

GE VERNOVA

GE VERNOVA ELECTRIFICATION SOFTWARE LLC

SOC 3 REPORT

FOR THE PROFICY SMART FACTORY CLOUD SYSTEM

FOR THE PERIOD OF NOVEMBER 15, 2025, TO FEBRUARY 15, 2026

Attestation and Compliance Services



Proprietary & Confidential
Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To GE Vernova Electrification Software LLC:

Scope

We have examined GE Vernova Electrification Software LLC's ("GE Vernova Electrification Software") accompanying assertion titled "Assertion of GE Vernova Electrification Software LLC Service Organization Management" ("assertion") that the controls within GE Vernova Electrification Software's Proficy Smart Factory Cloud system ("system") were effective throughout the period November 15, 2025, to February 15, 2026, to provide reasonable assurance that GE Vernova Electrification Software's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

GE Vernova Electrification Software uses various subservice organizations for cloud hosting and identity management services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GE Vernova Electrification Software, to achieve GE Vernova Electrification Software's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

GE Vernova Electrification Software is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that GE Vernova Electrification Software's service commitments and system requirements were achieved. GE Vernova Electrification Software has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, GE Vernova Electrification Software is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board (IAASB). 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.

Service Auditor's Independence and Quality Management

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statement on Quality Management Standards established by the AICPA and the International Standard on Quality Management established by the IAASB and, accordingly, maintain a comprehensive system

of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve GE Vernova Electrification Software's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve GE Vernova Electrification Software'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 GE Vernova Electrification Software'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.

Opinion

In our opinion, management's assertion that the controls within GE Vernova Electrification Software's Proficy Smart Factory Cloud system were effective throughout the period November 15, 2025, through February 15, 2026, to provide reasonable assurance that GE Vernova Electrification Software's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Columbus, Ohio
April 29, 2026

ASSERTION OF GE VERNOVA ELECTRIFICATION SOFTWARE SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within GE Vernova Electrification Software LLC's ("GE Vernova Electrification Software") Proficy Smart Factory Cloud system ("system") throughout the period November 15, 2025, to February 15, 2026, to provide reasonable assurance that GE Vernova Electrification Software's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented below 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 November 15, 2025, to February 15, 2026, to provide reasonable assurance that GE Vernova Electrification Software's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. GE Vernova Electrification Software's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 November 15, 2025, to February 15, 2026, to provide reasonable assurance that GE Vernova Electrification Software's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE PROFICY SMART FACTORY CLOUD SYSTEM

Company Background

GE Vernova Electrification Software is headquartered in Cambridge, Massachusetts and a part of GE Vernova Inc. which was officially incorporated as a separate legal entity in April of 2024 after being part of General Electric Company. GE Vernova Electrification Software served as a consolidation of GE Vernova's digital capabilities as it relates to their industrial product offerings. During the third quarter of 2025, GE Vernova signed a binding agreement to sell the Proficy manufacturing software business (Proficy) within Electrification Software business. The transaction is subject to information and consultation with employee representatives and other customary closing conditions, including certain regulatory approvals and expected to close in the first half of 2026.

GE Vernova Electrification Software solutions are intended to help businesses build innovative capabilities to improve profitability and performance. GE Vernova Electrification Software has established strategic partnerships with Fortune 500 information technology service providers to support their product offerings.

Description of Services Provided

GE Vernova Electrification Software's Proficy Smart Factory Cloud software suite is a part of the Proficy manufacturing software business. It provides a scalable cloud platform that serves as a basis for its Software-as-a-Service (SaaS) offering enabling operators to manage, monitor and optimize manufacturing operations.

The Proficy Smart Factory Cloud product suite is comprised of the following applications, each of which can be used independently or in combination:

