

白皮书

21 CFR 第 11 部分合规立场 SoloVPE 系统

2012 年 4 月 10 日

1.0 摘要

FDA 于 1997 年 3 月发布的 21 CFR 第 11 部分法规的最终版本提供了一个框架，在该框架中，各组织能够签署、创建、存储和提供对电子记录的安全访问。21 CFR 第 11 部分提供了与复制、访问和权限、审计日志和跟踪、版本控制以及电子签名应用于电子文件有关的指南和规则。21 CFR 第 11 部分的合规性包括程序要求和软件要求。程序要求包括验证电子记录系统、起草和维护电子记录系统使用的标准操作规程，并确保电子记录系统的用户对其适当使用、管理及其在维护合规性方面的作用进行充分培训。

本文件旨在概述 SoloVPE 系统可提供的功能，以符合 FDA 关于电子记录和电子签名的裁定（21 CFR 第 11 部分）。本文件的编写理解是，第 11 部分合规性要求组织除软件包中已有的技术控制外，还需实施程序和行政控制。仅在软件中可用的能力和功能不能保证符合要求的实现，因此提供的软件不能被认证为符合要求。最终，关于任何应用程序（包括作为 C Technologies, Inc. 产品可变光程线的一部分提供的软件）合规性的最终决定取决于我们的客户，并取决于他们对第 11 部分要求的解释和理解。

2.0 引言

本指南旨在向考虑实施 21 CFR 第 11 部分合规性安装的客户提供实质性信息，说明 SoloVPE 系统提供的软件中与客户总体规划相关的工具、能力和功能。软件的设计考虑到法规的要求，并将许多技术要素纳入软件中，以提供完整性以实现合规性和灵活性，以适应每个客户和安装的独特程序和政策。完全符合 21 CFR 第 11 部分要求的最终责任在于客户及其设计、实施和验证工作。CTI 将尽可能与客户合作，了解系统能力和实施选项方面的任何差距，并酌情纳入可能的增强。

3.1 背景

系统的成功实现需要完全理解软件的功能。对软件的全面理解需要全面了解软件环境的基础设施。对于 SoloVPE 系统，软件平台由三个主要组件组成：

- (1) 计算机操作系统 Microsoft Windows®
- (2) 光谱环境: Agilent Technologies Cary WinUV
- (3) 可变光程应用程序: C Technologies, Inc. SoloVPE TM 软件

这三个核心组件协同工作，为 SoloVPE 硬件的命令和控制创建完整的接口。Cary WinUV 光谱软件套件是一个完整的光谱工作台，旨在控制 Agilent（原 Varian Inc.）的 Cary 分光光度计生产线。该平台提供了各种硬件系统及其各自附件的直接控制和配置，为方法开发以及图形和报告中数据的采集、分析和呈现创建了通用用户界面。它有一系列选项，允许以多种不同的文件格式保存和检索数据。SoloVPE 软件与 Cary WinUV 平台无缝集成，因为可变光程能力的功能覆盖层是使用 Agilent 的专有 ADL（高级开发语言）光谱学编写命令集设计和工程的。它仅且仅存在于 Cary WinUV 软件环境中，并利用了 Agilent Cary WinUV 平台的核心功能。




对于 SoloVPE 系统的安全实现，C Technologies, Inc. 建议实施可选安全模块：

- (A) GLP 管理员（Agilent Cary WinUV）
- (B) SecureVPE（C Technologies, Inc. SoloVPE）

使用这些可选模块结合网络域和/或工作站级别的安全选项，可创建三个安全级别。该分层为被分配执行合规系统任务的个人或小组提供了一系列工具，这些工具可用于定制总体安全结构，以支持每个组织的政策、程序和 workflows，以及该公司使用的任何伴随历史学家、存档或电子笔记本软件。

