Access Control

AC-01 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AC-01 Control Summary Information
Responsible Role: Customer Administrator, Product1 Trust Program Manager, Program Manager
Parameter AC-01(a): all personnel
Parameter AC-01(a)(1): organization-level
Parameter AC-01(b): Appropriate service team personnel, security engineering teams, service provider personnel with authority on access control policies
Parameter AC-01(c)(1)-1: at least annually
Parameter AC-01(c)(1)-2: significant changes

Parameter AC-01(c)(2)-1: at least annually
Parameter AC-01(c)(2)-2: significant changes
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-01 What is the solution and how is it implemented?
Part a <u>Customer Responsibility</u> Government customers are responsible for developing and maintaining appropriate Access Control policies and procedures that govern access management activities for their organization and users. Customers are responsible for setting access control policies that support the confidentiality of stored content. For example, sensitive documents stored in SharePoint should not be shared outside of the Product1 boundary, and sensitive email should be sent using encryption. <u>Product1</u> **Part 1** The "Product1 Information Security Policy" provides the overarching security guidance for Product1. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Company organizations providing some level of support for the security of Product1. Policies are distributed via SharePoint to personnel responsible for implementing access control policies and procedures.

Part 2

Standards and procedures to facilitate execution of the Product1 Information Security Policy are documented in the Product1 SOPs and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Product1 SOPs are distributed via SharePoint to roles providing support for Product1 security.

Part b

Customer Responsibility

Government customers are responsible for designating an organization-defined official to manage the development, documentation, and dissemination of their organization's access control policy and procedures.

Product1

The "Product1 Information Security Policy" provides the overarching security guidance for Product1. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Company organizations providing some level of support for the security of Product1. Policies are distributed to personnel responsible for implementing access control policies and procedures via SharePoint.

The "Product1 Information Security Policy" is reviewed and updated annually.

Part c

Customer Responsibility

Government customers are responsible for annually updating their Access Control policies and procedures.

Product1

Part 1

The Product1 Information Security Policy is reviewed and updated at least annually or whenever a significant change occurs.

Part 2

The "Product1 Information Security Policy" and AC SOP are reviewed and updated at least

annually or whenever a significant change occurs.

AC-02 Account Management

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;

d. Specify:

1. Authorized users of the system;

2. Group and role membership; and

3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;

e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];

g. Monitor the use of accounts;

h. Notify account managers and [Assignment: organization-defined personnel or roles] within:

1. [FedRAMP Assignment: twenty-four (24) hours] when accounts are no longer required;

2. [FedRAMP Assignment: eight (8) hours] when users are terminated or transferred; and

3. [FedRAMP Assignment: eight (8) hours] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. [Assignment: organization-defined attributes (as required)];

j. Review accounts for compliance with account management requirements [FedRAMP Assignment: monthly for privileged accessed, every six (6) months for non-privileged access];

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

AC-02 Control Summary Information
Responsible Role: Customer Administrator, Product1 Trust Program Manager, Program Manager
Parameter AC-02(c): IDM eligibilities
Parameter AC-02(d)(3): RBAC
Parameter AC-02(e): Service Team Manager or Eligibility Owner
Parameter AC-02(f): Company Product1 Information Security Policy
Parameter AC-02(h): relevant security group members
Parameter AC-02(h)(1): twenty-four (24) hours
Parameter AC-02(h)(2): eight (8) hours
Parameter AC-02(h)(3): eight (8) hours
Parameter AC-02(i)(3): security group membership
Parameter AC-02(j): monthly for privileged accessed, every six (6) months for non-privileged access
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

AC-02 What is the solution and how is it implemented?

Part a

Customer Responsibility

All customers, including government and non-government customers, are responsible for identifying the account types for their organization in compliance with their organizational policies. Customers will configure their account types in their existing Active Directory infrastructure or they will configure account types in AAD.

Non-government customers will configure account types in AAD via SUE. For more information on managing customer account types via the Product1 Admin Center, see the following link:

Guest access to Product3 meetings, if enabled, allows anyone with a meeting invite to access the meeting lobby; this method of guest access is considered session access as no account is assigned to the guest user. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting. Government customers are responsible for disabling guest access to Product3 meetings to remain compliant with FedRAMP standards as advised in "Product1 Complementary Federal User Entity Control".

Non-government customers are responsible for determining if the use of guest access to Product3 meetings should be allowed for their organization. This setting can be configured by government and non-government customers.

SharePoint Online guest invitations allow external users to access an organization's SharePoint Online site(s). Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online, as an account type, should be allowed for their organization. Government customers are responsible for disabling guest access to SharePoint Online to remain compliant with FedRAMP standards. The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers.

For more information, see the Company Product1 Solution and Architecture Center:

Product1

Product1 accounts are only provided to Company personnel supporting Product1 services. Accounts with permissions to internal assets and resources are not provisioned to customers. Company personnel are assigned unique corporate network (CorpNet) AD accounts as part of a standard onboarding to Company. These CorpNet accounts, known as user alias', do not have access to any production environment by default.

For personnel supporting Product1 services, service team accounts are used to manage and administer Product1. Service team accounts tie to the user's CorpNet account. This alias is consistent across all of the user's accounts in all Company domains, including Product1. CorpNet and Product1 access are provisioned and managed using separate account management tools.

Below are the different account types that Product1 utilizes:

Standard Access
All personnel with standard access to Product1 are granted system metadata read access used for regular troubleshooting, release management, and other maintenance and monitoring activities. Standard access provides permissions to key Product1 tools, services, SharePoint sites, documentation, and a variety of dashboards.

Standard access does not provide access into the production environment. A user with standard access may have the need to review service-specific logs within Product1 to identify and diagnose issues. Any additional permissions above standard access requires elevation of access via Torus JIT, described below.

Elevated Access
All personnel must use JIT when interactive elevated access is required in the Product1 production environment. Except in the case of an approved exception as described below, there is no standing or persistent elevated access to the production environment. The primary exception is Break-Glass elevated access, described below.

In scenarios where JIT does not yet support management of elevated access, standing access may exist; these gaps in JIT support are identified and tracked as an exception, which requires approval. Software deployment via automated means (i.e., not using an interactive login) does not require interactive login to a resource that is accessed via JIT. In this case, a service team member submits a job (e.g., Pull Request in Product2 DevOps), and another team member reviews, approves, and then the safe deployment system deploys.

Elevated Access – Break-Glass Access
Product1 maintains Break-Glass accounts with elevated access for use in the scenario that the JIT service is not available. These accounts have persistent elevated access to perform maintenance activities if JIT is unable to provide temporary elevated access. These accounts are carefully managed, only to be used in emergencies, and have notifications associated with their use. Whenever such an account is utilized, a Severity 2 incident ticket is generated that requires the service that owns the resource to investigate and determine whether the access is valid.

Service Accounts
Non-user, non-interactive service accounts are used to run relevant services. Service accounts are not used for interactive logins. For example, software deployment via automated

means does not require interactive login to a resource that would normally be accessed via JIT. In this example, a service team member submits a job, such as a Pull Request in Product2 DevOps, and another team member reviews and approves.

Part b

Customer Responsibility

All customers, including government and non-government customers, are responsible for assigning account managers for the account types identified in part a of this control.

Product1

Product1 assigns account managers to each role type using IDM, which include workflows that enforce business rules. Throughout this SSP, these tools are collectively referenced as "account management tools".

Part c

Customer Responsibility

All customers, including government and non-government customers, are responsible for establishing conditions for group/role membership for their organization in compliance with their organizational policies.

Non-government customers will configure groups in AAD via SUE. For more information on managing customer groups/roles in AAD via the SUE portal, see the following link: <some_link>.

Product1

Service teams establish conditions for group/role membership by defining and enforcing conditions for each group/role in account management tools. In addition, service teams use Torus and IDM to enforce additional, more granular conditions for privilege escalation and approval for interactive sessions.

Product1 establishes conditions for group and role membership based on least privilege necessary for a user to perform their assigned duties. Predetermined conditions are established when groups are created.

Part d

Customer Responsibility

Part 1, 2, 3

Government and non-government customers are responsible for identifying organizationally authorized users and specifying access privileges for those users using their existing Active Directory (AD) infrastructure. These users utilize the customer AD infrastructure to identify, authenticate, and apply permissions to that user's session. Customers communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

Non-government customers will manage user accounts in AAD via SUE. For these customers, AAD is responsible for identifying organizationally authorized users and will enforce the access privileges defined by the customer. For more information on managing customer user identifiers and specifying access privileges in AAD via the SUE portal, see the

Product1

Part 1, 2, 3

Role Based Access Control (RBAC) is used to identify and control the access privileges of each service team personnel Service teams define their roles in IDM which contain a list of eligibilities. Eligibilities vary depending on the role that a specified service team personnel will assume within the service team. Privileges are defined in the eligibilities and enforced by Active Directory.

By default, these service team accounts initially belong to a security group that has remote system metadata read access, and no direct access to the production environment. If service team personnel need additional access to the production environment, they request that access and provide business justification using Just-In-Time (JIT) tools.

Part e

Customer Responsibility

All customers, including government and non-government customers, are responsible for requiring appropriate approvals for requests to establish organizational accounts in compliance with their organizational policies. Government and non-government customers will manage their accounts in their existing Active Directory infrastructure.

Non-government customers will configure account types in AAD via SUE. For more information on managing customer account types via the Product1 Admin Center, see the following link: <some_link>

Product1

In order to gain access to the production environment, service team personnel must first request access via the account management tools; access to the production environment is provided via security group membership. Approval to establish the account from the service team's management is required for a service team administrator to be added to the appropriate security group. These approvals are tracked and enforced by account management tools.

Part f

Customer Responsibility

Government customers are responsible for establishing, activating, modifying, disabling, and removing organizational accounts in accordance with their procedures using their AD infrastructure. Government users utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user's session. Government users communicate identification/authentication, and the associated permissions to AAD via certificate-based authentication.

For more information on managing user accounts in Active Directory (AD), see the following link: <some_link>

Non-government customers establish, activate, modify, disable, and remove organizational accounts following the same procedures outlined for government customers. Non-government customers manage user accounts in AAD via SUE.

For more information on managing customer accounts via the SUE portal, see the following link: <some_link>

Product1

Account changes are managed through IDM in accordance with Product1 Standard Operating Procedures (SOP) The Product1 Information Security Policy and rules have been defined in account management tools which provide an automated workflow that allows service teams to track account requests, approvals, creations, modifications, and deletions. Service team managers are responsible for approving account lifecycle events in account management tools, ensuring that Product1 establishes, activates, modifies, disables, and removes accounts appropriately.

Part g

Customer Responsibility

Government customers are responsible for monitoring the use of information system accounts managed by their AD. See AU-2, AU-3, AU-6, and SI-4 for more details about these

responsibilities.

Product1

Product1 monitors the use of information system accounts in accordance with the AU family of security controls. Product1 records the auditable events defined in AU-2 with the content defined in AU-3 and monitors those records in accordance with the control descriptions for AU-6 and SI-4.

Part h

Customer Responsibility

Part 1, 2, 3

Government and non-government customers are responsible for implementing processes to notify customer account managers when accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need-to-know changes.

Product1

Part 1, 2, 3

Product1 uses automated workflow account management tools that allow service teams to track the account management process through account request, approval, creation, modification, and deletion. As changes occur, the corresponding account manager is notified of the changes that require their approval. Information system usage and need-to-know are mapped to the roles defined by each service team. When an employee is transferred or their employment is terminated, the account management tools will automatically revoke the associated account's access to the privileges mapped to their previous role.

Part i

Customer Responsibility

Part 1, 2, 3

Government customers are responsible for managing organizational user accounts by granting access to Product1 based on: a valid access authorization; intended system usage; and other attributes as required by the organization or associated missions/business functions using their AD infrastructure. Government users utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user's session. Government users communicate identification/authentication, and the associated permissions to AAD via

certificate-based authentication.

For more information on managing user accounts in AD, see the following link: <some_link>

Non-government customers can manage organizational user accounts by granting access to Product1 based on: a valid access authorization; intended system usage; and other attributes as required by the organization or associated missions/business functions following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE.

For more information on managing customer accounts via the SUE portal, see the following link: <some_link>

Product1

Part 1, 2, 3

Product1 Membership in security groups that give access to the system is given only to those in specific roles that require system access. Service team managers are responsible for approving group membership. Service team personnel with the access approver role then review and approve or deny the type of access requested. Access is only provided for a finite period of time (no more than 24 hours) based on the expected duration of the work to be performed. If access is approved, Torus assigns the service team personnel to eligibilities with the minimum permissions required to perform the work and automatically revokes permissions at the end of the specified time period. The managers validate the eligibilities requested and justification provided and grant access once validated.

Part j

Customer Responsibility

Product1 Customers are responsible for reviewing the accounts of their organization's users in compliance with their organizational policies. Product1 allows for customers to manage/review their user accounts via SUE.

For more information on managing user accounts in AD, see the following link: <some_link>

Non-government customers may manage accounts in Product2 Active Directory via the Suite User Experience (SUE) portal. Customers are responsible for logging into the portal and reviewing the Product1 MT accounts of their users compliant with their organizational policies. Disabling or removing users in the SUE portal revokes access to Product1 MT for the affected users.

For more information on managing user accounts via the SUE portal, see the following link: <some_link>

Product1

The Product1 service teams review service team administrator accounts at least monthly.

