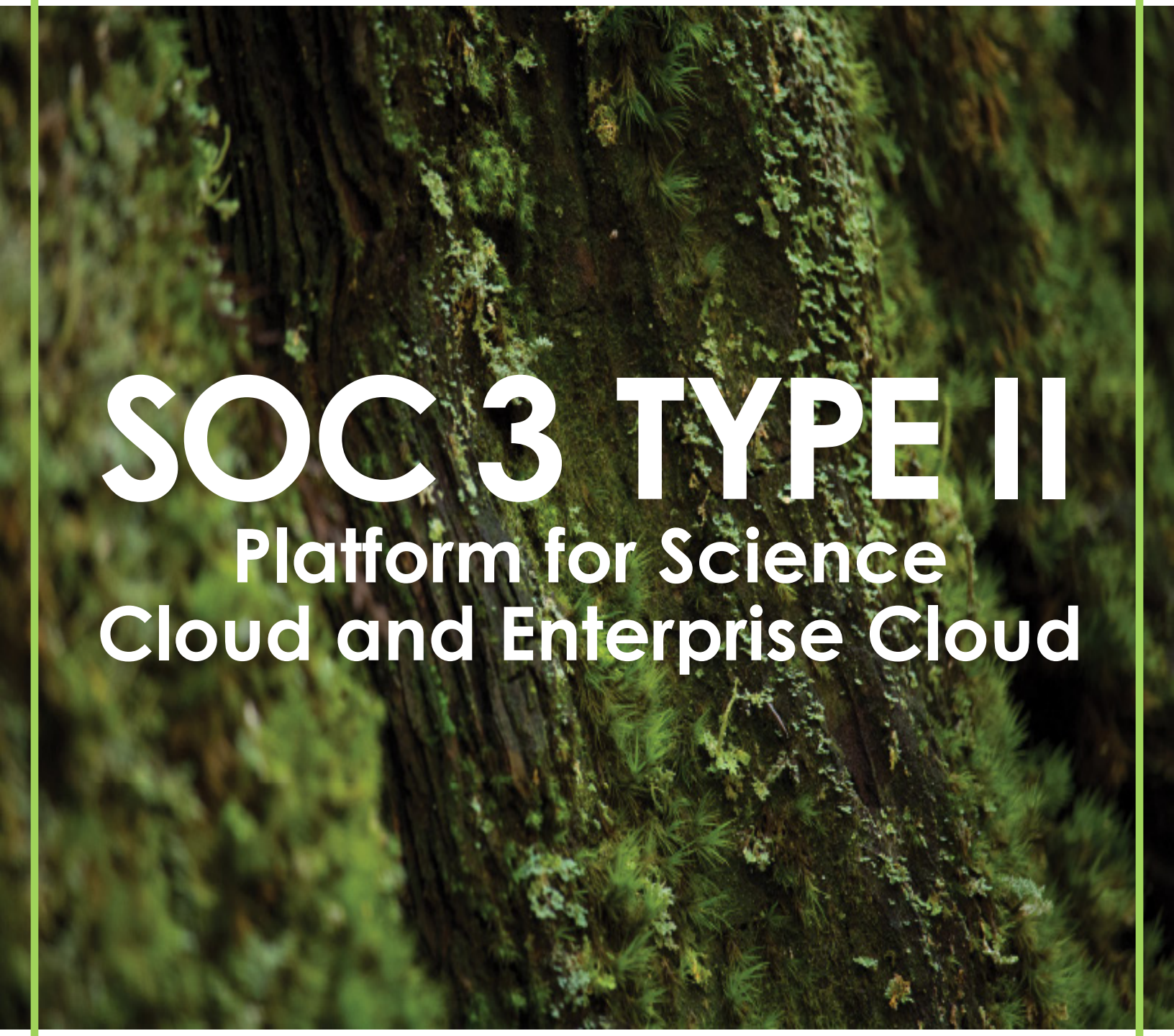
ThermoFisher SCIENTIFIC
The world leader in serving science

PLATFORM FOR SCIENCE™



SOC 3 TYPE II

Platform for Science Cloud and Enterprise Cloud

Report on Controls Relevant to Security

For the Period August 1, 2021 to July 31, 2022

KERRY L. SHACKELFORD CPA LLC

Thermo Fisher Scientific, Inc.

