project managers, administrative staff, executives, etc.).

Note that while the following discussion of the elements that may be included in a Clean Room Protocol contains recommended guidelines, these are not exclusive and other methodologies not described herein can also be used by an organization to protect against the disclosure or use of Outside Protected Information. The company developing the new product should seek advice from competent lawyers and business advisors about its specific situation and requirements. Again, the use of or failure to utilize any of the recommended guidelines discussed herein is not dispositive of the effectiveness of any Clean Room development project.

Whether a particular Clean Room implements more or less stringent measures may depend on several factors,10 including the goal(s) of the Clean Room; the industry11; the physical, financial, and practical limitations of the particular company in question; the specific development at issue; and other factors. As one court has explained, however, a Clean Room "is a valuable exercise only if procedures are followed to make certain that no improper material passes through the walls."12

The Clean Room Protocol may include the following:

- A description of the reason for, or purpose of implementing the Clean Room;
- The physical location of the Clean Room and/or Dirty Room (if applicable) and access control measures, if any;
- The virtual location of the Clean Room and/or Dirty Room (if applicable) and access control measures, if any;
- Identification of the Outside Protected Information that should not be disclosed to the Clean Team;
- Identification of the individuals who are on the Clean Team;
- Identification of individuals who have had exposure to Outside Protected Information and/or Dirty Team, if any;
- Identification of the Manager and/or Monitor(s), if any;
- Instructions and procedures to be followed throughout the Clean Room development process;
- Identification of any documents or materials to be provided to the Clean Team and/or Dirty Team (if any), such as a specification;

---

10 *See Miller UK Ltd. v. Caterpillar, Inc.*, No. 10-CV-03770, 2015 WL 10818831, at *6-7 (expert opinion excluded on question of whether "clean room design was necessary or appropriate *under the circumstances*" (emphasis added)).

11 *See, e.g., Comet Techs. USA Inc. v. XP Power LLC*, No. 20-CV-06408-NC, 2022 WL 2442810, at *2 (N.D. Cal. Mar. 2, 2022) (expert opinion on "an industry standard of clean room procedures to separate employees hired from competitors").

12 *Computer Assocs. Int'l v. Quest Software, Inc.*, 333 F. Supp. 2d 688, 701 (N.D. Ill. 2004); *cf. UPI Semiconductor Corp. v. Int'l Trade Comm'n*, 767 F.3d 1372, 1381-82 (Fed. Cir. 2014) (even where accused company "took steps to insulate its new product lines from any misconduct that took place in the past" and "engaged outside design firms to create new layouts and schematics," its efforts were insufficient to qualify as a trade secret clean room in light of evidence of contamination).

- An instruction to raise any issues regarding the Clean Room Protocol promptly; and
- Signed assurance/affirmation by each relevant person that the person will comply with the Protocol.

1. Purpose Description

Guideline No. 1 – To enable participants and evaluators of a Clean Room to understand the purpose of the Clean Room development, it may be helpful for the Protocol to set forth a description of the purpose of the Clean Room.

The purpose of the Clean Room development should usually be well defined from the beginning so that all participants understand what the goal is. Many employees may be unfamiliar with what a Clean Room is or why it is being implemented. It is usually recommended that the Protocol describe, at a high level, what a Clean Room is and the specific facts for why the company is implementing the Clean Room in a particular situation.

For example, the Protocol might explain that certain employees at the company had access to a competitor's Outside Protected Information as part of a license agreement that is expiring; rather than renewing the license, the company has decided to develop its own competing technology internally. To protect its innovations and guard against the risk of intellectual property claims from the competitor, the company has decided to implement a Clean Room development process whereby the employees working on the development of the new technology will not have any exposure to the competitor's Outside Protected Information.

As another example, the Protocol might explain that there is a dispute with a third party as to whether the company has the right to use certain information or the scope of the company's rights to use certain information. In such circumstances, the Protocol may explain that, out of an abundance of caution and to avoid or minimize disputes, the company has decided to implement a Clean Room development process.

2. Identification of the Outside Protected Information

Guideline No. 2 – To allow relevant individuals to identify the Outside Protected Information that should not be used by the Clean Team, consider whether the Protocol should describe, without disclosing, the Outside Protected Information.

To ensure there is no confusion about what is or is not allowed in the Clean Room, it is usually recommended that the Protocol identify the Outside Protected Information at issue. This should be done in a sufficient level of detail so the relevant individuals are able to identify the Outside Protected Information that should not be accessed by the Clean Team, but without disclosing the Outside Protected Information in the Protocol itself.