Access is based on specific roles and duties to support the operational environments. The foundation is granting elevated access for a limited duration through JIT not to exceed twenty-four (24) hours; and a formal program that monitors account activities enabled by auditing account management actions. This provides ongoing review of accounts and alerts of changes. The objective is a continuous rather than static review of access authorizations and activities.

Part k

Customer Responsibility

If government customers allow the use of group shared customer accounts, they are responsible for terminating group/shared account credentials when individuals leave the group.

Non-government customers will terminate credentials using SUE.

Product1

Product1 does not allow the use of shared/group service team accounts.

Part l

Customer Responsibility

Government customers are responsible for aligning account management processes with personnel termination and transfer processes within their organization.

Product1

Torus performs a full sync with the Human Resources Information System (HRIS) every 4 hours as well as differential syncs in near-real time. Syncs between these account management tools will revoke account access if the account no longer meets requirements for access; this could be for: inactivity, background check, clearance, EUPI attestation, or when an employee is transferred or their employment is terminated.

AC-02(01) Automated System Account Management

Support the management of system accounts using [Assignment: organization-defined automated mechanisms].

AC-02(01) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Program Manager
Parameter AC-02(01): IDM, MyAccess
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-02(01) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for automatically terminating temporary and emergency government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure (no more than 30 days for FedRAMP compliance). Government customers are responsible for employing their Active Directory (AD) infrastructure as automated mechanisms to support their organizational user accounts. Certificate-based authentication (CBA) is available to Government users to communicate identification/authentication and the associated permissions to AAD. For information regarding how to manage user accounts in AD, see the following link: <some_link>.

Non-government customers can employ AD as an automated mechanism following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers, AAD is employed as an automated mechanism to support their organizational user accounts.

For more information on managing customer accounts via the SUE portal, see the following link: <some_link>.

Product1

IDM is an automated workflow management tool that allows service teams to manage service team administrator and service accounts through account request, approval, creation, modification, and deletion. IDM integrates with Company Online Directory Service (MSODS) to provide identity synchronization, certificate management, service team administrator password resets and service team administrator provisioning from a single interface. Service team managers are responsible for approving requests in IDM.

By default, service team AD accounts belong to a security group that only has read access to the production environment. Additionally, if a service team administrator needs elevated privileges to the production environment, they request that access, providing a business justification using Torus and IDM. A service team administrator with the access approver role then reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, Torus and IDM assign the service team administrator to security groups with the minimum permissions required to perform the work and automatically revokes permissions at the end of the specified time period.

Falcon, ObjectStore, and SCS also use MyAccess to manage security groups, which are used to gain access to Product2 PaaS services, Source Depot, and configuration files.

AC-02(02) Automated Temporary and Emergency Account Management

Automatically [FedRAMP Assignment: Selection: disables] temporary and emergency accounts after [FedRAMP Assignment: no more than 24 hours from last use].

AC-02(02) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Parameter AC-02(02)-1: Disables
Parameter AC-02(02)-2: no more than twenty-four (24) hours from last use

Implementation Status (check all that apply):
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-02(02) What is the solution and how is it implemented?

Customer Responsibility

Government customers are responsible for automatically terminating temporary and emergency government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure (within 24 hours for FedRAMP compliance). Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For information regarding how to manage user accounts in AD, see the following link: <some_link>.

Non-government customers can manage terminating temporary and emergency accounts following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD the process for terminating temporary and emergency accounts will be manual.

For more information on managing accounts via the SUE portal, see: <some_link>.

Product1

The Company Security Program Policy (MSPP) prohibits the use of temporary and emergency accounts. All local guest accounts are disabled on the system or platform wherever they are located. All account requests follow the standard account management process.

For servers that are not domain-joined, the JIT process for granting access to a server

includes creating and enabling a local account for the duration of access. JIT sessions are task-based and have a default TTL of 4 hours and cannot exceed 24 hours, as documented in AC-2(11). When the life of an authenticator has ended, the service team member must re-request access, gain approval, and generate a new authenticator. Because this access is tied to a specific user's domain account and requires that the user first authenticate using multifactor authentication, Product1 does not consider this local account to be a temporary account for purposes of this control.

AC-02(03) Disable Accounts

Disable accounts within [FedRAMP Assignment: 24 hours for user accounts] when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

(d) Have been inactive for [FedRAMP Assignment: thirty-five (35) days (See additional requirements and guidance.)].

AC-02(03) Additional FedRAMP Requirements and Guidance:

AC-2 (3) Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

AC-2 (3) (d) Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP some_link.

AC-02(03) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Parameter AC-02(03)-1: twenty-four (24) hours for user accounts
Parameter AC-02(03)(d): Thirty-five (35) days for user accounts (See additional requirements and guidance.)
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented

☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-02(03) What is the solution and how is it implemented?

Part a

Customer Responsibility

Government customers are responsible for automatically disabling inactive government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For information regarding how to manage user accounts in AD, see the following link: <some_link>.

Product1

Service team accounts are automatically disabled after their Torus session is completed or expired. Torus sessions last no longer than 24 hours.

Part b

Customer Responsibility

Government customers are responsible for automatically disabling inactive government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For information regarding how to manage user accounts in AD, see the following link: <some_link>.

Product1

Service team accounts are automatically disabled after their Torus session is completed or are no longer associated with an individual. Torus sessions last no longer than 24 hours.

Part c

Customer Responsibility

Government customers are responsible for automatically disabling inactive government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For information regarding how to manage user accounts in AD, see the following link: <some_link>.

Product1

Service team accounts are automatically disabled when in violation of organizational policy. Torus sessions last no longer than 24 hours.

Part d

Customer Responsibility

Government customers are responsible for automatically disabling inactive government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For information regarding how to manage user accounts in AD, see the following link: <some_link>.

Product1

Service team accounts are automatically disabled after their Torus session is completed. Torus sessions last no longer than 24 hours.

AC-02(04) Automated Audit Actions

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AC-02(04) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

AC-02(04) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for automatically disabling inactive government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure (no more than 35 days for DISA SRG compliance). Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication. For information regarding how to manage user accounts in Active Directory, see the following link: <some_link>. Government customers are responsible for monitoring the use of information system accounts managed by their AD. See AU-2, AU-3, AU-6, and SI-4 for more details about these responsibilities. Non-government customers can audit account creation, modification, disabling, and termination actions as well as notify appropriate individuals for change to their organizational

user accounts following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, audit records of account creation, modification, disabling, and termination will be retained for 90 days; the process for notifying appropriate individuals for change to their organizational user accounts will be manual.

For more information on managing customer accounts via the SUE portal, see: <some_link>.

Product1

Product1 performs automated auditing of privileged service team accounts through account management tools, which provide a record of account creation, modification, disabling, and termination of accounts. A notification is sent to the account manager when accounts are changed or managed in any way.

Auditing of Product2 Portal accounts is inherited from Product2. Product2 performs auditing of privileged user accounts through an event forwarding tool, which provides a record of all changes made to accounts and notifies the Security Incident Management (SIM) team for any suspicious activities. The account management tools logs account creation, modification, and disablement actions. Monitoring is in place to record all changes to accounts in the Product2 managed domains. Alerts are generated to the workflow ticketing tool if anyone other than the members of the Online Services Security Accounts and Access team or the account management tool service account modifies a user account or security group in the Product2 managed domains. Network device access is audited via logs from the Product2 managed CISCO ACS system.

AC-02(05) Inactivity Logout

Require that users log out when [FedRAMP Assignment: inactivity is anticipated to exceed Fifteen (15) minutes].

AC-02(05) Additional FedRAMP Requirements and Guidance:

AC-2 (5) Guidance: Should use a shorter timeframe than AC-12.

AC-02(05) Control Summary Information
Responsible Role: Customer Administrator, Product1 Trust Program Manager, Service Engineer Operations
Parameter AC-02(05): inactivity is anticipated to exceed Fifteen (15) minutes
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented

☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-02(05) What is the solution and how is it implemented?

Customer Responsibility

Government customers are responsible for identifying and implementing their own requirements for expected inactivity or scenarios where government personnel are expected to log out.

Product1

Product1 requires that service team administrators log out of Product1 in advance of any expected unattended workstation inactivity, or when they have completed the task that was the purpose of the log in. Additionally, when a user has elevated to administrative access using the JIT process, that user's connections are automatically terminated upon expiration of the elevation.

AC-02(07) Privileged User Accounts

(a) Establish and administer privileged user accounts in accordance with [Selection: a role-based access scheme; an attribute-based access scheme];

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

AC-02(07) Control Summary Information

Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager
Parameter AC-02(07)(a): a role-based access scheme
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-02(07) What is the solution and how is it implemented?
Part a <u>Customer Responsibility</u> Government customers are responsible for establishing and administering privileged user accounts with a role-based access scheme that organizes Product1 customer privileges into roles in compliance with their organizational policies. Government customers will manage their account roles in their existing Active Directory infrastructure. For information regarding how to manage user accounts in Active Directory, see the following link: <some_link>. Non-government customers will manage their account roles in AAD via SUE. For more information on managing customer accounts via the SUE portal, see: <some_link>. <u>Product1</u> All service team personnel accounts are considered privileged. Service team users are assigned to security roles, which have a defined list of available permissions. By default, service team accounts belong to a security group that only has remote access to read system metadata, and no direct access to the production environment. If a service team user needs

elevated privileges to the production environment, they must request that access and provide a business justification using Torus and IDM. A service team user with the access approver role then reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, Torus and IDM assign the service team user to security groups with the minimum permissions required to perform the work and automatically revoke permissions at the end of the specified time period.

Additionally, for OSI and some IS teams, service team personnel are assigned a role within their service team that corresponds to a security group. Each security group is assigned permissions to correlating environments with just enough access to properly fulfill their tasks. Service team managers are responsible for approving role assignments.

Part b

Customer Responsibility

Government customers are responsible for tracking and monitoring privileged role assignments, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For more information on managing user accounts in Active Directory, see the following link: <some_link>.

Non-government customers can track and monitor privileged role assignments following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, audit records of assignment to privileged roles will be retained for 90 days; the process for tracking privileged role assignments will be manual.

For more information on managing customer account role assignments via the SUE portal, see: <some_link>.

Product1

All service team accounts are considered privileged and are tracked and monitored using automated account management tools. For service teams that require Just-In-Time elevated access to the production environment, role assignments are tracked and monitored through Torus and IDM.

Part c

See part b.
Part d Customer Responsibility Government and non-government customers are responsible for defining and taking required actions when privileged role assignments for customer users are no longer appropriate. Product1 Privileged role assignments are no longer appropriate when Product1 personnel no longer have need of the role to support their current work, or if their employment with Company is terminated. In those cases, Product4 follows the account management workflows to disable the account or revoke access. The system has the capability of terminating a user session on the Terminal Services Gateway (TSG) immediately. The TSGs are managed by Terminal Service Gateway service or inherited from Product2. First, the account associated with the user is disabled, then the session is terminated on the TSG. This prevents the user from further remote access of the system.

AC-02(09) Restrictions on Use of Shared and Group Accounts

Only permit the use of shared and group accounts that meet [FedRAMP Assignment: organization-defined need with justification statement that explains why such accounts are necessary].

AC-02(09) Additional FedRAMP Requirements and Guidance:

AC-2 (9) Requirement: Required if shared/group accounts are deployed

AC-02(09) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager
Parameter AC-02(09): exception-based criteria
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned

☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-02(09) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for defining conditions for establishing shared/group accounts and enforcing those conditions if they choose to establish shared/group accounts. Product1 Product1 does not allow the use of shared/group service team accounts unless the requirement to uniquely attribute user activity to the account is implemented; exceptions may be approved on a case-by-case basis.

AC-02(11) Usage Conditions

Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].

AC-02(11) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager
Parameter AC-02(11)-1: Time-based access control
Parameter AC-02(11)-2: Information system accounts with access to the production environment
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented

☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-02(11) What is the solution and how is it implemented?

Customer Responsibility

Government customers are responsible for enforcing the appropriate usage and time-based usage restrictions for all customer-controlled accounts.

Product1

Product1 requires the use of Torus, an internal Just-In-Time (JIT) access control tool, to access the production environment. Requests for access through Torus must be approved by an eligibility owner and there are limitations to the access granted:

• JIT sessions have a default TTL of 4 hours and cannot exceed 24 hours
• Sessions are also task-based – all requests must include a justification and grant a restricted set of permissions that are scoped to the requested task
• The management forest for Torus is isolated from, and does not trust, the management forests of other service teams, further protecting access control mechanisms from compromise

This process can be circumvented only in the event of an emergency through the use of a "breakglass" account. There are very few of these accounts. Use of one creates a Sev 1 alert to the incident response team and causes the breakglass account password to be rotated.

AC-02(12) Account Monitoring for Atypical Usage

(a) Monitor system accounts for [Assignment: organization-defined atypical usage]; and

(b) Report atypical usage of system accounts to [FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization].

AC-02(12) Additional FedRAMP Requirements and Guidance:

AC-2 (12) (a) Requirement: Required for privileged accounts.

AC-2 (12) (b) Requirement: Required for privileged accounts.

AC-02(12) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager
Parameter AC-02(12)(a): Atypical use configured in Near Real Time (NRT) Security Monitoring and automated security alert logic
Parameter AC-02(12)(b): At a minimum, the ISSO and/or service owners or OCEs within the organization
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-02(12) What is the solution and how is it implemented?
Part a Customer Responsibility Government customers are responsible for defining atypical use and monitoring for that use on their infrastructure. Government customers can additionally review Product1 application logs and analyze them for atypical use. Product1 Product1 uses Vanquish for Near Real Time (NRT) Monitoring for security alerting and

monitoring, which has two high-level methods of alerting. An alert can be configured to fire on a specific event or when multiple events correlate to show an indication of compromise. Atypical use is considered any action that falls outside of the normal baseline activity for each service team as defined by Vanquish.
Part b Customer Responsibility Government and non-government customers are responsible for reporting atypical usage to defined organizational personnel. Product1 Product1 follows normal incident reporting procedures if an indication of compromise is detected. These procedures require reporting incidents to the Product1 Security Incident & Response.