- Proficy Smart Factory OEE – OEE (Overall Equipment Effectiveness) is a key performance metric used in manufacturing to measure how effectively a machine, production line, or process is being utilized compared to its maximum possible potential during scheduled operating time. OEE shows the percentage of scheduled production time that was used to produce good parts at maximum speed.
- Proficy Smart Factory MES – s a specialized software system and suite of digital tools that manages, monitors, tracks, and controls the real-time execution of manufacturing operations on the shop floor — bridging the gap between high-level planning from an ERP system and the actual machines, operators, and processes producing goods.
- Proficy Smart Factory Production Management – Define, refine and control the route and operations required to make a specific product on a specific line. This module oversees production operations, including functions to control product flow between equipment, develop product genealogy reports, and make schedule changes to reduce excess inventory.
- Quality Management – Module drives consistent quality in products, providing real-time trends, statistics, SPC, and notifications. Integrating process, inspection, and test data from manual and automated sources, it houses information in one place (includes support for 21 CFR Part 11). It attaches comments, specifications, recipes, and procedure documents.
- Predictive Analytics – Proficy Smart Factory Predictive Analytics leverages Artificial Intelligence (AI) and Machine Learning (ML), to uncover patterns, identify anomalies, and enhance asset and process performance. GE Vernova's approach focuses on mining insights from both historical and real-time data, aligning operational improvements with broader goals like sustainability and operational excellence.
- Proficy Scheduler – Proficy Scheduler is a digital scheduling tool that is dedicated to detailed scheduling of production processes. It optimizes production and improves efficiency. Planning processes become less time-consuming and more effective, and costs are reduced on key parameters, including capacity, financing, and materials.

Note – the Proficy Smart Factory software is also offered in an on-premises implementation model. This report covers exclusively the cloud-based Software-as-a-Service (SaaS) offering.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

GE Vernova Electrification Software has put into place a set of policies and procedures to help ensure that security commitments are met. Information security policies and procedures defining key roles and responsibilities, risk management governing principles, and design principles to protect systems and data are documented. In addition to security procedures, standard operating procedures are documented for the operation of the Proficy Smart Factory system. Management has identified actions, in the form of control activities, and put them into place to enforce those standards.

Control activities are part of the process by which GE Vernova Electrification Software manages risk to achieve its business objectives. GE Vernova Electrification Software has applied a risk management approach to the organization to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the overall objectives of the organization. Control activities serve as mechanisms for managing the achievement of those objectives.

GE Vernova Electrification Software makes the following security commitments to their customers:

- Information security policies and procedures are implemented and maintained (e.g., asset and access management, physical and environmental security, change management, operations management, vendor management, incident response, business continuity).
- Logical and physical access to programs, data, and IT resources are restricted to authorized users, and access is restricted to performing authorized actions.
- Changes to the system, including changes to software, processes, and other system components are authorized, tested, documented, approved, and implemented; and network infrastructure is configured as authorized.
- Security incidents are detected, reported, contained, analyzed, remediated, and actions are taken to recover from impairment to service commitments and system requirements.
- Deviations, problems, and errors that may affect the service commitments and system requirements are identified, tracked, recorded, and resolved.
- Customer inquiries and disputes related to security and system operations will be responded to and resolved by GE Vernova Electrification Software in accordance with service level agreements.
- Sensitive data is secured and protected in the Proficy Smart Factory environment through industry standard security protocols, such as secure password protected login and data encryption.
- Employees and suppliers are subject to screening and background verification proportional to their roles and consistent with applicable laws.
- GE Vernova Electrification Software's commercial counterparties are required to meet certain security standards as part of their agreements with GE Vernova Electrification Software. Commercial counterparty security standards are reviewed by GE Vernova Electrification Software at the time of contract creation or renewal.

In accordance with management's assertion, and the description criteria, the service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to system users, in each individual case.

Infrastructure and Software

Production infrastructure supporting Proficy Smart Factory Cloud is hosted in the Amazon Web Services (AWS) cloud environment.

The in-scope infrastructure consists of multiple systems as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Proficy Smart Factory OEE	Product within the Proficy Smart Factory suite of tools used to predict asset failure	AWS RDS Postgres, AWS RDS SQL Server	AWS Windows, Ubuntu Linux hosted on AWS EKS with managed NodeGroup using Elastic Compute Cloud (EC2)
Proficy Smart Factory MES	Product within the Proficy Smart Factory suite of tools used to obtain a unified view of assets' current state and health.		
Proficy Smart Factory Production Management	Product within the Proficy Smart Factory suite of tools used to predict & address issues before they occur.		
Quality Management	Product within the Proficy Smart Factory suite of tools used to reduce risk and optimize life cycle cost.		
Predictive Analytics	Product within the Proficy Smart Factory suite of tools used to keep facilities contained and compliant.		
Proficy Scheduler	Product within the Proficy Smart Factory suite of tools used to reduce hazards risk within industrial processes.		