本文件的平衡部分包括关于这些组件和模块如何协同工作的更详细的信息，它们各自发挥的具体作用，以及如何使用它们实现合规性实现的一些示例和选项。

为了突出显示正在讨论的组件或层，整个文件中使用了以下符号：

图标	层	组分
	1	Windows（工作站/网络域）
	2	Agilent Cary WinUV-GLP 管理员
	3	SoloVPE-SecureVPE

4.0 详细信息

本文件的本章节提供了更详细的信息，说明 SoloVPE 系统中可用的工具如何作为总体合规计划的一部分应用于 21 CFR 第 11 部分法规的相关章节。

封闭系统的控制

§ 11.10 (a) 验证系统，以确保准确性、可靠性、一致的预期性能以及识别无效或更改记录的能力。



C Technologies, Inc. 由经过培训的服务人员以 SoloVPE 系统的安装确认/运行确认/性能确认 (IQOQPQ) 的形式提供验证服务。当系统通过 C Technologies 购买时，包括该服务，以确保硬件和软件正确安装在客户位置。在 IQOQPQ 之后，客户的合规实施团队可以开始制定所需政策和程序的过程，并根据合规计划使用系统可用的工具。C Technologies, Inc. 确实建议定期对系统进行再验证，并向 SoloVPE 所有者提供定期预防性维护服务。

系统中的审计追踪提供了关于系统访问、性能、使用和操作的信息，以帮助客户遵守法规。系统的所有三层均有审计追踪信息：

- 事件日志和网络日志可由客户配置以控制和监测访问。
- Agilent Cary WinUV 环境维护随每个数据文件一起保存的详细审计跟踪。
- GLP 管理员维护用户和组安全管理事件日志。
- SecureVPE 软件维护用户权限和组权限变更的审计跟踪。
- SoloVPE 软件维护系统相关事件日志。

§ 11.10 (b) 以人可读和电子形式生成准确和完整的记录副本的能力，适用于机构的检查、审查和复制。



Agilent Cary WinUV 环境是一个完整的光谱软件平台，旨在与 Cary 分光光度计的 Cary 线协同工作。它具有采集、分析、报告和保存光谱数据的能力。系统可以以电子方式以及更常见的文件 (CSV 和 RTF) 创建许多专有文件格式 (批次、数据、方法、报告和 Gram)。当 PDF 和 XPS 等便携式文档格式安装在计算机系统上时，也可以生成可广泛使用的程序。当物理打印机连接到系统时，硬拷贝输出也是一个选项。

创建、保存、修改和删除这些电子记录的能力可以通过客户对工作站、网络文件和文件夹权限的适当和支持性使用进行控制。客户负责建立适当的用户和组权限，并将其使用纳入工作流程和标准操作规程。



§ 11.10 (c) 保护记录，以便在整个记录保存期内准确、即时检索。



使用 SoloVPE 系统创建、保存、修改和删除电子记录的能力可通过客户对工作站、网络文件和文件夹权限的适当和支持性使用进行控制。客户负责建立适当的用户和组权限，并将其使用纳入工作流程和标准操作规程。Agilent Cary WinUV 软件包含创建输出的多种选项。其中一些选项，如 Agilent 的专有批文件可能包含数据、报告、方法、荟萃数据、审计追踪和电子签名信息。其他选项，如 PDF 或 XPS 文件，模拟电子纸张，并包含可使用附带打印机生成的电子版硬拷贝。客户必须决定哪些格式适合其合规性计划，然后使用 SoloVPE 系统及其自己的网络基础设施上提供的工具开发支持性文件和文件夹权限方法。此外，客户必须制定必要的政策和程

§ 11.10 (d) 限制系统访问授权人员。



对 SoloVPE 系统的访问控制可以在一定程度上设置在软件的所有三个级别。虽然这似乎是多余的，但每一层都提供了一些独特的选项和功能，客户在制定合规计划时应考虑这些选项和功能。虽然存在一些冗余，但每个层确实为合规实施团队提供了独特的安全工具。下表提供了每个层的基本概述，并探索了它们如何共同努力，以指导合规实施团队如何将它们纳入合规计划。