For example, using the same example as above, the Protocol might include the definition of "Confidential Information" as used in the license agreement and/or identify the specific types or categories of Outside Protected Information belonging to the competitor to which the company had access in the ordinary course of the licensing relationship to which it no longer has rights.

3. Identification of Clean Room Participants

Guideline No. 3 – To maintain an accurate record of Clean Room participants and facilitate compliance with the Clean Room Protocol, consider whether the Protocol should identify the individuals on the Clean Team, any individuals with exposure to or familiarity with the Outside Protected Information (such as those on the Dirty Team), the Manager(s), and/or any Monitor of the Clean Room.

a. Identification of Clean Team

The Protocol should usually identify, by name, the individuals who are on the Clean Team. If additional individuals are added to the Clean Team or members are removed, the Protocol should be updated accordingly and note the dates when each person joined or was removed.

Consideration may be given to requiring Clean Team members in particular situations to complete questionnaires concerning exposure to Protected Materials in order to establish their lack of exposure. For example, a questionnaire could more specifically probe an individual's prior work history with particular industry standard technologies and/or competitor-specific technologies (without disclosing the confidential details of such competitive technologies). Experience with the former could be beneficial to support a demonstration of independent development, while experience with the latter may counsel in favor of excluding the individual from the Clean Room development.

b. Identification of Individuals with Exposure to Outside Protected Information and/or Dirty Team

As noted above, individuals at the company with exposure to or familiarity with Outside Protected Information should not be on the Clean Team. In addition, where a Dirty Team is utilized, the Protocol should usually identify, by name, the individuals who are on the Dirty Team; if additional individuals are added to the Dirty Team or members are removed, the Protocol should be updated accordingly and note the dates when each person joined or was removed.

c. Identification and Role of the Monitor

If a Monitor is used, the person or persons designated as Monitors should usually be identified, by name, in the Protocol. If an outside company is designated as a Monitor, only specific employees of that company should be allowed to act as Monitors, and those persons should be named in the Protocol. Any people who are subsequently designated as Monitors or who are removed as Monitors should be noted in the Protocol, along with the dates when each person became or ceased being the Monitor. The role of the Monitor may be discussed in the Protocol, including the mechanisms

employed by the monitor—e.g., reviewing materials before they can be shared with a clean team; monitoring only between specific members of the development team; or periodic monitoring or testing of development documents for contamination.

The benefit of having an outsider as the Monitor is that they can be truly independent. Indeed, some courts have appointed a neutral, or even a magistrate judge, to oversee clean rooms. This removes any potential bias towards the company whose technology is being monitored. The downside of having an outsider is that although the outsider may have familiarity with the legal aspects of the case, s/he may not be as familiar with the technology and therefore may not recognize what is or is not Outside Protected Information.

The benefit of having an insider, such as an attorney or an engineer, as the Monitor is that they are likely to have better familiarity with the at-issue technology and thus an enhanced ability to keep out Outside Protected Information. They are also more likely to be familiar with the company's documents, data and procedures. The downside of having an insider as the Monitor is that they may be biased—or be perceived as being more biased—towards the company whose technology is being monitored, whether expressly or implicitly.

4. Clean Room Protocol Instructions and Procedures

Guideline No. 4 – To ensure that Clean Room participants understand their obligations and the procedures to be followed under the Protocol, consider whether the Protocol should contain clear instructions and procedures for the Clean Room and the Company maintains records of such instructions and procedures. The Clean Room Protocol instructions and procedures may include the following:

a. Instructions to the Clean Team

This section of the Protocol gives the Clean Team the specific instructions and procedures they are to follow in connection with the Clean Room development project—*i.e.*, the dos and don'ts. For example, instructions and procedures may include:

- Do not ask others who have had exposure to the Outside Protected Information to disclose Outside Protected Information or otherwise disclose any information about the Outside Protected Information;

- Keep a log of resources used or consulted—for example, keep a list of any documents provided to the Clean Team, any articles relied upon, and any products to which the Clean Team had access for purposes of reverse engineering (including when and how those products were obtained, receipts, etc.). To the extent that the company's ordinary development process is already documented using standard application development procedures that are themselves documented, trained on, and monitored for compliance, this step may be redundant.

- Follow the established communication methods and procedures (see below).

- Prepare periodic reports on the development timeline and progress (see below).