The Proficy Smart Factory architecture enables different IT systems & OT devices to connect to Proficy Smart Factory, which is a cloud-based enterprise platform for manufacturing execution management. It is an end-to-end solution combining data connectivity, analytics, and edge-to-cloud processing.

The manufacturing information is ingested in a secure way using certificates from DCS (Distributed Control System) Controller, PLC (Programmable Logic Controller), Instrument, MES (Manufacturing Execution System), OPC UA / DA / HDA (Open Platform Communications Unified Architecture / Data Access / Historical Data Access), Proficy Historian, Open Database Connectivity (ODBC), OSI-PI Historian, SAP, and File Servers through the Data Collection servers like GE Vernova's OSM (Outage & Switching Management), Proficy Historian, and finally presented to the customer using secure protocols.

The Proficy Smart Factory Cloud software suite is a Software-as-a-Service (SaaS) offering that enables operators to manage, monitor, and analyze manufacturing operations. The in-scope application is supported by underlying operating systems, databases, and supporting software components hosted within the AWS cloud environment described above. Application code is maintained in source control and deployed through the change management process described in the Procedures section below.

People

The personnel supporting the Proficy Smart Factory system includes, but is not limited to, the following:

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives. Members focus on the areas that are important to shareholders– strategy, risk management, leadership development, and regulatory matters.

- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas such as talent development, organization and employee support, talent recruitment, learning, compensation and benefits, HR operations, and labor relations.
- Cyber Security – responsible for providing cyber security risk management, data governance, identity and access management, secure software development requirements, incident response, and security assessment services.
- Cloud Operations and Platform Enablement (COPE) team – responsible for providing operations, privileged access management, encryption and key management.
- Team Leads – responsible for specific control activities or areas of operation.
- Legal Group – responsible for implementing the GE Vernova Electrification Software integrity framework, including the Open Reporting and Ombuds framework, Code of Conduct compliance training, and for ensuring the company is compliant with applicable regulatory, statutory, policy, and contractual requirements.
- IT and operations personnel – responsible for risk management and identification, monitoring, and compliance of security issues and incidents throughout the service delivery infrastructure. The IT department is subdivided into the following functional groups:
    - Infrastructure – responsible for the management and day-to-day system administration and operation of the various software and hardware supporting the underlying Proficy Smart Factory services.
    - Change Management – responsible for the development, IT testing, and migration of changes into the Proficy Smart Factory production system

Procedures

Access, Authentication, and Authorization

Logical access is managed in accordance with an access control policy. Access to system information, including confidential data, is protected by authentication and authorization mechanisms. Accessing production systems are required to authenticate utilizing a unique user account and predefined minimum password requirements. Users then log into virtual machines through Bastion using enterprise single-sign on with multi-factor authentication. A log monitoring application is utilized to monitor access to production and IT security personnel are alerted when predefined events occur. Administrative access to the production systems is restricted to user accounts accessible by authorized personnel. User access reviews are performed on quarterly basis to help ensure that only authorized personnel maintain access to the production environment.

An overview of the authentication process is as follows:

- Password requirements are set and enforced for each layer as defined within the access management policy.
- An encrypted VPN connection with two factor authentication is required to connect into production systems and TLS is utilized to secure remote connections.
- Unique user IDs are required for authentication to the system and applications.
- Privileged access is restricted to authorized personnel, and access, including VPN, is reviewed quarterly.

Information systems are segregated on networks based on the risks of data being stored and the internal and external users who need access to the systems. Customer environments are segregated from other customers and unauthorized persons in the cloud environment and OT connectivity. Privileged access to set up production of customer tenants is restricted to authorized personnel and is reviewed on a quarterly basis.

Access Requests and Access Revocation

Management has established security controls to restrict access to production systems to those who require access based on business need. A formal provisioning process has been established for managing user accounts and

controlling access to GE Vernova Electrification Software resources within the production environment. Employees are granted permissions based on their job roles and responsibilities after the access request is reviewed and approved by their respective manager with the ticketing system. The ability to create a new user or modify an existing user's access is limited to authorized personnel.

Responsibilities for shared information security roles in the use of the cloud services are allocated to identified parties, documented, communicated, and implemented by both the cloud service customer and the cloud service provider. Users, information systems and customer data are segregated on networks.