层	访问控制概述
	<ul style="list-style-type: none"> 对单个计算机的访问可以在工作站的本地级别进行控制，该工作站将为旧系统运行 Windows XP (Service Pack 3)，或在 2011 年 11 月 1 日之后销售的 Windows 7 (32 位) 系统。NTFS 权限可由客户自行决定设置用户权限和组权限，从而控制文件夹和文件上的 NTFS 权限。Microsoft 在建立安全配置文件方面提供了很大的灵活性。配置这些功能需要经过培训的 IT 专业人员的知识和经验，其在合规实施团队中的参与将是非常宝贵的。 当客户选择将 SoloVPE 系统计算机连接到网络域时，可以获得更多的复杂性和保护系统的选项。需要熟悉合规计划的网络管理员，以确保客户制定的政策和程序得到适当实施。 操作系统和网络中可用的安全控制为客户控制对 SoloVPE 系统的访问提供了巨大的灵活性，如登录监测、密码组策略（如复杂性和过期）、登录尝试跟踪和锁定。 此外，网络框架通常是可以控制和监测与其他软件包和系统结合的环境。
	<ul style="list-style-type: none"> GLP 管理员是 Agilent Cary WinUV 软件套件的主要安全组件。GLP 管理员允许用户创建具有各自特定权限配置文件的唯一用户和组。 GLP 管理员程序中设置的权限侧重于访问 Cary WinUV 软件套件中可用的程序以及在 Cary WinUV 软件中执行某些类型活动的权限。 对 GLP 管理员本身的访问受密码保护，必须指定管理员负责创建和修改应用程序中的设置。 GLP 管理员允许指定的管理员添加、修改和删除用户和组。 GLP 管理员允许管理员为计算机切换 Agilent Cary WinUV 开启和关闭（非用户或组特定）。此选项允许在完全安全或不安全模式下运行系统。 启用 GLP 检查时，对所有 Cary WinUV 软件应用程序（包括 SoloVPE 软件）的访问受用户名和密码控制，并强制执行该用户的安全配置文件。禁用 GLP 检查时，禁用访问控制，软件不知道使用系统的操作。 可控制的具体权限为： <ul style="list-style-type: none"> 授权用户/组权限运行特定应用程序。 授权用户/组修改其拥有的方法 授权用户/组修改所有方法 授权用户/组修改其拥有的报告 授权用户/组修改所有报告

- SecureVPE 应用程序是与 SoloVPE 系统软件相关的选项伴随产品。如前所述，SoloVPE 功能存在于 Cary WinUV 环境中。SecureVPE 应用程序与 Cary WinUV 套件中的 GLP 管理员应用程序合作，以提供与 SoloVPE 功能专门相关的扩展安全工具。
- SecureVPE 软件内置访问控制，并与 GLP 管理软件协同工作。GLP 管理员中的管理员也是 SecureVPE 应用程序中的管理员。具有管理权限的用户和组可以根据客户的判断访问 SecureVPE 软件，以允许客户的合规计划具有灵活性。
- SoloVPE 系统的访问可以在操作系统级别进行控制，也可以使用 Cary WinUV 级别的 GLP 管理员进行控制。SecureVPE 应用程序提供了控制对 SoloVPE 软件访问的第三种选项。
- SecureVPE 应用程序位于 GLP 管理员应用程序之上。系统将 GLP 管理员中创建的用户和组与 SecureVPE 数据库同步。此同步仅从 GLP 管理员单向到 SecureVPE 环境。SecureVPE 不允许添加或删除用户和组。
- SecureVPE 应用程序提供了特定的安全矩阵，该矩阵专门涉及在 Cary WinUV 环境中运行的 SoloVPE 软件。权限选项旨在为客户和管理员提供对 SoloVPE 环境中特定功能和功能访问的控制。在某些情况下，权限设置可以在启用和禁用之间切换按钮状态，或切换可见和不可见的按钮状态。在其他情况下，权限设置可以提供或撤销执行特定任务的选项，例如执行电子签名或是否启用自动保存功能。
- 对 SecureVPE 应用程序中可用权限设置的完整探索超出了本文件的范围。然而，重要的是要理解，在安全结构的这一层提供的控制仅与 SoloVPE 软件相关，并且需要与其他层一起配置，以实现合规实施团队的目标。