Report on the Platform for Science Relevant to Security

Table of Contents

KERRY L. SHACKELFORD CPA LLC
A CPA Firm Specializing in SOC, HIPAA & IT Audits

The Stone House
1524 Belford Court
Evergreen, Colorado 80439

Section I — Independent Service Auditor's Report

To the Board of Directors and Management of Thermo Fisher Scientific, Inc.:

Scope

We have examined Thermo Fisher Scientific, Inc.'s ("Thermo Fisher Scientific" accompanying assertion in Section II of this report titled "*Thermo Fisher Scientific's Assertion*" that the controls within Thermo Fisher Scientific's Platform for Science Cloud and Enterprise Cloud[1] ("the Platform for Science" or "the system") were effective throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("the applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Thermo Fisher Scientific's Responsibilities

Thermo Fisher Scientific's management is responsible for its assertion, selecting the applicable trust services criteria on which its assertion is based, and having a reasonable basis for its assertion. The Company is also responsible for:

- Describing the boundaries of the Platform for Science.
- Identifying its service commitments and system requirements.
- Identifying the risks that would threaten the achievement of its service commitments and system requirements.
- Designing, implementing, and operating effective controls within the system to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved.

Thermo Fisher Scientific has provided its assertion in Section II of this report titled "*Thermo Fisher Scientific's Assertion*" about the effectiveness of the controls within the system.

Independent Service Auditor's Responsibilities

Our responsibility is to express an opinion on management's assertion, based on our examination. Our examination was conducted in accordance with attestation standards

[1] The scope of the independent service auditor's report was limited to certain deployment models of the Platform for Science as described in the *Scope of Examination and Description* paragraph in *Section III — Thermo Fisher Scientific's Description of the Boundaries of the Platform for Science*.

established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the Company's service commitments and system requirements.
- Assessing the risks that the controls were not effective to achieve Thermo Fisher Scientific's service commitments and system requirements.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Thermo Fisher Scientific's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

(The remainder of this page left blank on purpose.)

Opinion

In our opinion, management's assertion that the controls within Thermo Fisher Scientific's Platform for Science were effective throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Kerry L. Shackelford CPA LLC
September 28, 2022
Evergreen, Colorado

Thermo Fisher Scientific
246 Goose Lane, Suite 100
Guilford, CT 06437
+1 866-823-0337
www.thermofisher.com

Section II — Thermo Fisher Scientific's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Thermo Fisher Scientific, Inc.'s ("Thermo Fisher Scientific") Platform for Science Cloud and Enterprise Cloud (the "Platform for Science" or "the system") throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section III of this report titled *"Thermo Fisher Scientific's Description of the Boundaries of the Platform for Science"* and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("the applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Thermo Fisher Scientific's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The service commitments and system requirements related to the applicable trust services criteria are presented in Section IV of this report titled *"Thermo Fisher Scientific's Service Commitments and System Requirements."*

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:
Liz Tonks
156F78F712C342B...

Liz Tonks
Senior Director of Quality Assurance & Regulatory
Digital Science
Thermo Fisher Scientific, Inc.

Section III — Thermo Fisher Scientific's Description of the Boundaries of the Platform for Science

Overview of the Organization

Thermo Fisher Scientific, Inc.

Thermo Fisher Scientific, Inc. ("Thermo Fisher Scientific" or the "Company") is the world leader in serving science, with annual revenue of approximately $40 billion. Thermo Fisher Scientific's Mission is to enable its customers to make the world healthier, cleaner, and safer. They help their customers accelerate life sciences research, solve complex analytical challenges, increase productivity in their laboratories, and improve patient health through diagnostics or the development and manufacture of life-changing therapies. Thermo Fisher Scientific delivers an unrivaled combination of innovative technologies, purchasing convenience, and comprehensive services through their industry-leading brands, including Thermo Scientific, Applied Biosystems, Invitrogen, Fisher Scientific, Unity Lab Services, Patheon, and PPD.