Upon notification of employee or contractor termination the ability to access systems and information is automatically removed. Additionally, HR provides a listing of terminated employees at least monthly for access review and revocation to be performed, where not automatically revoked. User access, including privileged access, reviews are performed on a quarterly basis to help ensure that access to data is restricted to authorized personnel.

Asset Management

GE Vernova Electrification Software maintains an asset management policy and a policy in place to help guide personnel in hardening virtual machines in the cloud computing environment. Network access control and intrusion detection are implemented to protect system resources. Malware protection is deployed to protect AWS infrastructure and hosts. Quarterly, system configuration Amazon Machine Images (AMIs) are reviewed to ensure hardening requirements are applied. Hardening configurations are updated and implemented as part of the review process. Testing is performed in lower environments and then change control records are created for production implementation.

A policy and supporting security measures are in place to manage the risks introduced by using mobile devices. Mobile device usage is part of mandatory training for employees. User installation of software is approved prior to installation.

Change Management

Documented change, configuration, patch management and software development lifecycle (SDLC) policies and procedures exist to clearly define that the authorization, development, testing, and implementation functions are segmented functions within the change management process. For changes outsourced to the cloud service provider or changes developed by the vendor and changes developed in-house, the process is monitored and documented. GE Vernova Electrification Software maintains secure development environments and confidential data is not transferred or stored within the development environments throughout the system development lifecycle.

Changes, updates, or new features to the system are communicated to internal and external users through e-mail, system alerts, and/or the sales team.

Routine Changes and Patching

Change Advisory Board (CAB) meetings are held on a weekly basis to discuss impending changes to the infrastructure and applications. Changes that affect production systems are documented through release notes and change tickets. Changes are migrated once approvals are received and documented. Routine changes and patching follow management's formal change management policies and procedures, including the authorization, testing, and approval of a change prior to implementation. Once approved, changes are migrated by authorized personnel. Access to tools used to deploy changes to production code is restricted from users who have the ability to develop changes. Access to develop changes is also restricted to authorized personnel. Secure development environments have been defined that are separate from the production environment that protects the confidentiality of production data.

Changes affecting the production environment are applied via patches provided by the vendor and follow the process identified above members of the change management team push these authorized patches into the production environment at least monthly.

GE Vernova Electrification Software follows the standard GE Vernova Electrification Software change management process to help provide reasonable assurance that unauthorized changes are not made to production application systems.

Members of project management, engineering, and operation teams meet on an as-needed basis to discuss and communicate ongoing and upcoming deployment projects that will impact the system. The meetings are intended to discuss the procedures needed to successfully implement new application releases. These meetings are held before a deployment is to be implemented into the production environment. The meetings are held to review and approve proposed application changes and to ensure that the deployed changes will not impact the performance of production systems. Approved changes are tracked within Aha! tool with change details and requirements. Once the change has been approved, a member of the engineering team implements the change and different individual(s) perform code reviews. Then changes follow a quality assurance (QA) process. Documented test plans and QA procedures are in place and are followed to ensure the changes do not adversely affect the system.

Emergency Changes

Emergency changes and are documented in a ticket post-mortem in accordance with change management procedures. These emergency changes are reviewed at the proceeding CAB meeting.

Configuration Changes

The information security requirements and configuration settings are documented to any additions or changes to the system in order to properly monitor the system. Quarterly reviews are performed on the system configuration standards and any changes required will follow the formal change process. Hardening configurations are updated and implemented as needed as a part of the review process that includes Operations, Cyber Security, Platform and Application Engineering teams as domain approvers. Testing is performed in lower environments and then change control records are created for production implementation.

Infrastructure Security

Vulnerability scanning tools are utilized to automatically identify security threats within the production environment. The vulnerability scanning tools are updated to identify new and upcoming security vulnerabilities. Annually, penetration testing is performed, and issues are investigated. GE Vernova Electrification Software's exposure to the identified vulnerabilities is evaluated and discussed during the quarterly Compliance Review Board (CRB) meetings.

In addition, anti-virus and anti-malware software are deployed to operating system servers to protect against security threats. Policies around the installation of software by users are established. Rules regarding unauthorized software use or installation are communicated to employees via company policies and controlled through the Software Request and Licensing process.