§ 11.10 (e) 使用安全、计算机生成、加盖时间戳的审计追踪，独立记录操作员条目的日期和时间以及创建、修改或删除电子记录的操作。记录变更不得遮盖先前记录的信息。此类稽查追踪文件应至少保存至受试者电子记录所需的时间，并可供机构审查和复印。



广泛的审计追踪记录在 SoloVPE 软件环境的各个级别内。客户对计算机工作站和网络域的配置都有广泛的选项，包括跟踪用户的操作和 Windows 操作系统中存在的各种事件日志。客户使用这些功能的程度必须由合规实施团队决定，并由其内部网络专家实施，这些决策需要包括其维护、备份和存档数据的计划。

GLP 管理员软件维护该环境中所有配置更改的审计日志，包括对用户和组的更改以及特定和全局安全设置和权限的更改。可以从 GLP 管理员应用程序中查看审计日志，不能直接编辑或删除。C Technologies, Inc. 建议客户制定政策和程序，处理审计信息的保留、备份和存档。

SecureVPE 软件维护对应用于 SoloVPE 软件环境的程序中的安全设置进行的审计日志配置更改。由于用户和组功能构建在 GLP 管理员控件之上，因此审计追踪活动的重点是用户和组权限的更改。审计追踪报告可从 SecureVPE 环境中查看，并驻留在数据库中，防止编辑和删除。C Technologies, Inc. 建议客户制定政策和程序，处理审计信息的保留、备份和存档。

§ 11.10 (f) 使用操作系统检查酌情强制执行允许的步骤和事件排序。



C Technologies, Inc. 建议客户合规实施团队制定政策和程序，利用 SoloVPE 系统软件中的能力和功能，通过使用操作系统检查强制执行步骤和事件的允许顺序。SoloVPE 软件的安全性特征，特别是 GLP 管理员和 SecureVPE 软件包允许客户设置具有特定权限的用户和组，允许创建方法、修改方法或简单运行方法。当权限配置正确时，用户将受到方法参数及其特定权限的约束。正确配置权限结合自动电子签名功能，使客户能够确保电子记录的完整性和真实性。

§ 11.10 (g) 使用权限检查，以确保只有经授权的个人才能使用系统、以电子方式签署记录、访问操作或计算机系统输入或输出设备、更改记录或执行手头操作。



SoloVPE 系统可配置为需要权限检查以访问系统、控制系统、进行配置或记录更改、以电子方式签署记录并授权各种类型的操作。客户合规实施团队负责围绕系统能力设计政策和程序，以满足其组织的合规目标。由于安全特性有多层，因此在设计安全计划时，必须考虑每层内可用的特定特征，因为每个层都可以配置为保护特定类型的访问、控制和数据。

在任何安全计划的组成部分中，当系统连接到计算机网络时，必须启动计算机工作站和网络域。Windows 操作系统和网络体系结构中可以使用大量的电力和灵活性。然而，权力和灵活性是有成本的，而成本是配置支持合规实施团队总体目标的安全配置所涉及的复杂性。在这里，客户必须让他们的 IT 工作人员参与，以成功地设计和实现他们的计算机/网络安全结构。控制工作站和任何可访问的文件服务器上 NTFS 文件系统内的读写和修改权限等问题对于确保记录能够正确创建、保护和存档至关重要。C Technologies, Inc. 提供了关于其软件包安全性要求的具体信息；然而，由于行业中存在复杂性和变异性，无法提供关于总体网络安全的指导。然而，在最基本的级别上，Windows 允许客户配置受密码保护的唯一用户 ID（帐户），可控制对计算机/网络的访问和该用户权限的总体配置文件。当以这种方式实现时，Windows 登录将创建第一道防线，用于在登录时保护计算机系统，如果登录用户离开计算机一段时间。它还可以用于控制文件数据的创建和保存位置和方式，以及是否可以修改、删除或覆盖。

