

Globus for CMMC Environments

Version: 1.0
Date: November 2026
Contact: support@globus.org

THE UNIVERSITY OF CHICAGO

Table of Contents

Executive Summary **3**
Overview **4**
Globus Security and Compliance Features **4**
Access Control and Least Privilege 4
Granular Sharing Policies 4
Identification and Authentication 5
Audit and Accountability Support 5
Communications Protection and Information Integrity 5
Globus Services within CMMC Environments **5**
Scoping and Shared Responsibility 6
Audit Support and Assessor Engagement 6
Globus's CMMC Assessment Status 6
Data stored or accessed by Globus **7**
File metadata 7
Identity and authentication data 7
User provided data 7
Globus Compute results 8
Globus Flow run state and action output 8
Operational and log data 8
Data not stored or accessed by Globus 9
Additional Resources 10

Executive Summary

Globus is a hybrid SaaS platform, operated by the University of Chicago, that provides secure data transfer, sharing, automation, and function execution for research organizations. This document explains how customers subject to Cybersecurity Maturity Model Certification (CMMC) requirements can use Globus in their own environments when handling Controlled Unclassified Information (CUI).

Globus data transfer and sharing services provide authentication, authorization, and access control for data on customer-managed systems. File contents move directly between customer-controlled endpoints over an encrypted channel and are never transmitted to or stored on Globus-operated infrastructure. Globus retains only metadata, such as file names, paths, and sizes, which customers should keep free of CUI. Because these services do not process, store, or transmit CUI, but do support authentication, customers may scope them as Security Protection Assets (SPAs) in their CMMC environments.

Other services, such as Compute and Flows, may be considered SPAs or Out of Scope depending on how they are used. Customers are also responsible for ensuring CUI does not appear in the data those services store, such as function arguments and results or flow inputs and outputs.

Each customer defines its own CMMC assessment boundary. Globus does not assess or certify customer deployments, but it will support customers and their Certified Third-Party Assessment Organization (C3PAOs) with documentation reviews, in answering technical questions, and by participating in assessor interviews.

Ultimately, security is a shared responsibility. Globus secures the services it operates. Customers secure their endpoints and storage, are responsible for user access and sharing permissions, and for documenting Globus's SPA role in their System Security Plan (SSP). The Globus security program is aligned with the 110 requirements of NIST SP 800-171 Rev. 2.

Overview

This document describes how Globus services can be used within customer-operated environments subject to the Cybersecurity Maturity Model Certification (CMMC) program. Organizations that handle Controlled Unclassified Information (CUI) on behalf of the Department of Defense are required to protect CUI per standards defined in CMMC.

Globus is a hybrid SaaS platform operated by the University of Chicago. Globus services provide secure data management and function execution capabilities to a wide range of users, including academic institutions, national laboratories, and research organizations across the globe.

Globus Security and Compliance Features

Globus product features make it easier to meet your security and compliance requirements. The features and capabilities described here can be configured by customers to support the NIST SP 800-171 requirements underlying CMMC. A Globus High Assurance subscription is required for certain features and functionality described throughout this document. Current High Assurance eligible services can be viewed here.

Access Control and Least Privilege

- Layered access controls (e.g., IdP, mapping/sharing policies, local account policies)
- Deny/Allow user and/or groups, deny/allow paths
    - Storage admins can configure restrictions to limit accessible paths
- Multiple roles with scoped access (e.g., Admin, Manager, Monitor)
- Limited third-party disclosure of data
    - Files move directly between source and destination and never enter the Globus system boundary.
    - Data can be shared without moving files to a third-party file sharing platform.
- Restrict data movement to/from other High Assurance storage systems

Granular Sharing Policies

- Narrowly-scoped sharing permissions for least privilege
- Enforcement of who can share what by policy
- Time limited sharing permissions enforced by policy
- Automatic removal of unnecessary guest collections by policy
- Roles to allow delegation of sharing permissions management
- Group based sharing permissions
- Globus policy prevents public or anonymous data sharing

Identification and Authentication

- Use of federated authentication
- Policy to require authentication with trusted identity providers
- Enforce Multi-factor Authentication (MFA) policy for data access
- Require time-limited authentication sessions
- Authentication sessions isolated by application