GE Vernova Electrification Software utilizes network and activity monitoring technologies to detect and mitigate cybersecurity threats. A Security Information and Event Management (SIEM) tool aggregates various logs from network, platform, and application infrastructure to centrally monitor and manage cybersecurity-related events. Cybersecurity meetings are held on a weekly basis to review security events received to improve monitoring, alerting, and response capabilities.

GE Vernova Electrification Software has insurance policies in place to protect against loss events that could impair the company's abilities to meet its commitments with regards to security.

Incident Response

Documented incident management policies are in place to guide personnel in cybersecurity incident response and Management Incidents are recorded and maintained in the form of incident tickets while e-mail communication is also utilized to communicate cybersecurity incidents directly to the cybersecurity team. Procedures have been implemented to communicate with internal and external stakeholders when a security incident occurs that results in the unauthorized use or disclosure of their information. Additionally, GE Vernova Electrification Software provides an anonymous hotline and external security event page for customers and employees to report cybersecurity incidents. Incidents are classified according to their severity levels to indicate the level of urgency of the incident to Cyber Security team members. Annually, GE Vernova Electrification Software evaluates and tests the effectiveness of cybersecurity incident response and incident recovery. Procedures are in place to communicate cybersecurity incidents to internal and external stakeholders. Cybersecurity incidents are analyzed, and procedures are improved as needed. Cybersecurity meetings are held on a weekly basis to review security events received to improve monitoring, alerting, and response capabilities.

Disaster Recovery

GE Vernova Electrification Software has created a business continuity plan and disaster recovery plan to guide personnel in procedures to protect against disruptions caused by unexpected events (e.g., during a crisis or disaster). The plans are available to internal users via the organization's intranet. These plans are reviewed and tested on an annual basis.

Data

GE Vernova Electrification Software considers customer information confidential and protects records from loss, destruction, falsification, unauthorized access, or release in accordance with contractual requirements and GE Vernova Electrification Software policies. Data is categorized in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. GE Vernova Electrification Software has established data transfer policies, procedures, and controls to maintain confidentiality using secure file transfer protocol (SFTP), HTTPS, an intrusion detection system (IDS), and encryption of data at rest and networks.

Encryption is implemented in accordance with the management's data protection plan. Formal data transfer policies, procedures, and controls are in place to protect the transfer of information. Data transmitted from external to internal networks is encrypted in accordance with approved algorithms. Data at rest is encrypted and access is restricted to authorized personnel.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Manufacturing Data	Data is available to authorized users for managing the manufacturing processes.	Confidential

Subservice Organizations

The cloud hosting and identity management services provided by AWS and GE Vernova Inc. were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS and GE Vernova Inc., alone or in combination with controls at GE Vernova Electrification Software, and the types of controls expected to be implemented at AWS and GE Vernova Inc. to meet those criteria.

Control Activities Expected to be Implemented at Subservice Organizations	Applicable Trust Services Criteria
AWS is expected to implement control activities to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the GE Vernova Electrification Software systems reside.	CC6.1 – CC6.3, CC6.5 – CC6.6
GE Vernova Inc. is expected to implement control activities to help ensure access to the identity management provider is provided based on user responsibilities.	CC6.1, CC6.3
GE Vernova Inc. is expected to implement control activities to help ensure access to the identity management provider requires unique user IDs for authentication to the system.	
GE Vernova Inc. is expected to implement control activities to help ensure access to the identity management provider has password requirements that are set and enforced as defined within their access management policy.	CC6.1

Control Activities Expected to be Implemented at Subservice Organizations	Applicable Trust Services Criteria
GE Vernova Inc. is expected to implement control activities for the identity management provider that helps ensure access requests are documented in their ticketing system and approved prior to access being granted.	CC6.2 - CC6.3
GE Vernova Inc. is expected to implement control activities for the identity management provider that helps ensure the ability to access systems and information is automatically removed upon termination of employment, contract, or agreement.	
GE Vernova Inc. is expected to implement control activities to help ensure access to the identity management provider is revoked when access is no longer required.	
AWS is expected to implement control activities for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
AWS is expected to implement control activities for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the GE Vernova Electrification Software systems reside.	CC6.7
AWS is expected to implement control activities to monitor the logical access control systems of the underlying network, virtualization management software, and storage devices for its cloud hosting services where the GE Vernova Electrification Software systems reside.	CC7.2

Complementary User Entity Controls

GE Vernova Electrification Software's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security category are applicable to the Proficy Smart Factory Cloud system.