GLP 管理员是第二个使用权限检查来保护 SoloVPE 系统的安全阈值。如前所述，GLP 管理员创建了专门与 Cary WinUV 软件套件相关的安全结构。GLP 管理员允许创建唯一的用户 ID 和密码组合，用于确保对 Cary WinUV 软件应用程序（包括 SoloVPE 软件）的访问和权限。配置的用户特定权限配置文件限制哪些用户可以访问系统，以及他们在 Cary WinUV 应用程序中工作时可以执行哪些任务，包括哪些应用程序可以访问，以及用户是否具有修改方法或报告的能力。启用 GLP 管理员登录提示时，需要输入有效的用户 ID 和密码组合，才能成功访问 Cary WinUV 应用程序。一旦登录，用户的特定配置文件将控制他们可以在软件和系统中进行哪些操作。

最终和最集中的安全级别由 SecureVPE 软件控制。SecureVPE 软件使

§ 11.10 (h) 使用设备（例如终端）检查，以酌情确定数据输入来源或操作说明的有效性。



GLP 管理员和 SecureVPE 软件安全层可以配置为通过身份验证提示提示，提示登录用户记录电子签名，要求登录用户在关键操作前后提供密码，以确保输入输出的有效性。

§ 11.10 (i) 确定开发、维护或使用电子记录/电子签名系统的人员具有执行其指定任务的教育、培训和经验。

C Technologies, Inc. 在生物制药行业中支持光纤光谱设备已有十多年的历史。作为 SoloVPE 系统实施的一部分，组织可以联系 C Technologies, Inc.，要求和审查其开发政策、流程和程序以及员工培训和经验的各个方面。

§ 11.10 (j) 制定和遵守书面政策，追究个人的责任，并对根据其电子签名发起的行动负责，以防止记录和签名造假。



C Technologies, Inc. 建议客户合规实施团队制定政策和程序，描述和管理员和最终用户必须使用 SoloVPE 系统执行的操作。对于管理员，应针对用户和组管理、密码管理、审计追踪配置和清除等系统相关操作制定政策和程序。对于最终用户，应为文件和文件夹创建、数据命名约定和电子签名应用程序、审查和批准等操作制定政策和程序。

§ 11.10 (k) 对系统文件使用适当的控制，包括：（1）对系统运行和维护文件的分发、访问和使用进行充分控制。
（2）修订和变更控制程序，以保持记录系统文件按时间顺序开发和修改的审计追踪。



C Technologies, Inc. 随 SoloVPE 系统提供的文件（包括 Agilent Cary WinUV 软件以及 SoloVPE 和 SecureVPE 软件）随软件的每个版本进行更新和分发。每组文档在适用于其特定版本时均可唯一标识。

开放系统的控制

§ 11.30 使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建之日起至接收时电子记录的真实性、完整性和机密性的程序和控制措施。



鉴于 SoloVPE 系统满足这一要求的能力和限制，C Technologies, Inc. 建议客户的合规实施团队实施适当的政策和程序。SoloVPE 系统和安全功能提供了特定功能，旨在支持与用户身份验证、数据完整性和机密性相关的合规性，具体如下：

身份验证：系统访问可以通过 Windows 操作系统/网络域访问控制以及 GLP 管理员的配置和实现进行控制。

完整性：客户可以通过分层和互补的方式配置各种安全级别，以限制特定用户 ID 生成、修改和存储数据，并在系统使用期间使用电子签名能力执行关键操作步骤。

机密性：为确保机密性，C Technologies, Inc. 建议客户建立适当的工作站和网络安全配置文件，包括本地和组策略，可根据经认证的用户 ID 控制哪些信息可见和可访问。适当的书面政策和程序也需要作为组织实施计划的一部分。