It may be helpful to conduct training on the Clean Room Protocol instructions and procedures for the Clean Team. The training may include an opportunity for members of the Clean Team to seek clarification on aspects of the instructions and procedures, either during the training or later during the development process.

b. Instructions to the Individuals with Access to Outside Protected Information and/or Dirty Team (if any)

This section of the Protocol gives any individuals who have or have had access to Outside Protected Information specific instructions and procedures they are to follow in connection with the Clean Room development project—*i.e.*, the dos and don'ts. For example, instructions and procedures may include:

- Do not disclose Outside Protected Information or any information about the Outside Protected Information to the Clean Team;

- Keep a log of resources used or consulted—for example, keep a list of any Outside Protected Information provided to the Dirty Team and any products to which the Dirty Team had access for purposes of reverse engineering (including when and how those products were obtained, receipts, etc.).

- Follow the established communication methods and procedures (see below).

- Keep a log of any materials provided to or communications with the Clean Team (if any).

c. Periodic Reports

In certain circumstances, the Clean Team may be required to prepare regular reports on its activities, for example, if the Clean Room is required by a court order or where the organization requires periodic progress reports or deems such reports advisable under the circumstances. If the Clean Team is instructed to prepare regular reports on its activities, the Protocol can specify the format and frequency of those reports, who is responsible for preparing the reports, to whom the reports should be submitted, and, depending on the circumstances, generally what type of information should be included in the periodic report.

d. Location of the Clean Room and/or Dirty Room

The Protocol can explain that a "Clean Room" is a place—that may or may not be an actual, physical room or space—where developers, scientists, and other employees have no exposure to any materials that contain or could contain the Outside Protected Information.

In certain situations, the Clean Room may be a physical space where access can be monitored and verified—for example, a room that can be accessed only by certain authorized personnel with a keycard or other system that tracks entry and exit. When a physical space is utilized, consider specifying in the Protocol the location of the Clean Room and including instructions around access restrictions, etc. In other situations, there may be no separate "room" at all, and the term "Clean Room" is simply a metaphor for a development process that is clean from Outside Protected Information.

Similarly, in situations where the Clean Room development project involves a Dirty Team, there may be an actual, physical room or space—the "Dirty Room." Again, where used, the location of the Dirty Room should usually be specified in the Protocol and should be in a different location from the Clean Room.

The Protocol may identify virtual locations (e.g., network folders, databases) where developers, scientists, and other employees may access any materials to be used for the Clean Room development. When virtual locations are utilized, the Protocol should usually specify those locations and include instructions regarding such locations, such as access restrictions.

Similarly, in situations where the Clean Room development project involves a Dirty Team, there may be virtual locations identified to house Outside Protected Information. Where used, the virtual locations of the Outside Protected Information may be specified in the Protocol and should usually be in a different location than the virtual Clean Room development materials. Clean Team members should not have access to the virtual locations of the Outside Protected Information, and access should be monitored as needed.

e. Communications methods and procedures

This section of the Protocol should usually specify any instructions regarding communications to or from the Clean Team. It should usually specify *how* communication is to take place and/or any restrictions on the methods of communication that are allowed—e.g., hardcopy documents, email, flash drives or other removable drives, collaboration software (e.g., MS Teams, Slack), etc. It should also usually specify *whether* communications may be made directly to the Clean Team or, in situations where a Monitor is used, if the Monitor must be copied or if any communications must first be screened by the Monitor before being passed to the Clean Team. And it should usually specify what information should be included in any communication—e.g., to clearly identify or label the communication as relating to the Clean Room development project.

To the extent any individuals with access to Outside Protected Information and/or the Dirty Team have communications with the Clean Team (directly or through a Monitor), it is usually recommended that instructions be given about the dos and don'ts of the content of those communications. Such instructions may include, for example:

- Provide only high-level specifications or business requirements to the Clean Team that do not disclose Outside Protected Information or any information about the Outside Protected Information;

- Keep a log of any communications or information provided to the Clean Team, including the date and content of the communication, and to whom and from whom it was sent. To the extent that the company's ordinary development communications are already documented using specific means (e.g., ticketing system) via standard application development procedures that are themselves documented, trained on, and monitored for compliance, this step may be redundant. Further, to ensure such communications are properly maintained, consider establishing a minimum length of time for archiving that may exceed the company's standard documentation practices.