AC-02(13) Disable Accounts for High-risk Individuals

Disable accounts of individuals within [FedRAMP Assignment: one (1) hour] of discovery of [Assignment: organization-defined significant risks].

AC-02(13) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager
Parameter AC-02(13)-1: one (1) hour
Parameter AC-02(13)-2: any significant risk
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-02(13) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for disabling user accounts posing a significant risk. Product1 The Product1 Security Incident & Response (SIR) team is notified by MSIT Corporate Security to monitor users that pose significant risk. Account management tools synchronize with the Human Resources Information System (HRIS). When a service team user is marked as disabled in HRIS, this information propagates to account management tools, which then automatically deactivates the service team domain account. Any accounts associated with the Company user are disabled in real time.

AC-03 Access Enforcement

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-03 Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)

☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-03 What is the solution and how is it implemented?

Customer Responsibility

Government customers are responsible for enforcing approved authorizations for logical access to the system, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication. Once permissions are communicated to AAD, AAD is responsible for enforcing those permissions for the users Product1 session.

For information regarding how to manage user accounts in Active Directory, see the following link: <some_link>.

Non-government customers can enforce approved authorizations for logical access to the system following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, AAD is responsible for enforcing the approved authorizations set by the customer in the SUE portal.

For more information on managing customer account privileges via the SUE portal, see the following link: <some_link>.

Product1

Product1 service teams enforce approved authorizations for logical access using role-based access control enforced by AD and Product2 Active Directory (AAD). Product1 uses AD to implement role-based access control (RBAC) via the use of AD groups. For the purposes of this control, the term "security group" references an AD group which is used to enforce RBAC permissions.

Product1 service teams are responsible for managing security groups in the production domain. Product1 has three major account types: service team, customer, and service. Service team accounts are used by service team personnel to manage and administer Product1 Customer accounts are used by customer users to access Product1. Service accounts are used by various services to authenticate to servers and other services.

AC-04 Information Flow Enforcement

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

AC-04 Control Summary Information
Responsible Role: Customer Administrator, Service Engineer Operations
Parameter AC-04: ACLs and firewall rules
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-04 What is the solution and how is it implemented?
<u>Customer Responsibility</u> Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Product1. Product1 will be accredited to store, process, and transmit up to moderate Impact information as defined by NIST SP 800-60. Non-government customers are responsible for ensuring that information stored, processed, or transmitted via the services provided to them by Product1 MT is appropriate and in compliance with the risk policies of their organization. Customer Lockbox is an optional feature that customers can use for controlling the flow of information in EXO. This feature allows customers to control Company administrators' ability to access their content. If in response to a customer support request, a Company

administrator needs access to customer content, that Company administrator initiates a Just In Time request which is routed to a customer administrator; this is in addition to the normal internal required access approvals. The customer administrator can then approve or deny this request via the customer administrator portal. Note that even if customers choose not to use this tool, Product1 Information Security Policy is to never access customer content unless initiated by a customer request, and access to this data is always restricted to screened personnel with required JIT approvals. Customer Lockbox places the technical enforcement of this policy within the customer's direct control.

For additional information, see: <some_link>.

Product1

Product1 implements information flow control by allowing only connections and communication which are necessary to allow systems to operate, blocking all other ports, protocols and connections by default. This includes intra-service communications as well as connections to external information systems. Access Control Lists (ACLs) restrict network communications by source and destination networks, protocols, and port numbers.

Product1 manages ACL and other firewall rule changes through the same configuration management processes as code changes, which includes review and approval steps. ACLs are stored in Product1's source code repository, Source Depot. ACL changes are implemented to the networking devices through various tools and APIs, including NetConf and Product2 management APIs.

The use of firewall rules and ACLs allows Product1 to control the flow of information within the system and between interconnected systems. The use of the RFC process ensures that data flows are authorized and approved.

A detailed diagram of the Product1 dataflows, which includes all internal and external information flows, is included in this SSP.

Product1 is being tested at a High Impact level to demonstrate compliance with the additional controls, but has not been sponsored for a High ATO at this time.

AC-04(04) Flow Control of Encrypted Information

Prevent encrypted information from bypassing [FedRAMP Assignment: intrusion detection mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].

AC-04(04) Additional FedRAMP Requirements and Guidance:

AC-4 (4) Requirement: The service provider must support Agency requirements to comply with M-21-31 (some_link) and M-22-09 (some_link).

AC-04(04) Control Summary Information
Responsible Role: Customer Administrator, Service Engineer Operations
Parameter AC-04(04)-1: intrusion detection mechanisms
Parameter AC-04(04)-2: blocking the flow of encrypted information
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-04(04) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for preventing encrypted information from bypassing content-checking mechanisms by (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; organization-defined procedures or methods. Product1 supports customer compliance with M-21-31 and M-22-09. Product1 Product1 prevents encrypted information from bypassing IDS through implementing information flow control by allowing only connections and communication which are necessary to allow systems to operate, blocking all other ports, protocols and connections by default. This includes intra-service communications as well as connections to external information systems. Access Control Lists (ACLs) are the preferred mechanism to restrict network communications by source and destination networks, protocols, and port numbers.

ACLs exist at both the host and network level. Product1 manages ACL approvals through the Request For Change (RFC) process (including review and risk acceptance) and the change process, and Product2 implements the approved change. Approved mechanisms to implement networked-based ACLs include: ACLs on routers managed by Product2 and firewall rules.

The use of firewall rules and ACLs allows Product1 to control the flow of information within the system and between interconnected systems. The use of the RFC process ensures that data flows are authorized and approved.

Service teams also employ HostIDS to further monitor for data exfiltration at the host level. NRT is used to alert based on specific security events as well as other indicators of compromise, through Vanquish, such as anomalous behavior and suspicious activity.

AC-04(21) Physical or Logical Separation of Information Flows

Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

AC-04(21) Control Summary Information
Responsible Role: Service Engineer Operations
Parameter AC-04(21)-1: TLS 1.2 and Active Directory Organizational Units
Parameter AC-04(21)-2: Separation of all sessions
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-04(21) What is the solution and how is it implemented?
Product1 Product1 separates all information flows logically using user session encryption. TLS 1.2 ensures the confidentiality and integrity of each flow; only the intended recipient can decrypt information. Additionally, each Product1 customer is placed in a separate Organizational Unit (OU) within Active Directory. Customer content within Product1 is always tied to the customer's specific OU and Product1 will only grant access to the data if there is a valid ticket from AAD authorizing access to the OU and the specific data. For a detailed discussion of how Product1 separates flows and tenant data, please see: <some_link> <some_link>

AC-05 Separation of Duties

a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and

b. Define system access authorizations to support separation of duties.

AC-05 Additional FedRAMP Requirements and Guidance:

AC-5 Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP.

AC-05 Control Summary Information
Responsible Role: Customer Administrator, Program Manager
Parameter AC-05(a): Code check-in and deployment duties; production access and audit configuration duties; access requesting and access granting capabilities
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-05 What is the solution and how is it implemented?

Part a

Customer Responsibility

Government customers are responsible for separating duties of their organizational users as necessary, to prevent malevolent activity without collusion in compliance with their organizational policies.

Government customers will manage their user accounts in their existing Active Directory infrastructure. For information regarding how to manage user accounts in Active Directory, see the following link: <some_link>.

Non-government customers manage their user accounts in AAD via SUE. For more information on managing customer accounts via the SUE portal, see the following link: <some_link>.

Product1

Service teams define their roles in IDM. Each role contains a list of eligibilities. Eligibilities vary depending on the role that a specified service team personnel will assume within the service team. The separation of duties is documented through eligibilities (roles) assigned to service team administrators in IDM. Each service team identifies roles that, if shared by a single person, would allow for malicious activity without collusion. When such role pairs exist, no individual is allowed to belong to both roles. Account permissions and role access are reviewed as part of the monthly account review process.

Additionally, service team administrators are required to request privileged access to the production environment and provide a business justification using Torus and IDM. A different service team administrator with the access approver role then reviews and either approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, Torus and IDM assign the service team administrator the minimum permissions required to perform the work and automatically revoke permissions at the end of the specified time period.

Implementing access control using Torus and IDM effectively prevents malevolent activity without collusion, as an individual has to review and approve the requestor's access request and would deny requests that would violate separation of duties requirements.

The separation of duties is documented through eligibilities (roles) assigned to service team administrators in account management tools.
Part b Product1 The separation of duties is documented through eligibilities (roles) assigned to service team administrators in IdM. Each security group in IdM has access to a specific list of eligibilities that grants specific permissions to accomplish various tasks. In order for an admin to accomplish a task in production, they must request elevation to the eligibility with the proper permissions to accomplish that task. A list of these roles can be made available to the customer upon request.

AC-06 Least Privilege

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AC-06 Control Summary Information
Responsible Role: Customer Administrator, Program Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06 What is the solution and how is it implemented?

Customer Responsibility

Government customers are responsible for employing the concept of least privilege, allowing only authorized accesses for government customer users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions in compliance with their organizational policies.

Government customers will manage their user accounts in their existing Active Directory infrastructure. For information regarding how to manage user account permissions in Active Directory, see the following link: <some_link>.

Non-government customers will manage their user accounts in AAD via SUE. For more information on managing account permissions via the SUE portal, see the following link: <some_link>.

Product1

Product1 service teams employ the concept of least privilege, documented in IDM Roles and Eligibilities, allowing only authorized accesses for service team users (and processes acting on behalf of service team users) that are necessary to accomplish assigned tasks in accordance with business functions and organizational need.

Service owners must employ the concept of least privilege for specific duties and information systems in accordance with risk assessments as necessary to adequately mitigate risk to operational assets, individuals, and/or other organizations. Service team administrator permissions and segregation of duties are defined in AC-5. Each service team is responsible for defining least privileged roles within their team. Roles are documented within IDM.

Teams use Torus JIT and IDM, by default; service team accounts belong to a security group that only has remote metadata access to the environment for that service team. This does not permit direct environment access, or access to customer content. If a service team administrator needs other privileges to the production environment, they must request that access and provide a business justification using Torus and IDM. A service team administrator with the access approver role then reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, Torus and IDM assigns the service team administrator to security groups with the minimum permissions required to perform the work and automatically revokes permissions at the end of the specified time period.

The use of this Just-In-Time permissions model ensures that service team administrators only ever have the least privileges required to accomplish assigned tasks in support of Product1

mission and business functions, restricted by elevation level, resource access, and time.

AC-06(01) Authorize Access to Security Functions

Authorize access for [Assignment: organization-defined individuals or roles] to:

(a) [FedRAMP Assignment: all functions not publicly accessible]; and

(b) [FedRAMP Assignment: all security-relevant information not publicly available].

AC-06(01) Control Summary Information
Responsible Role: Customer Administrator, Program Manager, Service Engineer Operations
Parameter AC-06(01)-1: service team administrators (and processes acting on behalf of service team administrators)
Parameter AC-06(01)(a): All functions not publicly accessible
Parameter AC-06(01)(b): all security-relevant information not publicly available
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06(01) What is the solution and how is it implemented?
Part a Customer Responsibility Government customers are responsible for explicitly authorizing access to security functions,

as defined by their organization, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For information regarding how to manage user accounts in AD, see the following link: <some_link>.

Non-government customers can explicitly authorize access to security functions following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, the customer is responsible for authorizing access to "tenant administration" privileges which are used to manage user accounts and system configuration via the SUE portal.

For more information on managing account privileges via the SUE portal, see the following link: <some_link>.

Product1

Service teams employ the concept of least privilege, allowing only pre-authorized access for service team administrators (and processes acting on behalf of service team administrators) which are necessary to accomplish assigned tasks in accordance with business functions and organizational need. Service owners employ the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to operational assets, individuals, and/or other organizations.

All access to the Product1 system must be explicitly authorized, including the following security related functions: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and system and security administration. Role owners are responsible for reviewing and approving role assignments, and roles are tailored for different job functions such that personnel only have the minimum access required to perform their duties. For some teams, service team accounts by default belong to a security group that only has user-level operating system access to the production environment for that service team - this does not permit access to customer content. Access to any higher level of permissions must be requested through Torus and IDM and authorized by the on-call approver.

Through the use of this just in time model, Product1 explicitly authorizes access to security functions.

Part b

See part a.

AC-06(02) Non-privileged Access for Nonsecurity Functions

Require that users of system accounts (or roles) with access to [FedRAMP Assignment: all security functions] use non-privileged accounts or roles, when accessing nonsecurity functions.

AC-06(02) Additional FedRAMP Requirements and Guidance:

AC-6 (2) Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

AC-06(02) Control Summary Information
Responsible Role: Customer Administrator, Program Manager
Parameter AC-06(02): All security functions
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06(02) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for requiring that users of information system accounts/roles with access to government security functions or security-relevant information use non-privileged accounts/roles when accessing other system functions. Government

customers are also responsible for auditing any use of privileged accounts/roles for such functions, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users communicate identification/authentication and the associated permissions to AAD via certificate-based authentication.

For information regarding how to manage user accounts in Active Directory see the following link: <some_link>.