数字签名：SecureVPE 软件系统允许实现电子签名，即系统使用过程中关键点发生的用户 ID 和密码认证提示事件。除自动提示外，系统还可配置为在用户登录时提示（用于登录和创建）并提示用户创建

§ 11.50 (a) 已签字的电子记录应包含与签名相关的信息，明确指出以下内容：

- (1) 签字人的印刷体姓名；
- (2) 签名执行的日期和时间；和
- (3) 与签名相关的含义（如审核、批准、责任或作者）。



用户通过 SoloVPE 软件应用程序接口执行电子签名，用户需要输入用户名和密码。电子签名与批文件中的数据以及文件唯一标识符的名称、签名人的全名、签名执行日期和时间以及签名的含义一起存储。用户还可以选择在执行电子签名时在电子签名中添加注释。在软件环境中的现有报告中，将添加一个人可读文本块，指示文件已进行数字签名。

§ 11.50 (b) (a) 中确定的项目应受与电子记录相同的控制，并应作为任何人类可读电子记录形式（如电子显示器或打印输出）的一部分纳入。

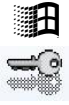


SoloVPE 软件附带每个电子签名详细信息的人类可读文本块。该信息保存在批文件中，并作为可审计活动的一部分。由于它与数据共存，所以其安全控制结构是相同的。

§ 11.70 对电子记录执行的电子签名和手写签名应与其各自的电子记录链接，以确保签名不能被删除、复制或以其他方式转移以普通方式伪造电子记录。

C Technologies, Inc. 建议，鉴于 SoloVPE 系统的能力和限制，客户的合规实施团队制定必要的政策和程序，以实现法规的这一要求的合规性。

§ 11.100 (a) 每个电子签名应为一个人独有，不得被任何人重复使用或重新分配给其他人。



C Technologies, Inc. 建议合规实施团队实施政策和程序，以确保用户名仅分配给一个人，并且每个人同意在任何情况下都不泄露其密码。鉴于 Windows/网络域用户名和 GLP 管理员用户名的能力和限制，这些策略和程序必须同时应用于这些系统。注：由于 SecureVPE 使用 GLP 管理员应用程序中创建的用户和组，因此无法在 SecureVPE 软件中管理（创建、修改或删除）用户名。

§ 11.100 (b) 在组织建立、转让或认证个人电子签名之前，组织应核实个人的身份。



C Technologies, Inc. 建议客户的合规实施团队纳入政策和程序，以确保根据个人在组织结构中的角色和职责以及在组织结构中的职位，将用户名分配给具有适当授权和批准的个人。

§ 11.100 (c) 使用电子签名的人员应向 FDA 证明，他们使用的电子签名与传统手写签名具有法律约束力相当，可能需要提供额外的证明，证明给定电子签名相当于签名人的手写签名。



C Technologies, Inc. 建议，鉴于 SoloVPE 系统软件组件的能力和限制，客户合规实施团队应执行政策和程序，以能够遵守本法规的认证要求。与用户标识相关的系统软件组件和输出选项可证明电子签名确实创建了与传统手写签名具有法律约束力的等效项，作为客户实施计划和执行的一部分。

§ 11.200 (a) 非基于生物统计学的电子签名应：

(1) 使用至少两个不同的标识组件，如识别码和密码。

(i) 当个人在单个、连续的受控系统访问期间执行一系列签名时，应使用所有电子签名组件执行首次签名；后续签名应使用至少一个电子签名组件执行，该电子签名组件仅可由个人执行，且设计为仅供个人使用。