Digital Science and Digital Engineering

The former Core Informatics, now part of Thermo Fisher Scientific's Digital Science business unit ("Digital Science"), was founded in 2005 by a group of former lab scientists with intimate knowledge of the small molecule drug discovery process. Digital Science partners with customers in biopharma, genomics, and other industries to deliver lab informatics solutions to derive more value and insight from their scientific data. Prior to being acquired by Thermo Fisher Scientific in March 2017, Core Informatics had been recognized numerous times as one of the fastest growing private companies in the United States and as one of Connecticut's best places to work.

Beginning in 2020, the Technical Operations team was moved within the organization from Digital Science to the Digital Engineering business unit ("Digital Engineering"). Digital Engineering works in collaboration with Digital Science to develop, maintain, and support Thermo Fisher Scientific's customer-facing software products, including the Platform for Science ("PFS").

Overview of Subservice Organizations

Subservice organizations are third-party service providers (a.k.a., vendors) whose services are relevant to report users' understanding of the PFS and whose controls are necessary, in combination with Thermo Fisher Scientific's controls, to provide reasonable assurance that the Company's service commitments and system requirements are achieved based on the applicable trust services criteria. Thermo Fisher Scientific uses subservice organizations to achieve operating efficiency and obtain specific expertise. The following is the principal subservice organization used by the Company in support of the PFS:

Amazon Web Services ("AWS")—
The PFS instances within the scope of this report are hosted in Amazon Web Services ("AWS") data center facilities. AWS is responsible for providing cloud computing services, including cloud-based virtual IT infrastructure management tools and system components.

AWS' controls are necessary, in combination with controls at Thermo Fisher Scientific, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. AWS' control activities have been carved out from Section III of this report titled *"Thermo Fisher Scientific's Description of the Boundaries of the Platform for Science,"* and the examination. AWS' control activities are described in their SOC 2 Type II report.

Thermo Fisher Scientific uses other third-party service providers (e.g., contractors); however, they are not included in this report as Thermo Fisher Scientific has implemented its own controls independent of those of others that meet the applicable trust services criteria.

Complementary Subservice Organization Controls

Thermo Fisher Scientific expects that AWS will perform certain controls considered necessary, in combination with Thermo Fisher Scientific's controls, to provide reasonable assurance that one or more of Thermo Fisher Scientific's service commitments and system requirements were achieved. Such controls are referred to as *complementary subservice organization controls* and include:

Area	Control Activities Expected to be Implemented
Network Device Security	AWS is responsible for ensuring that the virtual IT infrastructure management tools and system components used by Thermo Fisher Scientific are logically secure and operate as described and configured.
Physical Access	AWS is responsible for ensuring that physical access controls at data center facilities used to support Thermo Fisher Scientific are effective in restricting physical access to authorized and appropriate personnel.
Media Protection and Encryption	AWS is responsible for ensuring that customer data in the Amazon Relational Database Service ("RDS") is encrypted with strong encryption and that encryption keys are protected.
Logging and Monitoring	AWS is responsible for ensuring that logged activity from the virtual IT infrastructure management tools and system components is preserved.

Overview of the Platform for Science

Services Provided

The PFS is part of a Platform-as-a-Service solution enabling lab informatics. The PFS software is the underlying data management infrastructure designed to support scientific organization workflows. It provides the scientific community with a flexible, cost effective, and secure way to collect, store, access, share, and use scientific data. Thermo Fisher Scientific's services related to the PFS include:

Business Analysis and Implementation—
Thermo Fisher Scientific implements the PFS for customers and guides them through major project tasks and milestones including setting project objectives, gathering and defining requirements, configuring the system, acceptance testing the functionality of the configured PFS, and deployment.