- Any communication with or information provided to the Clean Team may be closely scrutinized if the Clean Room is later challenged, for example, in any subsequent litigation. For that reason, it is usually recommended that any such communications be kept to a minimum and that care is taken to ensure that no Outside Protected Information is disclosed (inadvertently or otherwise).

f. Identification of Documents and Materials

It is usually recommended that the Protocol list those documents and materials that will be provided to the Clean Team and Dirty Team (if any), including any hardware or software. Any documents discovered later or determined to be necessary during the development procedure should usually be added to this list.

g. Instruction to Raise Issues

The Protocol should usually be set up so that any violations, while not impossible, would almost certainly be noticed and recorded so that steps to remediate those violations could be taken. To this end, those involved in the Clean Room development process should be instructed to raise any issues or potential issues immediately. For example, the Protocol may state: "If you realize at any point that you or another member of the Clean Team have had exposure to Outside Protected Information, notify [insert contact person] immediately."

If an issue is raised, the Monitor or others should determine whether any Outside Protected Information was disclosed to the Clean Team. If so, the company may need to determine how best to resolve the situation, which may depend on the specific facts of the situation, including the type of disclosure, to whom the disclosure was made, the purpose of the Clean Room,[13] etc. Resolutions may include, for example:

[13] For example, in the case of a court-ordered clean room, the fact of the disclosure of Protected Information may need to be disclosed to a judicial officer to determine the appropriate remedy.

- Removing certain individuals from the Clean Room development project who have violated the Protocol;

- Removing certain individuals from the Clean Team if they have been exposed to Outside Protected Information; or

- Issuing instructions to the Clean Room on how to not use the Outside Protected Information and/or how to remedy any taint.

- Quarantining the relevant documents and information.

- Taking other measures to ensure and to document that the Outside Protected Information was not further used or incorporated into any products.

- Terminating the Clean Room development project and starting the process over from the beginning with a new Clean Team.

Considerations of what resolution(s) to use may include the following:

- Whether Outside Protected Information was used by the Clean Team, and whether that information truly is trade secret or confidential or instead was kept from the Clean Team only out of an abundance of caution;

- Whether the Dirty Team communicated directly or indirectly with the Clean Team, and the nature of the communication;

- Whether any Outside Protected Information that was used affects the entire project, or only a separable portion of the project;

- How far along the project is and how important the Outside Protected Information was to the development; and

- The purpose of the Clean Room

5. Signed Assurance/Affirmation

Guideline No. 5 – To document that Clean Room participants and other relevant

individuals will comply with the Protocol, consider whether the Protocol should include a signed acknowledgement.[14]

It is usually recommended that everyone involved in the Clean Room project sign agreements not to violate the Protocol and to commit to following the documented procedures. This includes everyone on the Clean Team, the Dirty Team (if any), the Monitor (if any), and any other relevant employees as necessary or appropriate for the particular Clean Room project (*e.g.*, project managers, administrative staff, executives, etc.). All people involved should understand the importance of the development project and the seriousness of the endeavor. They should also be advised that violations of the procedures may have serious consequences.

In addition, at the end of the Clean Room project, consider whether to have everyone involved in the Clean Room project attest that they have not used any Outside Protected Information. In some circumstances, a company may also wish to obtain signed attestations from employees *outside* the Clean Room, saying that they did not give any Outside Protected Information to the development team. In addition, if an employee involved in the Clean Room project gives notice that he or she intends to leave the company prior to the end of the Clean Room project, a company may also wish to obtain a signed attestation from that employee prior to his or her departure confirming that that employee did not use Outside Protected Information during the course of his or her participation in the Clean Room project.

[14] *See, e.g.*, *Bridgetree, Inc. v. Red F Mktg. LLC*, No. 3:10-CV-00228-FDW, 2013 WL 443698, at *23–24 (W.D.N.C. Feb. 5, 2013) (specifying that only employees and agent who had no exposure to the trade secret would be allowed to enter the clean room, also requiring that they read the court order and sign an affidavit that they would comply).

APPENDIX A: SAMPLE CLEAN ROOM PROTOCOL[15]

Clean Room Protocol for Development of [Insert Description]

Date:

To: Recipients ("Clean Team"):

List full name of all recipients—i.e., the "Clean Team"

Purpose of Protocol and Identification of Outside Protected Information:

As you know, [Company] is planning to develop its own [insert description], without relying on, using, or referencing any confidential or trade secret material from outside [Company] to which [Company] does not have rights [or to which [Third Party] has alleged [Company] does not have rights] (hereinafter "Outside Protected Information"), including but not limited to any Outside Protected Information [Company] may have obtained or had access to from [Third Party]. The purpose of developing [insert description] in a Clean Room environment is to protect [Company's] innovations and minimize the risk that [Third Party] could argue that [Company] infringed its intellectual property [and/or violated the terms of its contract with [Third Party]]. This document describes a protocol to implement and operate such a Clean Room.