Non-government customers can require that non-government customer users of information system accounts/roles with access to security functions or security-relevant information use non-privileged accounts/roles when accessing other system functions. Non-government customers can also audit any use of privileged non-government customer accounts/roles for such functions following the same procedures outlined for government customers, or they can elect to manage non-government customer user accounts in AAD via SUE. For customers using AAD, the customer is responsible for authorizing access to "tenant administration" privileges which are used to manage user accounts and system configuration via the SUE portal. Customers can elect to create a separate, non-privileged account for their administrative personnel to access other functions of Product1 MT. AAD audits all actions taken by tenant administration accounts; audit logs are retained for 90 days.

For more information on managing customer account privileges via the SUE portal, see the following link: <some_link>.

Product1

Service teams require all individuals with administrative privileges to use their assigned accounts for performing business and security administrative functions in the production environment. Product1 requires that service team administrators of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions.

AC-06(03) Network Access to Privileged Commands

Authorize network access to [FedRAMP Assignment: all privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.

AC-06(03) Control Summary Information
Responsible Role: Customer Administrator, Program Manager
Parameter AC-06(03)-1: All privileged commands
Parameter AC-06(03)-2: Maintenance and operational needs

Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06(03) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for enforcing least privilege when authorizing network access to privileged commands. Product1 Product1 requires all individuals with administrative privileges to use their assigned accounts for performing business and security administrative functions in the production environment. These administrative functions are identified within IDM for each service team.

AC-06(05) Privileged Accounts

Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

AC-06(05) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Parameter AC-06(05): Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented

☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06(05) What is the solution and how is it implemented?
Customer Responsibility Customers are responsible for restricting privileged customer-controlled accounts. Product1 Product1 restricts privileged access to the system to the internal roles identified and approved in the account management tools.

AC-06(07) Review of User Privileges

(a) Review [FedRAMP Assignment: at a minimum, annually] the privileges assigned to [FedRAMP Assignment: all users with privileges] to validate the need for such privileges; and

(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-06(07) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Parameter AC-06(07)(a)-1: At a minimum, annually
Parameter AC-06(07)(a)-2: All users with privileges

Implementation Status (check all that apply):
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AC-06(07) What is the solution and how is it implemented?

Part a

Customer Responsibility

Government customers are responsible for reviewing user privileges.

Product1

Product1 reviews privileged accounts at least annually. Privileges are enforced by IDM and are reviewed by managers on a quarterly basis through assigned tasks in Product2 DevOps or the User Account Review (UAR) tool.

Part b

Customer Responsibility

Government customers are responsible for reassigning or removing privileges for customer-controlled accounts when appropriate.

Product1

Product1 follows the IDM workflows to disable the privileged account or revoke access when Product1 personnel no longer have need of the role to support their current work or if their

employment with Company is terminated.

AC-06(08) Privilege Levels for Code Execution

Prevent the following software from executing at higher privilege levels than users executing the software: [FedRAMP Assignment: any software except software explicitly documented].

AC-06(08) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Parameter AC-06(08): Any software except software explicitly documented
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06(08) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for enforcing software execution privileges on customer-deployed resources. Product1 Software execution at a higher privilege level than users executing the software is not applicable for servers and network devices. Product1 only permits administrator access to server who by default have code execution privileges. Tools are only accessible by Product1

administrators; therefore, no read only access is provided.

AC-06(09) Log Use of Privileged Functions

Log the execution of privileged functions.

AC-06(09) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06(09) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Product1 access. For these events, these customers are responsible for capturing what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Customers using Windows servers to support their infrastructure automatically meet this requirement as Windows captures these event details by default. For more information regarding Windows event logging, see: <some_link>. Product1 Product1 includes the execution of privileged functions in the list of events to be audited by

the system.

All commands run by all accounts are logged. Non-privileged actions (for example, browsing the public internet, use of email clients, etc.) are not allowed within the production environment. Additionally, some teams use just in time (JIT) tools to allow privileged access to be granted within the production environment. Execution of privileged functions using Torus and IDM is audited.

AC-06(10) Prohibit Non-privileged Users from Executing Privileged Functions

Prevent non-privileged users from executing privileged functions.

AC-06(10) Control Summary Information
Responsible Role: Product1 Security Manager, Product1 Trust Program Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-06(10) What is the solution and how is it implemented?
Product1 Product1 does not have non-privileged users on the system. Product1 prevents non-privileged users from accessing privileged functions. Customers do not have access to any functionality related to Product1 safeguards/countermeasures.

AT-02 Literacy Training and Awareness

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and [FedRAMP Assignment: at least annually] thereafter; and

2. When required by system changes or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];

c. Update literacy training and awareness content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

AT-02 Control Summary Information
Responsible Role: Customer Administrator, Product1 Trust Program Manager, Program Manager
Parameter AT-02(a)(1): At least annually
Parameter AT-02(a)(2): significant changes, new employee onboarding, or prior to accessing the system
Parameter AT-02(b): consistency, repetition
Parameter AT-02(c)-1: At least annually
Parameter AT-02(c)-2: security or privacy incidents
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)

☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

AT-02 What is the solution and how is it implemented?

Part a

Customer Responsibility

Government customers are responsible for providing security awareness training to their employees and vendors as necessary, including training on security awareness training and role-based training, as appropriate per job description. This training shall include requirements that customer users not bypass Product1 security through actions such as:

1. Improperly forwarding documentation through Exchange Online
2. Circumventing, disabling, or downgrading session-level encryption
3. Improperly securing documentation hosted in SharePoint Online

Product1

Part 1

Product1 provides security and privacy awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users. This is accomplished by requiring all staff to take a New Employee Orientation (NEO) security awareness training course, Standards of Business Conduct, within the first 30 days of their employment or transfer into the organization. This training course is facilitated by Core Services Engineering (CSE) and Corporate Security, and encompasses standard business security measures, basic information security, and user actions to maintain security and to respond to suspected security incidents.

In addition, all staff are required to take security and privacy awareness training annually after their initial training. Product1 has implemented the security training control by requiring all new users (employees and contractors) to take the initial security and privacy awareness training annually. Non-operational personnel, anyone that is involved in development and quality assurance, are also required to take the mandatory training. In addition, training related to the system being accessed, along with associated procedures, may be required. Security training is also required when there is a significant change to the system environment.

Part 2

Product1 provides security and privacy awareness training to all information system users (including managers, senior executives, and contractors) when required by system changes.

This is accomplished by requiring all staff to take a New Employee Orientation (NEO) security awareness training course, Standards of Business Conduct, within the first 30 days of their employment or transfer into the organization. This training course is facilitated by CSE and Corporate Security, and encompasses standard business security measures, information security, and user actions to maintain security and to respond to suspected security incidents.

In addition, all staff are required to take security and privacy awareness training annually after their initial training. Product1 has implemented the security training control by requiring all new users (employees and contractors) to take the initial security and privacy awareness training at least annually. Non-operational personnel, anyone that is involved in development and quality assurance, are also required to take the mandatory training. In addition, training related to the system being accessed, along with associated procedures, may be required. Security training is also required when there is a significant change to the system environment.

Part b

Product1 requires all information system users (including managers, senior executives, and contractors) to take Security and Privacy Foundations training as part of their initial training and annually thereafter. Consistent and repetitive training for all users helps to ensure that personnel understand privacy responsibilities and procedures.

Part c

Product1

Security Foundations Training trainings are updated on a regular basis to account for updates or changes that render previous training inaccurate. The trainings are sent to personnel through automated learning system communications. Training completions are documented and retained for investigation purposes. Additionally, service teams update training materials after security or privacy incidents.

Part d

Annual Security Foundations Training includes basic level training on how to detect, report and implement best practices to safeguard Company and its customers. Service teams incorporate lessons learned into training materials as part of their incident post-mortem process.

AT-02(02) Insider Threat

Provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-02(02) Control Summary Information
Responsible Role: Customer Administrator, Product1 Trust Program Manager, Program Manager
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AT-02(02) What is the solution and how is it implemented?
Customer Responsibility Government customers should provide security awareness training to their users that includes content related to recognizing and reporting potential indicators of insider threat. Product1 Product1 security and privacy awareness training includes content related to recognizing and reporting potential indicators of insider threat.

AT-02(03) Social Engineering and Mining

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

AT-02(03) Control Summary Information

Responsible Role: Customer Administrator, Product1 Trust Program Manager, Program Manager
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AT-02(03) What is the solution and how is it implemented?
Customer Responsibility Government customers should provide security awareness training to their users that includes content related to recognizing and reporting potential and actual instances of social engineering and social mining. Product1 Product1 security and privacy awareness training includes content related to recognizing and reporting potential and actual instances of social engineering and social mining.

AT-03 Role-based Training

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:

1. Before authorizing access to the system, information, or performing assigned duties, and [FedRAMP Assignment: at least annually] thereafter; and

2. When required by system changes;

b. Update role-based training content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

AT-03 Control Summary Information
Responsible Role: Customer Administrator, Product1 Trust Program Manager, Program Manager
Parameter AT-03(a): all personnel accessing the system
Parameter AT-03(a)(1): at least annually
Parameter AT-03(b)-1: at least annually
Parameter AT-03(b)-2: new employee onboarding, security or privacy incidents
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AT-03 What is the solution and how is it implemented?
Part a <u>Customer Responsibility</u> Government customers are responsible for providing role-based training to their employees and vendors as necessary, including training on basic security awareness training and role-based training, as appropriate per job description. This training shall include requirements that customer users not bypass Product1 security through actions such as:

1. Improperly forwarding documentation through Exchange Online
2. Circumventing, disabling, or downgrading session-level encryption.
3. Improperly securing documentation hosted in SharePoint Online

Product1

Part 1

Product1 provides role-based security-related training before authorizing access to the system or performing assigned duties, and at least annually thereafter.

Part 2

Product1 provides role-based security-related training before authorizing access to the system or when required by information system changes.

Part b

Customer Responsibility

Government customers are responsible for providing role-based security training to their employees and vendors as necessary (at least annually for government customers relying on FedRAMP certification).

Product1

Product1 service teams review and update role-based training content at least annually and throughout new employee onboarding. Additionally, service teams update training materials after security or privacy incidents.

Part c

Service teams incorporate lessons learned into training materials as part of their incident post-mortem process.

AT-04 Training Records

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [FedRAMP Assignment: five (5) years or 5 years after completion of a specific training program].

AT-04 Control Summary Information
Responsible Role: Product1 Trust Program Manager
Parameter AT-04(b): five (5) years or 5 years after completion of a specific training program
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AT-04 What is the solution and how is it implemented?
Part a Product1 Product1 utilizes corporate training tools to document and monitor security training. Corporate training tools provides a report, which tracks who has taken the basic security awareness and specific information system training. Each employee has access to their own account, which includes courses taken and elective courses that are suggested. A report can be generated from this tool to show what courses were taken by a specific employee.
Part b Product1 Product1 utilizes corporate training tools to retain employee training records for basic security

awareness and specific information system security training for at least 5 years.

CP-09 System Backup

a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [FedRAMP Assignment: daily incremental; weekly full];

b. Conduct backups of system-level information contained in the system [FedRAMP Assignment: daily incremental; weekly full];

c. Conduct backups of system documentation, including security- and privacy-related documentation [FedRAMP Assignment: daily incremental; weekly full]; and

d. Protect the confidentiality, integrity, and availability of backup information.

CP-09 Additional FedRAMP Requirements and Guidance:

CP-9 Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

CP-9 (a) Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative.

CP-9 (b) Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative.

CP-9 (c) Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative.

CP-09 Control Summary Information
Responsible Role: Product2, Customer Administrator, Service Engineer Operations
Parameter CP-09(a)-1: database
Parameter CP-09(a)-2: Daily incremental; weekly full
Parameter CP-09(b): Daily incremental; weekly full
Parameter CP-09(c): Daily incremental; weekly full

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☒ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☒ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

CP-09 What is the solution and how is it implemented?

Part a

Customer Responsibility

Exchange Online:

Exchange Online is a highly configurable service that allows organizations to control how long data is preserved and when it is deleted. By default, content deleted from Exchange can be restored for 14 days. With single item recovery and mailbox retention, customers can recover items in a mailbox upon inadvertent, malicious, or premature deletion.

• Customer Administrators are responsible for configuring retention polices to meet organizational requirements when Exchange Online defaults are not adequate.
• Customer Administrators are responsible for configuring retention policies consistent with recovery time objectives (RTO) and recovery point objectives (RPO).
• When required, Customer Administrators are responsible for increasing retention periods beyond default values.
• Customer Administrators are responsible for setting retention policy locks to make retention policy configurations immutable when required to meet recovery time and recovery point objectives.

For more information, see Exchange Online Data Resiliency - Company Service Assurance: <some_link>

SharePoint and OneDrive:

Versioning: SharePoint and OneDrive have built-in features that help protect customer information. SharePoint versioning retains a minimum of 500 versions of a file by default, files and can be configured to retain more versions if desired. The UI doesn't allow a value of fewer than 100 versions to be set, but it's possible to set the system to store fewer versions using public APIs. For reliability, any value less than 100 isn't recommended and can result in user activity causing inadvertent data loss. For more information about versioning, see Versioning in SharePoint (<some_link>).

Files Restore: is the ability to go 'back in time' on any Document Library in SharePoint to any second of time in the last 30 days. This process can be used to recover from ransomware, mass deletions, corruption, or any other event. This feature uses file versions so reducing default versions can reduce the effectiveness of this restore. For more information about the Files Restore feature see: <some_link>.