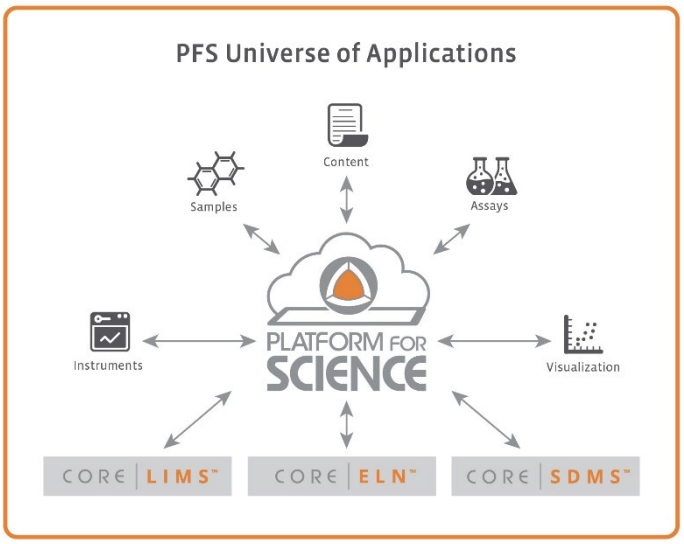
Training—
Thermo Fisher Scientific provides customers with access to the Education Center, an eLearning portal which gives customers on-demand access to interactive training material, narrated slides, demonstration videos, and quizzes. For advanced topics, the Company offers remote, instructor-led training sessions.

Support—
Thermo Fisher Scientific provides implementation support and makes the Support team available to new customers for the first three months. Post-implementation, the Company provides customers with access to the Help Center, which enables them to communicate questions, issues, and feature requests.

Maintenance—
Thermo Fisher Scientific corrects errors in the PFS software, periodically releases new features, and maintains all customer AWS IT environments (including the setup of test and production instances of the PFS and the initial migration of the customer's configurations from test to production).

Platform for Science

Thermo Fisher Scientific provides the scalable and extensible PFS that enables customers to quickly and easily build workflows to meet their specific needs and add capabilities as they grow. This flexible, extensible, cloud-based platform helps customers easily collect, store, access, share, and use scientific data. Changes to these solutions are made through configurations, not custom code, and are immediately available throughout the platform and standards-based OData API. Thermo Fisher Scientific provides solutions that work together on top of the PFS to support data capture across customer scientific workflows. The PFS database serves as the repository for all structured and unstructured customer data.



The key solutions in the PFS universe of applications include:

CORE | LIMS—Provides lab data management capabilities for samples, assays, inventory, workflows, requests, and more.

CORE | ELN—Provides electronic lab notebook capabilities for experiment definition, tracking, approval, and more.

CORE | SDMS—Provides an automated data capture framework to read and parse instrument data files into Thermo Fisher Scientific's products.

Thermo Fisher Scientific supports several deployment models of the PFS:

PFS Cloud—The PFS Cloud instances are hosted on auto-scalable, cloud-based IT infrastructures in a multi-tenant SaaS model.

PFS Enterprise Cloud—The PFS Enterprise Cloud instances are hosted on auto-scalable, cloud-based IT infrastructures dedicated to individual customers.

PFS HIPAA Cloud—The PFS HIPAA Cloud is an enhancement of the PFS Enterprise Cloud deployment model for customers who must comply with the requirements of HIPAA.

PFS Validated Cloud—The PFS Validated Cloud is an enhancement of the PFS Enterprise Cloud deployment model for FDA regulated customers.

PFS On-Premises—The PFS is hosted on customer-owned and managed IT infrastructure.

Scope of Examination and Description

The scope of the independent service auditor's SOC 3 Type II examination was limited to customers using production instances of the PFS Cloud and PFS Enterprise Cloud deployment models. The SOC 3 Type II examination is not applicable to other deployment models such as PFS instances under a customer's management or PFS instances running on a customer's IT infrastructure.

Although the PFS Enterprise Cloud deployment model includes the PFS HIPAA Cloud and the PFS Validated Cloud deployment models, the scope of the SOC 3 Type II examination and description was limited to the requirements of the applicable trust services criteria and does not address the requirements of the HIPAA or FDA regulations that are additional to the applicable trust services criteria.

The remainder of the description of the PFS is limited to the PFS Cloud and PFS Enterprise Cloud deployment models in scope.