(ii) 当个人在受控系统访问的单个连续周期内执行一个或多个未执行的签名时，每次签名均应使用所有电子签名组件执行。

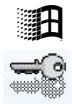
(2) 仅供其真正的所有者使用；和

(3) 管理和执行，以确保除真正所有者外的任何人尝试使用个人的电子签名需要两个或更多个人的合作。

§ 11.200 (b) 基于生物特征电子签名的设计应确保其真实所有者以外的任何人不得使用。

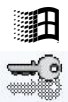
SoloVPE 系统不使用生物鉴别技术。相反，系统用户输入其用户名和密码组合以授权签名。

§ 11.300 识别码/密码的控制。使用基于识别码和密码的电子签名的人员应采用控制措施，以确保其安全性和完整性。此类控制应包括：11.300 (a) 保持每个组合识别码和密码的唯一性，使得没有两个人具有相同的识别码和密码组合。



C Technologies, Inc. 建议客户合规执行团队制定政策和程序，以确保识别码和密码组合的唯一性。Windows 操作系统和网络域管理功能提供了广泛类型的密码策略，包括复杂性、老化、更改需求、锁定、重用预防和过期。客户应让其 IT 部门参与，以确定支持其总体实施计划的策略。这些策略也应应用于 GLP 管理员进行的用户 ID 维护。

§ 11.300 (b) 确保定期检查、召回或修订识别码和密码发布（例如，以涵盖密码老化等事件）。



C Technologies, Inc. 建议客户合规执行团队制定政策和程序，以确保定期审查和管理识别码和密码。Windows 操作系统和网络域管理功能提供了广泛类型的密码策略，包括复杂性、老化、更改需求、锁定、重复使用预防和过期。在创建和监测与用户 ID 和密码相关的策略方面，GLP 管理员的复杂程度与 Windows 系统不同，因此必须通过适当实施管理策略和程序进行定期审查。

5.0 结论

C Technologies, Inc., 斜率光谱™的创始人和 SoloVPE 可变光程光谱系统的发明人，致力于与其客户合作，以成功实施和部署其技术。UV-Vis 测量的实用性和广泛适用性反映在我们的客户和安装地点的多样性中，从全球范围广泛的行业的学术机构、政府机构和公司不等。我们的许多客户在生物制药行业，受到来自不同国家机构和药典的各种监管限制。C Technologies, Inc. 致力于与客户合作，确保其系统的能力和函数使客户能够设计和实施合规安装。由于客户监管环境的变异性和复杂性，C Technologies, Inc. 未提供经认证的转钥匙安装服务。相反，C Technologies, Inc. 通过与 Agilent Technologies 及其技术人员的密切关系提供支持服务，以协助每个客户的合规实施团队充分理解 SoloVPE 系统及其软件的工具和能力要求，以帮助成功地制定符合其组织和合规目标的合规计划。最终，合规性仍然是每个安装站点的每个客户的责任。

6.1 参考文献

- (1) 行业指南：第 11 部分，电子记录；电子签名-范围和应用（药物评价和研究中心合规办公室[CDER]，FDA 2003 年 8 月）
- (2) 联邦公报/第 62 卷，第 54 号/1997 年 3 月 20 日，星期四/法规和法规 21 CFR 第 11 部分[文件编号 92N-0251]http://www.fda.gov/ora/compliance_ref/part11/FRS/back_ground/11cfr-fr.htm

如需更多信息，请联系：

C Technologies, Inc.

直拨：+ (US) 908 707 1009

Solo Service Direct: + (US) 908 707 1201

info@solovpe.com

溶液 com

C Technologies, Inc. 2012 版权所有

本材料的版权归 C Technologies, Inc. 所有。未经 C Technologies, Inc. 的明确书面许可，不得全部或部分复制本材料。本文件中的信息可随时更改，不另行通知。保留所有权利。所有其他产品或公司名称仅用于识别目的，并且是其各自所有者的商标。

*斜率光谱®和 SoloVPE™被声明为 C Technologies, Inc. 的商标。

Windows®是 Microsoft Corporation Agilent Technologies®的注册商标，是 Agilent Corporation 的注册商标

有关 SoloVPE 和相关产品的更多信息，请访问网站：www.solovpe.com