Preservation Hold Library: Files stored in SharePoint or OneDrive sites can be retained by applying retention policy settings. When a document with versioning is subject to retention settings, versions get copied to the Preservation Hold library and exist as a separate item. If a customer suspects their files have been compromised, they can investigate file changes by reviewing the retained copy. Customer Administrators are responsible for configuring retention policies when Preservation Hold Libraries are required.

Recycle Bin: Customers are responsible for restoring corrupted files. Customers have 93 days to restore deleted data from the recycle bin.

For more information, see SharePoint and OneDrive data resiliency in Company Product1 - Company: <some_link>

WProduct1:

Customers using WProduct1 are responsible for establishing a process for backing up their data in accordance with their organizational policies. Product1 has protections in place to preserve customer data in the event of data center failure, but customer-initiated modifications, including deletion, of data is not covered by Product1.

Product1

Company Product1 workloads, including SharePoint and Exchange, are built on resiliency principles, ensuring data replication across active/active data centers in near-real time. Data utilized for restoration activities leverage the same built-in data resiliency and integrity checks applied to live data. Within Company Product1 production environments, peer replication between Product2 datacenters ensures that there are always multiple live copies of data. Product1 services utilize versioning to ensure redundancy and accuracy of information. Standard images and scripts are used to recover lost servers, and replicated data is used to restore corrupted storage.

Only the following services store user-level information: CIA, EOP, EXO, Product3, SIP, ODSP, and IS. Services storing customer data will have separate instances specific to MT and GCC.

Exchange Online:

In Exchange Online, every mailbox is hosted in Database Availability Groups (DAGs) and replicated to geographically separate datacenters within the same region. Each mailbox database has four copies distributed across datacenters within the DAG: one active copy, two up-to-date copies, and one 7-day lagged copy used in the rare event of catastrophic logical corruption.

For more information, see Exchange Online Data Resiliency - Company Service Assurance: <some_link>

SharePoint and OneDrive Protection:

SharePoint and OneDrive Protection have built-in features that help protect customer information.

For SharePoint and OneDrive, files are written simultaneously to a primary and secondary datacenter region. Multiple types of checksums are stored within metadata in a separate location; corresponding files are used to ensure data integrity through all stages of the data lifecycle.

• File hash stored in metadata: Hash of the entire file is stored with file metadata to ensure document level data integrity is maintained during all operations
• Blob hash stored in metadata: Each blob-item stores a hash of the encrypted content to protect against corruption in underlying Product2 storage.
• Data integrity job: Every 14 days, each site is scanned for integrity by listing items in the database and matching those up with listed blobs in Product2 storage. The job reports any blob-references missing storage-blobs and can retrieve those blobs through the Product2 storage soft-delete feature if needed.

For more information, see SharePoint and OneDrive data resiliency in Company Product1 - Company: <some_link>

Product3:

Teams chats are stored within Exchange Online user mailboxes and files are stored in either SharePoint or OneDrive. Company Teams data is protected by the controls and recovery mechanisms available within these services.

For more information, see Service resilience in Company Teams - Company Service

Assurance: <some_link>

Product2-leveraged Services:

Product1 services leveraging Product2 storage solutions inherit backup capabilities from Product2. For user-level information in Product2 Storage, data is synchronously replicated locally using Locally Redundant Storage (LRS), which provides redundancy equivalent to three copies. In addition, data is asynchronously replicated to a separate datacenter in the zone or to a remote region for accounts which have configured Zone-Redundant Storage (ZRS), Geo-Redundant Storage (GRS), or Read-Access Geo-Redundant Storage (RA-GRS). The backups sent to Product2 Storage are encrypted using Federal Information Processing Standards (FIPS) 140-2 compliant AES 256-bit encryption.

For information on data integrity, refer to: <some_link>

Part b

Customer Responsibility

Customers are responsible for backing up system-level information relating to their use of WProduct1 Cloud PCs.

Product1

All system-level information required for service restoral is securely stored within CorpNet. This is achieved through internal code repository tools, namely Product2 DevOps and Source Depot. Product2 DevOps, which utilizes GIT, provides version control to support secure change management processes. For data integrity, Product2 Storage regularly monitors and verifies data stored using cyclic redundancy checks (CRCs). If data corruption is detected, it's repaired using redundant copies.

Product2 DevOps relies on both Product2 Blob Storage and Product2 SQL Database to help protect data during hardware or service failures. Product2 Storage geo-replicates data between two regions in the same geographical location. For Product2 Blob Storage, data is replicated three times within a single region. Data is replicated asynchronously to a second region in the same geographical location. As such, Product1 always maintains the equivalent of six copies of data.

The use of multiple copies enables failover to a separate region if there's a major outage or disaster, while also having local redundancy for hardware failures within the region. For Product2 SQL Database storage, daily backups are maintained offsite if there's a regional disaster.

To safeguard against accidental data loss, Company employs point-in-time backups for both blobs stored in Product2 Blob Storage and databases within Product2 SQL Database. Each

storage account maintains a separate copy of all blobs, with changes being appended to the existing data. These backups are immutable, eliminating the need to rewrite any existing storage during backup procedures.

Product2 SQL Database includes standard backup features, which are utilized by Product2 DevOps. Data is retained for 28 days, with these backups also being replicated in a paired region to facilitate recovery during a regional outage.

For more information, see: <some_link>.

Part c

Product1

All system documentation is securely stored within CorpNet. Use of Product2 IaaS/PaaS services is inherited from Product2.

Product1 maintains backups of system documentation, including security-related and privacy-related documentation, through SharePoint or within Product2 DevOps. SharePoint uses versioning and is replicated in near real-time.

SharePoint and OneDrive Protection:

SharePoint and OneDrive Protection have built-in features that help protect system documentation.

• Versioning: Retains a minimum of 500 versions of a file by default and can be configured to retain more, if system documentation is corrupted, a previous version of the file can be recovered.
• Files Restore: is the ability to go 'back in time' on any Document Library in SharePoint to any second of time in the last 30 days. This process can be used to recover from ransomware, mass deletions, corruption, or any other event. For more information about the Files Restore feature see: <some_link>.
• Recycle bin: If system documentation is inadvertently deleted, the recycle bin will store data for 93 days before permanent deletion. After the 93-day recycle pipeline is complete, deletion takes place independently for Metadata and for Blob Storage. Metadata is removed immediately from the database, which makes the content unreadable unless the metadata is restored from backup. SharePoint maintains 14 days-worth of backups of metadata. These backups are taken locally in near real time and then pushed to storage in redundant Product2 Storage containers on a 5-10-minute schedule.
• File hash stored in metadata: Hash of the entire file is stored with file metadata to ensure document level data integrity is maintained during all operations
• Blob hash stored in metadata: Each blob-item stores a hash of the encrypted content to protect against corruption in underlying Product2 storage.
• Data integrity job: Every 14 days, each site is scanned for integrity by listing items in the

database and matching those up with listed blobs in Product2 storage. The job reports any blob-references missing storage-blobs and can retrieve those blobs through the Product2 storage soft-delete feature if needed.

For more information, see SharePoint and OneDrive data resiliency in Company Product1 - Company: <some_link>

Product2 DevOps:

Use of Product2 DevOps is inherited from Product2. Product2 DevOps relies on both Product2 Blob Storage and Product2 SQL Database to help protect data during hardware or service failures. Product2 Storage geo-replicates data between two regions in the same geographical location. For Product2 Blob Storage, data is replicated three times within a single region. Data is replicated asynchronously to a second region in the same geographical location. As such, Product1 always maintains the equivalent of six copies of data.

The use of multiple copies enables fail over to a separate region if there's a major outage or disaster, while also having local redundancy for hardware failures within the region. For Product2 SQL Database storage, daily backups are maintained offsite if there's a regional disaster.

To safeguard against accidental data loss, Company employs point-in-time backups for both blobs stored in Product2 Blob Storage and databases within Product2 SQL Database. Each storage account maintains a separate copy of all blobs, with changes being appended to the existing data. These backups are immutable, eliminating the need to rewrite any existing storage during backup procedures.

Product2 SQL Database includes standard backup features, which are utilized by Product2 DevOps. Your data is retained for 28 days, with these backups also being replicated in a paired region to facilitate recovery during a regional outage.

For more information, see: <some_link>.

Part d

Customer Responsibility

WProduct1 customers are responsible for protecting the confidentiality, integrity, and availability (CIA) of customer-controlled backup data.

Product1

Product1 configures Product2 services appropriately to protect the confidentiality, integrity, and availability of backup or versioning data. Use of Product2 services inherited from Product2.

Product1 protects the confidentiality and integrity of all customer information through the use of Federal Information Processing Standards (FIPS) compliant TLS 1.2/1.3 protocols and AES 256-bit encryption. In instances where information is uploaded to Product2 Storage, data is automatically encrypted. As part of the drive to ensure that Company is only using cryptographically secure protocol versions, all teams within Product1 are provided guidance to deprecate older protocols and ciphers. Service Teams are only allowed to leverage TLS 1.2/1.3 and higher protocols for both incoming and outgoing connections. Product1 leverages Key Performance Indicator (KPI) alerting system to ensure service teams are only leveraging TLS 1.2/1.3 and higher protocols. The KPIs are alerted to Product1 service and leadership teams for actions.

For more information on Product2-leveraged infrastructure for integrity and availability of data, see Data redundancy - Product2 Storage: <some_link>

For more information on how Product1 protects the availability of customer data, see part a.

CP-09(01) Testing for Reliability and Integrity

Test backup information [FedRAMP Assignment: at least monthly] to verify media reliability and information integrity.

CP-09(01) Control Summary Information
Responsible Role: Customer Administrator, Product2, Service Engineer Operations
Parameter CP-09(01): At least monthly
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☒ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

CP-09(01) What is the solution and how is it implemented?

Customer Responsibility

Customers are responsible for utilizing features of Product1 to restore any data that has been lost or corrupted. Customers are also responsible for periodic testing and validation of recovery procedures.

Product1

Company Product1 workloads, including SharePoint and Exchange, are built on resiliency principles, ensuring data replication across active/active data centers in near-real time. Data utilized for restoration activities leverage the same built-in data resiliency and integrity checks applied to live data. Within Company Product1 production environments, peer replication between Product2 datacenters ensures that there are always multiple live copies of data. Standard images and scripts are used to recover lost servers, and replicated data is used to restore corrupted storage.

Exchange Online:

In Exchange Online, every mailbox is hosted in Database Availability Groups (DAGs) and replicated to geographically separate datacenters within the same region. Each mailbox database has four copies distributed across datacenters within the DAG: one active copy, two up-to-date copies, and one 7-day lagged copy used in the rare event of catastrophic logical corruption.

Log File Checks: All transaction log files generated by an Exchange database undergo several forms of consistency checks. When a log file is created, the first thing done is a bit pattern is written and then a series of log writes is performed. This structure enables Exchange Online to execute a series of checks (lost flush, CRC, and other checks) to validate each log file as it is written, and again as it's replicated.

Resilient File System: To help prevent corruption from occurring at the file system level, Exchange Online is being deployed on Resilient File System (ReFS) partitions to provide improved recovery capabilities. ReFS is a file system that is designed to be more resilient against data corruption thereby maximizing data availability and integrity. Specifically, ReFS brings improvements in the way that metadata is updated which offers better protection for data and reduces data corruption cases. It also uses checksums to verify the integrity of file data and metadata ensuring that data corruption is easily found and repaired.

For more information, see Exchange Online Data Resiliency - Company Service Assurance: <some_link>

SharePoint and OneDrive Protection:

SharePoint and OneDrive Protection have built-in features that help protect customer information.

For SharePoint and OneDrive, files are written simultaneously to a primary and secondary datacenter region. Multiple types of checksums are stored within metadata in a separate location; corresponding files are used to ensure data integrity through all stages of the data lifecycle.

• File hash stored in metadata: Hash of the entire file is stored with file metadata to ensure document level data integrity is maintained during all operations
• Blob hash stored in metadata: Each blob-item stores a hash of the encrypted content to protect against corruption in underlying Product2 storage.
• Data integrity job: Every 14 days, each site is scanned for integrity by listing items in the database and matching those up with listed blobs in Product2 storage. The job reports any blob-references missing storage-blobs and can retrieve those blobs through the Product2 storage soft-delete feature if needed.

For more information, see SharePoint and OneDrive data resiliency in Company Product1 - Company: <some_link>

Product3:

Teams chats are stored within Exchange Online user mailboxes and files are stored in either SharePoint or OneDrive. Company Teams data is protected by the controls and recovery mechanisms available within these services.

For more information, see Service resilience in Company Teams - Company Service Assurance: <some_link>

System Data & System Documentation:

Company ensures that backups of Company Product1 system documentation and system data needed for service restoration are securely kept within CorpNet. This is achieved through SharePoint's inherent data resilience capabilities and internal code repository tools, namely Product2 DevOps and Source Depot. For data integrity, Product2 Storage regularly monitors and verifies data stored using cyclic redundancy checks (CRCs). If data corruption is detected, it's repaired using redundant copies. Product2 Storage also calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. CRC checks are performed prior to replication of data as well as periodically - once a month for HDDs, twice a month for SSDs. CRC calculations are tested against values stored in metadata to ensure data integrity within Product2 storage.

For information on data integrity and Product2 DevOps refer to:
Data redundancy - Product2 Storage <some_link>

Data protection overview - Product2 DevOps Services <some_link>

For additional details on how Product2 further protects Product1 data within Product2 storage using data-at-rest protections, see Product2's SSP SC-28.