Infrastructure

The instances of the PFS within the scope of this report are hosted in AWS data center facilities.

The Thermo Fisher Scientific network relevant to the PFS consists of the corporate network and the AWS virtual IT infrastructure system components in scope (AWS Accounts and Virtual Private Clouds ("VPCs") for PFS Cloud and PFS Enterprise Cloud customers). The corporate virtual private network ("VPN") defines network users and restricts their access to IT resources, including the AWS-based virtual IT infrastructure system components.

For both PFS Cloud and PFS Enterprise Cloud deployment models, the AWS-based virtual IT infrastructure system components consist of an AWS VPC designed with a de-militarized zone ("DMZ") to limit the footprint of the IT environment visible from the Internet. The DMZ may include multiple load balancers and multiple application servers. AWS VPC Security Group(s), Network Access Control List(s), and Route Table(s) are used to restrict Internet traffic between the DMZ and the internal network. The PFS database server is located on the AWS internal network.

Software

Server Operating Systems: Servers in the IT environment run a Linux Amazon Machine Image ("AMI"), except for the PFS's ELN servers which run the Microsoft Windows Server operating system.

Workstation Operating Systems: User workstations run the Microsoft Windows and Apple macOS operating systems.

Other Supporting Software: Other software of significance used to support the PFS includes:

Antivirus Software—
Antivirus software is deployed to workstations and servers to protect the IT environment against malicious software. Symantec Endpoint Protection, Trend Micro Apex One, or CrowdStrike Falcon are used for workstations, and Trend Micro Deep Security is used for servers.

AWS Certificate Manager—
Used to store and protect the digital certificates used to encrypt the PFS's transmissions whether via the user interface ("UI") or APIs.

AWS Elastic Cloud Compute ("Amazon EC2")—
Used to deploy and configure the PFS's web servers.

AWS Identity and Access Management ("IAM") System—
AWS IAM is used to securely control user access to AWS services and resources.

AWS Key Management Service—
Used to store and protect the encryption keys used to encrypt customer data.

AWS Relational Database Service ("RDS")—
AWS RDS is a fully managed Oracle database service used to store the PFS's customer data.

Cloud-based Software Version Control System—
GitHub is used to maintain the PFS application source code. Atlassian BitBucket was used from the beginning of the audit period to October 2021, prior to converting to GitHub.

File Transfer Protocol ("FTP") Server—
Used by a small number of customers to securely transfer bulk data.

Intrusion Detection and Prevention System ("IDPS")—
Trend Micro Deep Security's Intrusion Prevention module detects and prevents IT environment intrusions or otherwise alerts appropriate personnel to potential malicious activity for follow-up.

Log Management Systems—
Splunk collects and reviews logged activity from the AWS-based virtual IT infrastructure system components and the PFS application.

Microsoft Active Directory—
Used as a directory service to authenticate corporate network users and manage group lists for access control purposes.

Secure Shell ("SSH")—
Used to connect directly to virtual hosts from the internal network for administration purposes.

Single Sign-On ("SSO") Systems—
Idaptive and Okta SSO systems are used by Thermo Fisher Scientific personnel to access the AWS-based virtual IT infrastructure system components and customer instances of the PFS, respectively. The SSO systems in use enforce multi-factor authentication.

Specops—
Specops is an add-on to Microsoft Active Directory which further restrict the allowable composition of passwords and support length-based password aging.

Ticketing Systems—
Atlassian Jira is used to document and manage application and IT infrastructure changes and customer support requests, among other uses. ServiceNow is used to document and manage security incidents.

Virtual Private Network ("VPN") System—
Pulse Secure is used by Thermo Fisher Scientific personnel to securely access the internal network and IT resources from outside Company offices and sites.

Vulnerability Scanners—
NetSparker detects security vulnerabilities in the AWS-based virtual IT infrastructure system components and in the PFS's application code base.

Application Software: The PFS is a web-based application with a browser-based user interface. Thermo Fisher Scientific has established secure coding practices based on best practices prescribed by the Open Web Application Security Project and software engineers are trained in secure coding practices.

People

The key teams involved in supporting the PFS include:

Engineering Team—
The Engineering team is responsible for all PFS software development, testing, and maintenance.