[If contractual restrictions are at issue, relevant provisions may be included in the protocol and/or an appendix to the protocol—e.g.:

[Company's] contract with [Third Party] prohibits [Company] from, among other things, copying, altering, decompiling, reverse engineering, disassembling, or creating derivative works from [Third Party's] [product—e.g., "software," "hardware," "technical documentation," etc.]. In short, [Company] cannot use [Third Party's] [product] to develop [insert description]. A copy of the relevant provisions of [Company's] contract with [Third Party] are attached as Exhibit A to this Protocol.]

or

[15] This Sample Clean Room Protocol represents WG12's views about certain aspects of clean room development, including when a protocol may be provided, what a protocol may contain, and how a protocol may be tailored to the specific development process at issue. The Sample Clean Room Protocol is not intended to state or displace current law regarding clean rooms, which is developing and often fact dependent and thus does not lend itself to the development of more authoritative Best Practice recommendations. Rather, the Sample Clean Room Protocol is intended to constitute a practical example of WG12's consensus Principles and Guidelines regarding such a protocol. In certain circumstances, it may also be appropriate to put a similar protocol in place for the "Dirty Team" or "Specification Team" as described above in Part III.C.2.

[Third Party] disclosed certain Confidential Information to [Company] pursuant to the [contract]. [Company's] contract with [Third Party] defines "Confidential Information" as [insert definition].]

[Where contractual restrictions are not at issue, a description of the Outside Protected Information that does not disclose any protected details of the information itself may be included in the Protocol and/or an appendix to the Protocol—e.g.:

Company is prohibited from using certain chemical combinations developed by competitor [*insert name*] for improving jet fuel burn rates.]

Procedures:

Below are instructions and procedures to help ensure and demonstrate that [Company's] development efforts are independent of any [Third-Party] Outside Protected Information. In general, the Clean Team's development activities should be independent from activities of any [Company] employees who may have had exposure to any [Third-Party] Outside Protected Information.

[*Include as applicable*: **Team Members: Specification Team**

You will be provided with a Specification to assist the Clean Team in developing [insert description]. The Specification will describe the required features of the product that will be developed in a way that does not use, contain, or disclose any Outside Protected Information. The following individuals were involved in developing Specification:

List full name of all participants.]

Team Members: Clean Team

Prior to any involvement with the Clean Team, all Clean Team members must have signed non-disclosure/confidentiality agreements with the Company. No persons who have had exposure to any [Third-Party] Outside Protected Information shall have any involvement with the Clean Team's development activities.

[*Include as applicable:* The following persons may have had exposure to [Third-Party] Outside Protected Information: [insert list of full names or append as Exhibit].]

Do not ask anyone who may have had exposure to Outside Protected Information to disclose Outside Protected Information to you or otherwise disclose any information about the Outside Protected Information to you.

The Manager(s) will manage and supervise the entire Clean Room setup process. The Manager(s) shall be [name and contact information].

[*Include as applicable:* The Manager shall be accountable for the Clean Room development process.]

[*Include as applicable:* The Monitor is responsible for screening communications with and between members of the Clean Team to avoid contamination [OR to ensure they do not contain or reflect Outside Protected Information]. [AND/OR The Monitor is responsible for reviewing the Specification before it is provided to the Clean Team to ensure it does not contain or reflect Outside Protected Information]. The Monitor shall be [name and contact information].]

Record Keeping and Use of Materials

Keep records of the independent development.

[*Include as applicable*: The following materials will be provided to you and may be used by you during the Clean Room development process: [insert list and update as needed].]

[*Include as applicable*: Only materials in Appendix [__] to this Protocol may be provided to the Clean Team.]

Keep a log of resources used or consulted during the Clean Room development process—for example, keep a list of any documents provided to the Clean Team, any articles consulted, and any products to which the Clean Team had access for purposes of reverse engineering (including when and how those products were obtained, receipts, etc.). The documentation should include as much detail as feasible about the individuals involved, the products and processes developed (including when and where such products and processes were developed), and all sources of information.

[*Include as applicable*: Ordinary application development procedures should be used to document resources used or consulted during the Clean Room development process.]

[*Include as applicable*: Clearly mark the documents used as part of the Clean Room development process.]