CP-09(02) Test Restoration Using Sampling

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

CP-09(02) Control Summary Information
Responsible Role: Product2, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

CP-09(02) What is the solution and how is it implemented?
Product1 User level information is stored in Product2 Storage. Product1 uses geo-replication to provide redundancy to alternate geographic locations. Data durability is obtained by synchronously replicating data across multiple databases in different datacenters. Restoration tests are performed for all backup data owned by Product1. The use of Product2 Storage is inherited from Product2.

CP-09(03) Separate Storage for Critical Information

Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.

CP-09(03) Control Summary Information
Responsible Role: Service Engineer Operations
Parameter CP-09(03): Critical information system software and other security-related information including source code, builds, customer content, and access control data.
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

CP-09(03) What is the solution and how is it implemented?
Product1 Product1 has defined critical information system software and other security-related information as source code, builds, customer content, and access control data. This critical functionality and data is replicated and stored across at least two data centers.

IA-02 Identification and Authentication (organizational Users)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

IA-02 Additional FedRAMP Requirements and Guidance:

IA-2 Requirement: For all control enhancements that specify multifactor authentication, the implementation must adhere to the Digital Identity Guidelines specified in NIST Special Publication 800-63B.

IA-2 Requirement: Multi-factor authentication must be phishing-resistant.

IA-2 Requirement: All uses of encrypted virtual private networks must meet all applicable Federal requirements and architecture, dataflow, and security and privacy controls must be documented, assessed, and authorized to operate.

IA-2 Guidance: “Phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

IA-02 Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-02 What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for uniquely identifying and authenticating their organizational users via their Active Directory infrastructure. When a user of an organization attempts to access Product1, the user is redirected to a login page. The user provides their credentials and a login request is created backed by a X.509 certificate and authenticated by AAD. Customers are responsible for enforcing organizationally appropriate identification and authentication requirements including the use of unique identifiers.

For more information on Active Directory object naming, see: <some_link>.

Non-government customers inherit these controls from AAD. When users enter their username at the Product1 MT hosted login screen, AAD matches the user's domain to the appropriate Active Directory Organizational Unit and attempts to establish a secure session with the user's client. Once the session is established, AAD validates the user's authenticators and issues the user a SAML ticket containing information about the user's unique identity and group membership. Customer administrators use the SUE administration portal to set identification and authentication requirements for their organization. AAD enforces unique identifiers for these customers.

For more information on Active Directory object naming, see: <some_link>.

Product1

Product1 uses Product2 Active Directory (AAD) for identifying, Torus for authenticating access for Company users in the environment. Product1 personnel accessing Product1 are uniquely identified by their AD or AAD username and authenticate using FIPS 140-2 Validated YubiKey 5 (#3914) and FIPS 140-2 Compliant YubiKey 4 (#3517) or approved FIPS 140-2 compliant TPM modules. AD strictly enforces unique identifiers.

For more information on Active Directory object naming, see: <some_link>.

IA-02(01) Multi-factor Authentication to Privileged Accounts

Implement multi-factor authentication for access to privileged accounts.

IA-02(01) Additional FedRAMP Requirements and Guidance:

IA-2 (1) Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

IA-2 (1) Requirement: Multi-factor authentication must be phishing-resistant.

IA-2 (1) Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

IA-02(01) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned

☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

IA-02(01) What is the solution and how is it implemented?

Customer Responsibility

Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Product1. Product1 requires customers to implement certificate-based authentication to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements.

For more information about certificate-based authentication, see: <some_link>.

Non-government customers may not be required to implement multifactor authentication. Non-government customers may implement multifactor authentication following the same procedures outlined for government customers (above) or they may elect to allow access using single factor authentication. Customers are responsible for determining the access requirements appropriate for the risk tolerances of their system and information.

Guest access to Product3 meetings, if enabled, is via single factor authentication. Government customers are responsible for determining if the use of guest access to Product3 sessions should be allowed for their organization. This setting can be configured by government customers.

Guest access to SharePoint Online, if enabled, is via single factor authentication. Government customers are responsible for determining if the use of guest access to SharePoint Online should be allowed for their organization. This setting can be configured by government customers.

For more information, see the following Product1 help article: <some_link>.

Product1

Product1 implements multifactor authentication for network access by Product1 personnel using FIPS 140-2 Validated YubiKey 5 (#3914) and FIPS 140-2 Compliant YubiKey 4 (#3517) and approved FIPS 140-2 compliant TPM modules. All Company users connect to the system via TSG or Product2 managed Terminal Services Gateways (TSGs) as described in AC-17; the TSGs require the user to present a certificate bound to the card (something you have) with a PIN (something you know).

IA-02(02) Multi-factor Authentication to Non-privileged Accounts

Implement multi-factor authentication for access to non-privileged accounts.

IA-02(02) Additional FedRAMP Requirements and Guidance:

IA-2 (2) Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

IA-2 (2) Requirement: Multi-factor authentication must be phishing-resistant.

IA-2 (2) Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

IA-02(02) Control Summary Information
Responsible Role: Customer Administrator, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-02(02) What is the solution and how is it implemented?

Customer Responsibility

Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Product1. Product1 requires customers to implement certificate-based authentication to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements.

For more information about certificate-based authentication, see: <some_link>.

Non-government customers may not be required to implement multifactor authentication. Non-government customers may implement multifactor authentication following the same procedures outlined for government customers (above) or they may elect to allow access using single factor authentication. Customers are responsible for determining the access requirements appropriate for the risk tolerances of their system and information.

Guest access to Product3 meetings, if enabled, is via single factor authentication. Government customers are responsible for determining if the use of guest access to Product3 sessions should be allowed for their organization. This setting can be configured by government customers.

Guest access to SharePoint Online, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online should be allowed for their organization. This setting can be configured by government and non-government customers.

For more information, see the following Product1 help article: <some_link>.

Product1

All Product1 accounts used by Product1 personnel are considered privileged. Multifactor authentication is implemented for all Product1 accounts.

IA-02(05) Individual Authentication with Group Authentication

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

IA-02(05) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager
Implementation Status (check all that apply): ☒ Implemented

☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

IA-02(05) What is the solution and how is it implemented?

Customer Responsibility

Government customers are responsible for uniquely identifying individuals using group authenticators.

Product1

Product1 does not use shared accounts. Individual service engineers are assigned into a security group, and in order to use these credentials, a user must go through multifactor authentication to uniquely identify their credentials.

IA-02(06) Access to Accounts —separate Device

Implement multi-factor authentication for [FedRAMP Assignment: local, network and remote] access to [FedRAMP Assignment: privileged accounts; non-privileged accounts] such that:

(a) One of the factors is provided by a device separate from the system gaining access; and

(b) The device meets [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography].

IA-02(06) Additional FedRAMP Requirements and Guidance:

IA-2 (6) Guidance: PIV=separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials.

IA-2 (6) Guidance: See SC-13 Guidance for more information on FIPS-validated or NSA-approved cryptography.

IA-02(06) Control Summary Information
Responsible Role: Customer Administrator, Product2, Product1 Security Manager, Service Engineer Operations
Parameter IA-02(06)-1: local, network and remote
Parameter IA-02(06)-2: privileged accounts; non-privileged accounts
Parameter IA-02(06)(b): FIPS-validated or NSA-approved cryptography
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-02(06) What is the solution and how is it implemented?
Part a Customer Responsibility Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Product1. Product1 requires customers to implement certificate-based authentication to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements. For more information about certificate-based authentication, see: <some_link>. Non-government customers may not be required to implement multifactor authentication. Non-government customers may implement multifactor authentication following the same procedures outlined for government customers (above) or they may elect to allow access using single factor authentication. Customers are responsible for determining the access

requirements appropriate for the risk tolerances of their system and information.

Guest access to Product3 meetings, if enabled, is via single factor authentication. Government customers are responsible for determining if the use of guest access to Product3 sessions should be allowed for their organization. This setting can be configured by government customers.

Guest access to SharePoint Online, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online should be allowed for their organization. This setting can be configured by government and non-government customers.

For more information, see the following article: <some_link>.

Product1

Product1 uses multifactor authentication for network and remote access by Product1 personnel using FIPS 140-2 Validated YubiKey 5 (#3914) and FIPS 140-2 Compliant YubiKey 4 (#3517) and approved FIPS 140-2 compliant TPM modules. Company uses Thales IDPrime930 cards and the IDEMIA ID-One PIV cards as its smart card models. Product1 issues FIPS 140-2 validated components that have an active status per the Cryptographic Module Validation Program.

For more information, see: <some_link>

All Company users connect to the system via TSG or Product2 managed Terminal Services Gateways (TSGs) or admin consoles as described in AC-17; the TSGs or admin consoles require the user to present a certificate bound to the card or TPM module (something you have) with a PIN (something you know).

There is no local access to the Product1 environment. Product1 personnel do not have physical access to Product1 servers, and Product2 personnel do not have logical access to Product1 servers. Local access that may require authentication in other environments usually results in replacement of hardware in the Product1 environment.

Product1 does not allow non-privileged users to access the system. Product1 prevents non-privileged users from accessing privileged functions through RBAC and the requirement of two-factor authentication.

Part b

See part a.

IA-02(08) Access to Accounts — Replay Resistant

Implement replay-resistant authentication mechanisms for access to [FedRAMP Assignment: privileged accounts; non-privileged accounts].

IA-02(08) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Service Engineer Operations
Parameter IA-02(08): privileged accounts; non-privileged accounts
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

IA-02(08) What is the solution and how is it implemented?
Customer Responsibility Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Product1. Product1 requires customers to implement certificate-based authentication to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements. For more information about certificate-based authentication, see: <some_link>. Non-government customers authenticate directly to Product2 Active Directory (AAD). AAD is responsible for implementing replay-resistant authentication mechanisms for these customers.

Product1

Product1 uses multifactor authentication for network access to privileged accounts by Product1 personnel using FIPS 140-2 Validated YubiKey 5 (#3914) and FIPS 140-2 Compliant YubiKey 4 (#3517) and approved FIPS 140-2 compliant TPM modules. All Company users connect to the system via TSGs or Admin consoles as described in AC-17; the TSG or Product2 managed Terminal Services Gateways (TSGs) and Admin consoles require the user to present a certificate bound to the card (something you have) with a PIN (something you know).

Access to the Product1 production environment using the YubiKey/TPM module solution is protected from replay attacks by the built-in Kerberos functionality of Active Directory (AD). In Kerberos authentication the "authenticator" sent by the client contains additional data, such as an encrypted IP list, the client's timestamp, and the ticket lifetime. If a packet is replayed, the timestamp is checked. If the timestamp is earlier than or the same as a previous authenticator, the packet is rejected.

For more information on Active Directory and Kerberos, see: <some_link>.

Product1 does not allow non-privileged users to access the system. Product1 prevents non-privileged users from accessing privileged functions through RBAC and the requirement of two-factor authentication.

IA-02(12) Acceptance of PIV Credentials

Accept and electronically verify Personal Identity Verification-compliant credentials.

IA-02(12) Additional FedRAMP Requirements and Guidance:

IA-2 (12) Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

IA-02(12) Control Summary Information
Responsible Role: Customer Administrator
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate

☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☒ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

IA-02(12) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for accepting and electronically verifying Personal Identity Verification (PIV) credentials for government customer users and to implement certificate-based authentication for access to Product1. For more information about certificate-based authentication, see: <some_link>. Product1 Product1 does not utilize Personal Identity Verification (PIV) credentials for service team administrators. PIV cards are not available to Product1 service team personnel. As such this control is not applicable to Product1 service team personnel.

IA-03 Device Identification and Authentication

Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

IA-03 Control Summary Information
Responsible Role: Customer Administrator, Service Engineer Operations
Parameter IA-03-1: All devices within the information system accreditation boundary
Parameter IA-03-2: Network
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

IA-03 What is the solution and how is it implemented?

Customer Responsibility

Government Customers are required to ensure their information systems uniquely identify and authenticate approved device types prior to establishing a connection with Product1.

Non-Government Customers may not be required to provide a list of approved devices prior to establishing a connection with Product1 MT. Non-Government customers should implement industry best practices to determine connection requirements appropriate for the risk tolerances of their system and information.

Product1

Product1 uses Active Directory (AD) to uniquely identify and authenticate all devices within the Product1 boundary before establishing a network connection. All Product1 physical servers are joined to an AD domain when deployed. Active Directory Forest members are uniquely identified by Universally Unique Identifiers (UUIDs) with device authentication performed using Kerberos, which is a part of the Windows networking protocols.

Virtual machines are identified by the virtual machine deployment ID assigned by Product2 and authenticated via TSL certificates managed as part of the Product2 provisioning process. When establishing a Company Product2 subscription, a subscription ID is created. The Fabric Controller (FC), which manages all VMs in Company Product2, uses this subscription ID to tie VMs to particular subscriptions. For more information about the Fabric Controller see the Product2 SSP.

For teams managed by PilotFish, an identity certificate is distributed to every machine on a PilotFish cluster. Each identity certificate contains a unique identifier (machine name), the environment, and machine function (server role).