Human Resources Team—
The Human Resources team is responsible for human resources-related processes, including personnel screening, orientation, training, and termination.

Information Technology ("IT") Team—
The IT team at corporate and within Digital Science manages the IT environment and resources used to support the PFS including the network and user workstations.

Product Team—
The Product team is responsible for the definition of the PFS's functionality.

Quality Operations Team—
The Quality Operations team is responsible for maintaining the quality management system ("QMS"), including standard operating procedures, the training program, and regulatory compliance for the entire organization. A member of the Quality Operations team serves as the PFS Security Officer and the SOC 2 compliance coordinator.

Security Team—
The PFS Security Officer is supported by the Corporate Information Security team and a PFS Security team which includes leaders from Quality Operations, Technical Operations, Customer Support, Human Resources, and Site Management. The Security team is responsible for the security of the PFS.

Technical Operations Team—
The Technical Operations team within Digital Engineering manages the IT environment, including the AWS-based virtual IT infrastructure system components comprising each instance of the PFS.

Procedures

The automated and manual procedures relevant to the PFS and the transaction streams, files, databases, and output used or processed by the PFS include security-related control activities in the following areas, among others:

- Security Management
- Personnel Screening, Security Awareness, and Training
- Network Device Security
- Logical Access
- Protection from Malicious Software
- Physical Access
- Media Protection and Encryption
- Logging and Monitoring
- Incident Response Plan and Breach Notification
- Change Management

Data

Customer data is maintained in the AWS-based virtual IT infrastructure system components and resides in production database servers deployed using Amazon's RDS. The PFS database servers are not visible from the Internet. Customer data is not stored outside of AWS. Backup copies of customer data are maintained using AWS RDS backup snapshots.

Changes to the Platform for Science During the Period

The significant changes made to the PFS throughout the period August 1, 2021, to July 31, 2022, included the following:

Branford Site Closure—
Effective November 15, 2021, all Branford-based personnel were reassigned to "remote" status, and by December 31, 2021, Thermo Fisher Scientific closed the Branford site.

IT Infrastructure—
Thermo Fisher Scientific has gradually transitioned legacy systems and technologies to corporate-supported systems and technologies. New technologies introduced during the period include GitHub, GuardDuty, Pulse Secure VPN, Slack, and the ServiceNow ticketing system, among others.

Complementary User Entity Controls

The controls designed and implemented by Thermo Fisher Scientific to achieve compliance with the applicable trust services criteria require that user entities (i.e., customers) design and implement certain controls complementary to those designed and implemented by Thermo Fisher Scientific. This section summarizes these complementary user entity controls for customer review and consideration.

Logical Access

The PFS is customer-configurable and is capable of enforcing customer-specified password policy settings. User entities should configure the PFS's password policy settings according to their preferences.

The PFS is customer-configurable and is capable of automatically locking a user's session after a period of inactivity. User entities should configure the PFS's session lock according to their preferences.

Customers should have controls in place to administer the access of their personnel to the PFS and validate that access is updated in a timely manner for personnel terminations and changes in job responsibilities.

(The remainder of this page left blank on purpose.)

Section IV — Thermo Fisher Scientific's Service Commitments and System Requirements

Thermo Fisher Scientific's principal service commitments and system requirements include:

- Maintain commercially reasonable and appropriate administrative, physical, and technical safeguards to protect customer data equivalent to those safeguards used to protect Thermo Fisher Scientific data.
- Limit Thermo Fisher Scientific personnel's access to customer data based on business need and provide only the minimum necessary access needed.
- Not disclose customer data to unauthorized third parties, including other Thermo Fisher Scientific customers.
- Promptly notify customers of confirmed incidents of unauthorized access to their data, if any, within 24 hours and provide support and assistance to the customer's breach investigation.
- Upon termination of the agreement and if requested, delete or destroy all customer data in its possession.
- Maintain a Quality Management System aligned with ISO 9001 standards that include policies and procedures including, but not limited to, disaster recovery, data backup and recovery, business continuity, data security, customer incident management, and change management.