Keep records of instructions given to the Clean Team.

[*Include as applicable:* Keep all communications or information provided to the Clean Team, including the date and content of the communication and who it was sent from and to.]

[*Include as applicable*: To the extent that the company's ordinary development communications are already documented using specific means (e.g., ticketing system) via standard application development procedures that are themselves documented, trained on, and monitored for compliance, you may rely on such processes to document Clean Room development.]

[*Include as applicable*: To ensure Clean Room development communications are properly maintained, such communications shall be maintained through archiving for [insert a minimum length of time that may exceed the company's ordinary documentation practices].]

Physical/Virtual Spaces

[*Include as applicable*—i.e., when using a separate physical space for Clean Room development: The Clean Room shall be located in [___].

[*Include as applicable:* The Clean Room may be accessed only using keycards. No piggybacking on keycard access shall be permitted.]

[*Include as applicable:* Members of the Specification Team shall not have access to the Clean Room.]

[*Include as applicable:* No Outside Protected Information should be brought into the Clean Room [AND/OR] no resources may be brought into the Clean Room without the approval of the Monitor.]

[*Include as applicable*: Resources used or consulted during the Clean Room development shall not be removed from the Clean Room.]

[*Include as applicable*: A separate Dirty Room which may contain documents, data, and other information used to develop [interface/competing technology/etc.] shall be located at [___].]

[*Include as applicable:* The Dirty Room may be accessed only using keycards. No piggybacking on keycard access shall be permitted.]

[*Include as applicable:* Members of the Clean Team shall not have access to the Dirty Room.]]

[*Include as applicable—i.e., when using virtual security measures*: The Clean Team virtual development resources shall be located at [___].

[*Include as applicable:* Access to Clean Team virtual development resources shall be controlled by [Manager/Monitor/dedicated IT resource].]

[*Include as applicable:* The names of individuals who are granted access to Clean Team virtual development resources shall be kept on access control lists.]

[*Include as applicable:* Access to Clean Team virtual development resources shall be periodically monitored by [Manager/Monitor/dedicated IT resource].]

[*Include as applicable:* Access to Clean Team virtual development resources shall be periodically audited by [Manager/Monitor/dedicated IT resource].]

[*Include as applicable:* Clean Team members must not access (or have the ability to access) any electronic data sources containing Outside Protected Information.]

[*Include as applicable:* No Outside Protected Information should be placed into the Clean Team virtual development space(s) or electronic resources [AND/OR] no resources may be placed in the Clean Room development virtual space(s) or electronic resources without the approval of the Monitor.]

[*Include as applicable*: Resources used or consulted during the Clean Room development shall not be removed from the Clean Room development virtual space(s) or electronic resources.]

[*Include as applicable:* Separate Dirty Room development virtual space(s) or electronic resources which may contain documents, data, and other information used to develop [interface/competing technology/etc.] shall be located at [___].]]

Communications

[*Include as applicable*: Any communications between Clean Team and Specification Team must be in writing.]

[*Include as applicable*: and must be made first to the Monitor, who may modify such written communications before transmission to the intended recipient].]

Reporting

[*Include as applicable*: Prepare [periodic/daily/weekly/other] written reports on the development timeline and progress.

[Manager] shall be responsible for preparing such reports.

[*Include as applicable:* Such reports should be sent to the Monitor via email.]]

If you realize at any point that you or another member of the Clean Team have had exposure to Outside Protected Information or that any of the procedures in this document are not being followed, notify [insert contact person] immediately.

Contact [insert Manager(s) name and phone number] if you have any questions or concerns.

Signed Assurance/Affirmation

This acknowledgement is to be signed and returned to [insert contact name] upon receipt and review of the forgoing Clean Room Protocol for Development of [Insert Description] (the "Protocol").

By signing below, I hereby affirm and acknowledge that I understand the instructions set forth in the Protocol and agree to abide by them. I further affirm that I have not had exposure to any [Third-

Party] Outside Protected Information as of the date of my signature below. If I have any questions or if I realize at any point that I have had exposure to, or learned confidential information about, [Third-Party] Outside Protected Information, I will immediately notify [insert contact name and phone number].

> [*Include as applicable*: I understand that if I violate the Protocol or refuse to comply with reasonable instructions from the Monitor or Manager, I will be subject to disciplinary action, up to and including termination of my employment, and may face further legal action as appropriate.]

Employee Signature: _____

Employee Name: _____

Date: _____