IA-07 Cryptographic Module Authentication

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

IA-07 Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-07 What is the solution and how is it implemented?
Customer Responsibility Government customers do not have access to request cryptographic certificates from Product1. If they require cryptographic certificates, they must follow their organizational procedures to procure certificates from a valid certificate authority. Product1 Product1 implements FIPS 140-2 encryption mechanisms on all communications between partners and between customers using cryptographic certificates issued by CertDojo which are anchored to the Company Root Certificate Authority. In this implementation, the Company Root Certificate Authority is the cryptographic module for Product1. In order to request a cryptographic certificate, an Product1 service team administrator must be authenticated to the MSIT managed corporate network. The Product1 service team administrator navigates to the internal Company site <http://ssladmin> to request a certificate. The request is routed to the administrator's manager for approval. Once the certificate is issued, the administrator uses

two factor authentication to access Product1 servers to install the certificate. This process meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

IA-08 Identification and Authentication (non-organizational Users)

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

IA-08 Control Summary Information
Responsible Role: Customer Administrator
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☒ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-08 What is the solution and how is it implemented?
Customer Responsibility Product1 government customers are responsible for determining users who have access to their information system. Thus, the responsibility is incumbent upon the customer to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users) who should have system access. The government customer can invite guests and non-organizational users to SPO, Product3, but the guest must be authorized/admitted to the session by the credentialed government customer user for Product3. It is the responsibility of the government customer to follow their

own Rules of Behavior and policies around inviting guests to their systems.

Product1

Product1 does not allow any non-organizational users to authenticate to production systems. Government customer users are considered organizational and are covered via IA-2.

If government customers decide to allow access to non-organizational users (or processes acting on behalf of a non-organizational user), they must ensure that such users or processes are uniquely identified and authenticated using credentials that meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational requirements.

IA-08(01) Acceptance of PIV Credentials from Other Agencies

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

IA-08(01) Control Summary Information
Responsible Role: Customer Administrator
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-08(01) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for accepting and electronically verifying Personal

Identity Verification (PIV) credentials. When enabled, certificate-based authentication allows customers authenticating with PIV credentials access to the environment.

Product1

Product1 does not utilize Personal Identity Verification (PIV) credentials for service team administrators. PIV cards are not available to Product1 service team personnel. Government customers are permitted to configure certificate-based authentication and are therefore responsible for implementing authentication access control systems that accept and electronically verify PIV credentials issued to other federal agencies as noted in Customer Responsibility.

Customers can authenticate using X.509 certificates on their smart cards directly against Product2 AD. There is no special configuration needed on the Windows clients to accept the smart card authentication. For more information, see: <some_link>.

IA-08(02) Acceptance of External Authenticators

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

IA-08(02) Control Summary Information
Responsible Role: Customer Administrator
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☒ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-08(02) What is the solution and how is it implemented?

Part a

Customer Responsibility

Government customers are responsible for accepting and electronically verifying FICAM-approved third-party credentials. Government customers are permitted to configure certificate-based authentication and are therefore responsible for implementing authentication mechanisms that accept only FICAM-approved third-party credentials. Government customers accessing Product1 utilize or support FICAM-approved third-party credentials for their service team users.

Government customers are permitted to configure certificate-based authentication and are therefore responsible for employing only FICAM-approved information system components to accept third-party credentials.

Product1

Product1 MT does not accept or process any government customer credentials.Product1 does not utilize or support FICAM-approved third-party credentials for service team users. Product1 supports customers accepting FICAM-approved third-party credentials for customer resources. Customers are responsible for only accepting FICAM-approved third-party credentials for customer resources. If government customers decide to allow access to non-organizational users, they must authenticate using FICAM-approved third-party credentials. Government customers are responsible for ensuring that approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational requirements as noted in the Customer Responsibility.

Customers are responsible for only accepting FICAM-approved third-party credentials for customer resources. Product1 does not utilize or support FICAM-approved third-party credentials for service team administrators. If government customers decide to allow access to non-organizational users, they must accept only FICAM-approved third-party credentials using FICAM-approved information system components. Government customers are permitted to configure certificate-based authentication and are therefore responsible for ensuring that approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational requirements as noted in Customer Responsibility.

Product1 does not implement PIV requirements. Certificate-based authentication is required for Government customers using PIV.

Part b

Customer Responsibility

Government customers are responsible for accepting and electronically verifying FICAM-approved third-party credentials. Customers must document and maintain a list of accepted external authenticators.

Product1

See part a.

IA-08(04) Use of Defined Profiles

Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].

IA-08(04) Control Summary Information
Responsible Role: Customer Administrator
Parameter IA-08(04): FICAM-issued profiles
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☒ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

IA-08(04) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for conforming to FICAM-issued profiles. Government customers are permitted to configure certificate-based authentication and are therefore responsible for employing only FICAM-issued profiles.

Product1

Product1 supports customer use of FICAM-issued profiles. Customers are responsible for only accepting FICAM-approved third-party credentials for customer resources. Product1 does not utilize or support FICAM-approved third-party credentials for service team administrators. If government customers decide to allow access to non-organizational users, they must accept only FICAM-approved third-party credentials using FICAM-issued implementation profiles of approved authentication protocols as noted in Customer Responsibility.

System and Information Integrity

SI-01 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SI-01 Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Service Engineer Operations

Parameter SI-01(a): Service Engineer Operations, Program Manager, Developer, Tester, Product1 Trust Program Manager, Product1 Security Manager, BCM
Parameter SI-01(a)(1): organization-level
Parameter SI-01(b): Appropriate service team personnel, security engineering teams, service provider personnel with authority on system and information integrity policies
Parameter SI-01(c)(1)-1: at least annually
Parameter SI-01(c)(1)-2: significant changes
Parameter SI-01(c)(2)-1: at least annually
Parameter SI-01(c)(2)-2: significant changes
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

SI-01 What is the solution and how is it implemented?
Part a Product1 **Part 1** The Product1 Information Security Policy provides the overarching security guidance for Product1. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Company organizations providing some level of support for the security of Product1. Product1 SOPs and policies are distributed to roles providing support for system and information integrity via SharePoint.

Part 2

Standards and procedures to facilitate execution of these policies are documented in the Product1 SOPs and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Product1 SOPs to each control is compiled.

part b

Customer Responsibility

Government customers are responsible for designating an organization-defined official to manage the development, documentation, and dissemination of their organization's system and information integrity policy and procedures.

Product1

The "Product1 Information Security Policy" provides the overarching security guidance for Product1. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Company organizations providing some level of support for the security of Product1. Policies are distributed to personnel responsible for implementing system and information integrity policies and procedures via SharePoint.

The "Product1 Information Security Policy" is reviewed and updated annually.

Part c

Product1

Part 1

The Product1 Information Security Policy is reviewed and updated at least annually.

Part 2

The Product1 SOPs are reviewed and updated at least annually or whenever a significant change occurs.

SI-02 Flaw Remediation

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [FedRAMP Assignment: within thirty (30) days of release of updates] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

SI-02 Control Summary Information
Responsible Role: Customer Administrator, Product2, Product1 Security Manager, Service Engineer Operations
Parameter SI-02(c): within thirty (30) days of release of updates
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

SI-02 What is the solution and how is it implemented?
Part a <u>Customer Responsibility</u> Government customers are responsible for ensuring that customer users are using secure browsers and properly patched information systems to access Product1.

WProduct1: Government customers utilizing WProduct1 services are responsible for identifying, reporting, and correcting information system flaws on their own VMs.

Product1

Product1 identifies, reports, and corrects information system flaws through vulnerability management, incident response management, and patch/configuration management processes. The Product1 Security Incident Response Program assists with identifying and reporting of information system flaws. Product1 receives vulnerability-related data from multiple sources of information which include: Company Security Resource Center (MSRC), vendor Web sites, other third-party services (e.g. Internet Security Systems) and internal/external vulnerability scanning of services. Product1 Security will determine which updates are applicable within the Product1 environment. Potential changes are tested in advance. Patching schedules are defined by Product1 Security to install security-relevant software and firmware updates within 30 days for high vulnerabilities, 90 days for moderate vulnerabilities.

Additionally, the Product1 TVR team and Product2 analyze and test vendor-supplied software (Qualys scan engine). Flaws found during testing are reported to the appropriate vendor, and vendor patches are tested and applied as they are received.

Product1 inherits firmware changes from Product2, which is responsible for firmware updates to the Product1 infrastructure. Services with inherited compute also inherit this control from Product2. Product2.
For containers, when patches are available, a new container image is pulled from Company Container Registry (MCR) and prepped for use. A new build is also created when components added to the MCR container image need to be patched.

Part b

Product1

Product1 service teams test potential software changes prior to deployment, either in a separate test environment, or by removing a server from production, making changes, testing, and returning it to production upon successful completion.

Product1 inherits the testing of firmware from Product2, which is responsible for the testing of firmware prior to deployment into the Product1 infrastructure. Services with inherited compute also inherit this control from Product2. Product2.

Part c

Product1

As described in part a of this control, Product1 installs security-relevant software updates within 30 days for updates associated with high risk vulnerabilities, 90 days for updates associated with medium/moderate.

Product1 inherits the installation of firmware from Product2, which is responsible for the installation of firmware into the Product1 infrastructure. Services with inherited compute also inherit this control from Product2. Product2.

For teams using PilotFish, firmware and software updates are managed by PilotFish. All PilotFish machines are required to receive security updates within 30 days of release and must apply OS upgrades once a month.

Part d

Product1

The flaw remediation process follows the standard configuration management process, which includes testing, reviews, flaw remediation, and approvals of changes before they are installed in the production environment. The configuration management process is documented in the CM family of controls.

SI-02(02) Automated Flaw Remediation Status

Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [FedRAMP Assignment: at least monthly].

SI-02(02) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager
Parameter SI-02(02)-1: scanners
Parameter SI-02(02)-2: At least monthly
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate

☐ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

SI-02(02) What is the solution and how is it implemented?
Customer Responsibility Government customers are required to employ automated mechanisms to determine the state of information system components with regard to flaw remediation on their information systems as required by their organization's security policy. Non-Government customers of Product1 MT inherit automated protection mechanisms from Company within the environment. Non-Government customers are responsible for client-side network scans on all their endpoints in accordance with their security policy. Product1 Product1 utilizes Qualys for vulnerability management. This tool performs periodic and on-demand scanning against the environment and determine the state of information system components with regard to flaw remediation. Qualys uses the patch and vulnerability information from industry sources to scan the Product1 environment. These scans are configured to run at least monthly.

SI-02(03) Time to Remediate Flaws and Benchmarks for Corrective Actions

(a) Measure the time between flaw identification and flaw remediation; and

(b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].

SI-02(03) Control Summary Information
Responsible Role: Product1 Security Manager, Product1 Trust Program Manager
Parameter SI-02(03)(b): Thirty (30) days for high risk flaws, ninety (90) days for moderate risk flaws
Implementation Status (check all that apply): ☒ Implemented

☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☒ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing authorization

SI-02(03) What is the solution and how is it implemented?

Part a

Product1

As part of the Product1 TVR process, the scanners produce timestamps which are kept for initial flaw detections and remediation and are used to calculate the time elapsed between the two.

Part b

Product1

Product1 uses the TVR process to continuously track and correct information system flaws as detailed in RA-5. The benchmarks are to remediate high risk flaws within 30 days of discovery, moderate risk flaws within 90 days of discovery and low risks flaws within 180 days of discovery.

SI-03 Malicious Code Protection

a. Implement [FedRAMP Assignment: signature based and non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints and network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [FedRAMP Assignment: to include blocking and quarantining malicious code]; and send alert to [FedRAMP Assignment: administrator or defined security personnel near-realtime] in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-03 Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Service Engineer Operations
Parameter SI-03(a): signature based and non-signature based
Parameter SI-03(c)(1)-1: At least weekly
Parameter SI-03(c)(1)-2: To include endpoints and network entry and exit points
Parameter SI-03(c)(2)-1: to include blocking and quarantining malicious code;
Parameter SI-03(c)(2)-2: administrator or defined security personnel near-real time
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

SI-03 What is the solution and how is it implemented?

Part a

Customer Responsibility

Government customers are responsible for ensuring that customer users are using information systems running anti-malware software to access Product1.

Product1

The use of anti-malware software is a principal mechanism for protection of Product1 assets from malicious software. The software detects and prevents the introduction of computer viruses, malware, rootkits, worms, and other malicious software onto the service systems. Anti-malware software provides both preventive and detective control over malicious software. System Center Endpoint Protection (SCEP), Windows Defender, Forefront Endpoint Protection (FEP) or Company Endpoint Protection (MEP) is installed as part of the initial build on all systems.

Additionally, IP scans and quarantines in real time all email and email attachments both entering and leaving the system for viruses and other malware.

Part b

Product1

Each anti-malware package tracks the version of the software and what signatures are running. The automatic download and application of signature updates when available from the vendor's virus definition site is centrally managed by the appropriate anti-malware tool for each service team in accordance with the team's defined change management processes. EXO applies Safe Deployment Practices (SDP) to Defender signatures after a malformed signature update caused a high severity incident. Signature updates follow a ringed deployment on a weekly cadence, but the SDP process introduces a slight delay in these signatures reaching the production environment. Testing signature updates in preproduction environments help ensure stability of the information system, but also contributes to a signature update interval of approximately 15 days.

Part c

Product1

Part 1

CIA, CII , Delve, EXO, Falcon, IP, IS, TSG, OSI, Profile Card, SCS, SPO, SUE, WProduct1:

The following functions are centrally managed by the appropriate anti-malware tool on each endpoint for each service team:

• Periodic scans of the file system (at least weekly)
• Real-time scans of files as they are downloaded, opened, or executed

Anti-malware tools detect files determined to be malicious and send alerts to Product1 administrators, which triggers the incident response process.

PDRS, Product3, ObjectStore, Product4 for Web:

PilotFish utilizes real-time scanning of files as they are downloaded, opened, or executed. If the scanning tool is disabled, a Sev 1 alert is generated.
PilotFish also monitors for changes to its desired state; deviations from this state will automatically mark the host as unhealthy, remove it from the network, and subsequently tear it down and rebuild.
Anti-malware tools detect files determined to be malicious and send alerts to Product1 administrators, which triggers the incident response process.

Part 2

When anti-malware tools detect malware in a real-time scan, they block it and an alert is generated and sent to Product1 service team personnel, Product1 Security, and/or Product2 OSSC. When anti-malware tools detect malware in a periodic scan, the malware is quarantined. The receiving personnel initiate the Incident Response process. Incidents are tracked and resolved, and postmortem analysis is performed, as discussed in the Product1 Security Incident Response Plan.

Acceptable output from MpPreference includes a setting of '0' or '2,' both of which will quarantine detected threats and initiate the Incident Response process.

Part d

Product1

When anti-malware tools detect malware, they block the malware and an alert is generated and sent to Product1 service team personnel, Product1 Security, and/or Product2. The receiving personnel initiate the Incident Response process. Incidents are tracked and resolved, and postmortem analysis is performed, as discussed in the Product1 Security Incident Response Plan.

SI-04 System Monitoring

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and

2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SI-04 Additional FedRAMP Requirements and Guidance:

SI-4 Guidance: See US-CERT Incident Response Reporting Guidelines.

SI-04 Control Summary Information
Responsible Role: Product2, Product1 Security Manager, Service Engineer Operations
Parameter SI-04(a)(1): Ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise; monitoring objectives as described in system specific SCOM packs
Parameter SI-04(b): Near Real Time Security Monitoring (NRT), automated security alerting tools and repository service
Parameter SI-04(g)-1: Monitoring for information specified by Product1 Security Team
Parameter SI-04(g)-2: Product1 Security Manager

Parameter SI-04(g)-3: Daily and as needed
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☒ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

SI-04 What is the solution and how is it implemented?
Part a Product1 **Part 1** Service teams have deployed Near Real Time monitoring solutions that generate all real-time alerts and audit logs from both SCOM and the repository. All the service team-specific monitoring requirements beyond the base set defined in Product1 Security Auditing SOP for Product1 are integrated into a SCOM pack. In addition, service teams upload their logs to a repository service, where they are aggregated and processed. The uploader service generates reports using automated security alerting tools. These automated security alerting tools assist in identifying normal usage of the system and deviations from that normal range. Additionally, they examine records to confirm that the system is functioning in an optimal, resilient, and secure state. Unusual activity is flagged and alerted in Near Real Time. The repository also aggregates logs for further review. Any log event that indicates a potential security violation must be immediately brought to the attention of Product1 Security. Teams using PilotFish use K9, a tool that collects security logs and performs real-time analysis, as well as archiving them to a repository service for forensic analysis. Unusual activity will generate alerts and the PilotFish team coordinates with the appropriate service team for any required follow-ups or investigations. Service teams will work with the Product1 SIR team to address all security incidents.

Part 2

Local connections are disallowed by policy within Product4. No personnel have local access. Product2 performs network monitoring and detection of unauthorized connections in accordance with their security policy. Monitoring is also inherited for services using inherited compute from Product2. Remote authentication failures are logged and stored within a repository service. For further information, please see AC-17 and AC-7.

Part b

Product1

Audit logs are uploaded to repository and reports are generated using automated security alerting tools. These automated security alerting tools assist in identifying normal usage of the system and deviations from that normal range. The automated security alerting tools use heuristics to identify unauthorized use of the operating system. Unusual activity is flagged and alerted in near real time and a repository aggregates logs for further review. Any log event that indicates a potential security violation must be immediately brought to the attention of Product1 Security.

For services using inherited compute via Product2, this control is inherited from Product2.

For teams using PilotFish, audit logs are uploaded to a repository service and reports are generated using PilotFish/K-9. PilotFish/K-9 assists in identifying normal usage of the system and deviations from that normal range. PilotFish/K-9 uses heuristics to identify unauthorized use of the operating system. Unusual activity is flagged for further review. Any log event that indicates a potential security violation must be immediately brought to the attention of Product1 Security.

Part c

Product1

Part 1

All servers act as monitoring devices and are configured to log all security-relevant events. Product1 monitors and alerts in Near Real Time for all hosts in the environment. Suspicious events generate alarms and notifications to service team staff and appropriate contingent staff. Logs are aggregated in a repository service and reports are generated using the automated security alerting tools.

For teams using PilotFish, all servers act as monitoring devices and are configured to log all security-relevant events. Product1 monitors all hosts in the environment. Suspicious events

generate alarms and notifications to service team staff and appropriate contingent staff. Logs are aggregated in a repository service and reports are generated using PilotFish/K-9.

Part 2

All servers are configured to log all exceptions and security-relevant events. Additionally, Product1 monitors all devices and has those logs exported to a centralized system for aggregated alerting/monitoring. Therefore, Product1 has determined that there is no need for ad-hoc deployment of monitoring devices as documented in "Ad-hoc Monitoring Devices Decision Log (SI-4)".

Part d

Product1

Audit logs are uploaded to a repository service from all servers in the Product1 environment. Each service team receives near real-time alerting on security events through various alerting tools and reports can be generated from the alerts and from the uploader service. Each team is responsible for reviewing and analyzing the alerts for indications of inappropriate or unusual activity, including indications of compromise. Findings are reported and escalated using standard security incident management channels: Tickets are opened to track these security incidents using ticket tracking software and the Product1 Security team is engaged when appropriate.

All servers upload logs to a repository service for aggregation and analysis. Handling and access to event and anomaly data is detailed in the AU family of controls.

Part e

Product1

Product1 Security notifies service teams if a change in the level of monitoring is necessary due to indications of increased risk, and service teams adjust monitoring accordingly. Servers are configured to increase logging parameters in response to an indication of increased risk, and the automated security alerting tools heuristics are tailored to look for specific threats, in conjunction with any alerts received via NRT Security Monitoring, based on the nature of the risk to organizational operations and assets.

Part f

Product1

Product1 Security, in consultation with Corporate External Legal Affairs (CELA), has defined a

set of log events and alerts that meet federal regulatory requirements for incident management and investigation. This structure is intended to support identification of known suspicious activity and to support the investigation of misuse and abuse of Product1 services. To fully comply with applicable regulations, the service teams follow defined requirements for event collection and notification processes. These requirements are contained in the Product1 Security and PilotFish/K-9 onboarding document.
Part g Product1 All servers upload logs to a repository service for aggregation and analysis. Reports are generated from this data using NRT Security Monitoring and the automated security alerting tools as described AU-6 and AU-7. These reports are available daily and as needed. For teams using PilotFish, all servers upload logs to a repository service for aggregation and analysis. Reports are generated from this data using PilotFish/K-9 as described AU-6 and AU-7. These reports are available daily and as needed.

SI-04(01) System-wide Intrusion Detection System

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

SI-04(01) Control Summary Information
Responsible Role: Product1 Security Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility)

☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

SI-04(01) What is the solution and how is it implemented?
Product1 All servers upload logs to a repository service for aggregation and analysis. Consolidated reports are generated from this data using the automated security alerting tools as described AU-6 and AU-7, and cover system-wide intrusion detections. For teams using PilotFish, audit logs are uploaded to a repository service for aggregation and analysis. Reports are generated from this data using Pilotfish/K-9 as described AU-6 and AU-7. These reports are available daily and as needed. For services using inherited compute via Product2, this control is inherited from Product2.

SI-04(02) Automated Tools and Mechanisms for Real-time Analysis

Employ automated tools and mechanisms to support near real-time analysis of events.

SI-04(02) Control Summary Information
Responsible Role: Product1 Security Manager, Service Engineer Operations
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

SI-04(02) What is the solution and how is it implemented?
Product1 Service teams operate active monitoring systems that generate automated real-time alerts and audit logs from both SCOM and the uploader service. These automated tools perform analysis and trigger emails to Service Team Engineering groups when a specified threshold has been reached or event has occurred. Upon receipt, Service Team Engineering personnel uses a ticketing tool and creates a bug to analyze and track the issue and follow incident response procedures. Teams using PilotFish use K9, a tool that collects security logs and performs real-time analysis. Unusual activity generates alerts, and the PilotFish team coordinates with the appropriate service team for any required follow-ups or investigations. Service teams will work with the Product1 SIR team to address all security incidents. For services using inherited compute via Product2, this control is inherited from Product2.

SI-04(04) Inbound and Outbound Communications Traffic

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic [FedRAMP Assignment: continuously] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

SI-04(04) Control Summary Information
Responsible Role: Product2, Product1 Security Manager, Service Engineer Operations
Parameter SI-04(04)(b)-1: Continuously
Parameter SI-04(04)(b)-2: denial of service activities or conditions
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

SI-04(04) What is the solution and how is it implemented?
Part a Product1 Product2 monitors for unusual traffic patterns using OneDDOS. In addition, service teams monitor for denial of service attacks by monitoring the following key health metrics: CPU usage, network connections, disk input/output operations per second (IOPS), and disk space usage. Product1 service teams also monitor and review web server (e.g. IIS) logs and other application logs (as applicable) for unusual or unauthorized activities or conditions. Any unapproved connections detected through auditing or alerting will be triaged using security incident response processes.
Part b Product1 See Part (a).

SI-04(05) System-generated Alerts

Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

SI-04(05) Additional FedRAMP Requirements and Guidance:

SI-4 (5) Guidance: In accordance with the incident response plan.

SI-04(05) Control Summary Information
Responsible Role: Product1 Security Manager, Service Engineer Operations
Parameter SI-04(05)-1: At a minimum, the ISSM and ISSO

Parameter SI-04(05)-2: Real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B

Implementation Status (check all that apply):
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☒ Service Provider System Specific
☐ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

SI-04(05) What is the solution and how is it implemented?

Product1

Product1 Security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include Near Real Time Security Monitoring (NRT Security Monitoring), System Center Operations Manager (SCOM) and the automated security alerting tools, which are configured to provide real time alerts to Service Team Operations personnel in situations that require immediate action. Service Team Operations personnel act as the designee of the SCA / ISSO.

For teams using PilotFish use K-9 which is configured to provide real time alerts to Service Team Operations personnel in situations that require immediate action. The list of events being monitored is stored on each respective team's SharePoint site.

For services using inherited compute via Product2, this control is inherited from Product2.

SI-04(10) Visibility of Encrypted Communications

Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].

SI-04(10) Additional FedRAMP Requirements and Guidance:

SI-4 (10) Requirement: The service provider must support Agency requirements to comply with M-21-31

SI-04(10) Control Summary Information
Responsible Role: Customer Administrator
Parameter SI-04(10)-1: none
Parameter SI-04(10)-2: none
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

SI-04(10) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for making provisions so that customer-defined encrypted communications traffic are visible to information system monitoring tools. Product1 This control does not apply to Product1. Product1 does not inspect or monitor customer traffic. By default, Product1 is unaware of what data is outbound from the environment by the

customer. In the event of customer data spillage, upon customer request, Product1 may assist with the incident including accessing customer data according to the Product1 Incident Response Policies and Procedures.

SI-04(11) Analyze Communications Traffic Anomalies

Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.

SI-04(11) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Service Engineer Operations
Parameter SI-04(11): Terminal Service Gateways (TSG)
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☒ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☒ Inherited from pre-existing authorization for Product2 Government (F1603087869), 4/17/2020

SI-04(11) What is the solution and how is it implemented?
Customer Responsibility Government customers are responsible for analyzing communications traffic anomalies for customer-deployed resources, including an analysis of outbound communications traffic at the external boundary and at customer-defined interior points within the system to discover anomalies.

Product1

Product1 monitors for and protects against mining of system data and customer content. All access to Product1 occurs through remote access to the TSG or Product2 managed Terminal Services Gateways (TSG). The Product1 Security team monitors remote access for any large data exfiltration through the TSGs. Product1 Security uses a robust security monitoring and alerting tool to ingest logs from hosts and other networking infrastructure in the environment, compare these logs to an extensive ruleset, and alert Security personnel when a match is found between the two. Service teams also employ HostIDS to further monitor for data exfiltration at the host level. NRT is used to alert based on specific security events as well as other indicators of compromise such as anomalous behavior and suspicious activity.

In addition, access to the Product1 system is limited to a small number of Product1 cleared service team administrators. Product1 cleared service team administrators have taken role-based access training, security awareness training and have been background screened.

If Product1 becomes aware of any unlawful access to any customer content stored in its equipment or in its facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of customer content (each considered a security incident), Product1 will: (a) notify the affected customer of the security incident; (b) investigate the security incident and provide the customer with information about the security incident; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.

In the event of customer data spillage, upon customer request, Product1 may assist with the incident including accessing customer data according to the Product1 Incident Response Policies and Procedures.

SI-04(12) Automated Organization-generated Alerts

Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].

SI-04(12) Control Summary Information
Responsible Role: Customer Administrator, Product1 Security Manager, Service Engineer Operations
Parameter SI-04(12)-1: service team engineering groups
Parameter SI-04(12)-2: SCOM and repository service

Parameter SI-04(12)-3: When there are threats identified by authoritative sources
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

SI-04(12) What is the solution and how is it implemented?
Customer Responsibility Customers are responsible for monitoring and alerting security personnel of any unusual activities for systems that connect to Product1. Product1 Product1 automated security monitoring and alerting tools generate real time alerts and audit logs from both SCOM and the repository service. These automated tools perform analysis and trigger emails to Service Team Engineering groups when a specified threshold has been reached or event has occurred. Upon receipt, Service Team Engineering personnel use a ticketing tool and create a bug to analyze and track the issue and follow incident response procedures.