Audit and Accountability Support

- Transfer records include all task activity, including list of all transferred files
- Real time monitoring of all transfer tasks
- Ability to pause or cancel transfer tasks or suspend users
- Audit record of all data access events
- Access to usage reports for task level summary of all historical transfers

Communications Protection and Information Integrity

- Encryption of all data in transit
- Encryption of all communication with Globus services
- Data integrity verification by policy
- Support for FIPS 140 compliant cryptographic modules

Globus Services within CMMC Environments

Organizations seeking a Level 2 CMMC assessment must classify the assets in their assessment scope into one of five asset categories based on the asset's relationship to CUI. A Security Protection Asset provides security functions or capabilities to an organization's CMMC assessment scope, but may not process, store, or transmit CUI.

Globus data transfer and sharing services provide authentication, authorization, and access control functions for data on customer-managed systems, which may include CUI. When Globus is used to transfer or share CUI, the file contents are never transmitted to or stored on Globus-operated infrastructure. Data moves directly between the source and destination endpoints over an encrypted channel established between the two customer-managed systems. Globus stores file metadata (e.g., file names, path information, file size). Customers should not include CUI in this metadata.

Because Globus data transfer and sharing services do not process, store, or transmit CUI, customers can scope them as Security Protection Assets. Other Globus services, (e.g., Compute, Flows) can function either as Security Protection Assets or as Out of Scope assets, depending on how the organization uses those services.

Scoping and Shared Responsibility

Globus is responsible for securing the Globus-operated services that provide Security Protection Asset functions. Customers are responsible for the systems they operate and for how they use Globus, including securing their Globus Connect Server endpoints and underlying storage, managing user access and sharing permissions, ensuring CUI does not cross into the Globus system boundary, and documenting Globus's Security Protection Asset role in their System Security Plan (SSP). Additional information is available in Globus's Shared Responsibility Matrix.

Each customer determines their own CMMC assessment boundary. Globus will support a customer's C3PAO assessment but does not directly assess or certify that any customer deployment meets CMMC requirements. Compliance depends on the customer's deployment configuration, organizational controls, institutional policies, contractual terms, and C3PAO assessment findings.

Audit Support and Assessor Engagement

Security Protection Assets fall within the scope of a CMMC assessment and are assessed against specific security requirements relevant to the functions they provide. An assessor may evaluate whether the SPA is appropriately secured and whether the customer has accurately characterized its role.
Globus is willing to engage with our customers and their C3PAOs to support CMMC assessments. This may include participating in documentation reviews, answering technical questions about Globus architecture and security controls, and, where appropriate, joining assessor interviews to explain Globus's role as an SPA.

Globus's CMMC Assessment Status

In November 2025, Globus completed a CMMC Level 1 self-assessment against the 15 practices in FAR Clause 52.204-21 and submitted an affirmation in the Supplier Performance Risk System (SPRS). Globus's security program is also aligned with the 110 security requirements of NIST SP 800-171 Revision 2.

A Cloud Service Provider within the CMMC assessment scope that processes, stores, or transmits CUI must be FedRAMP authorized. Globus services are not currently FedRAMP authorized, consistent with its categorization as a Security Protection Asset, which does not process, store, or transmit CUI. It is the organization's responsibility to ensure CUI does not cross into the Globus system boundary. The following section describes the organizational data stored in the Globus system boundary.

Data stored or accessed by Globus

Globus's hosted services process, store, and transmit a variety of data categories.

File metadata

Globus monitors transfer progress and executes integrity checks. When a user browses a collection, the directory listing is requested through the Globus Transfer service and returned to the user. When a user submits a transfer, the request is recorded in the Transfer service's database. As a result, Globus processes, stores, and transmits file metadata, such as file names, directory paths, and file attributes such as size and modification time.

Identity and authentication data

Globus acts as an identity broker and receives usernames, email addresses, and identity provider-specific identifiers. These attributes are released to Globus by the institutional identity provider following a successful, federated authentication. Institutional credentials are never accessed or stored by Globus.

User provided data

Users and administrators enter descriptive metadata and configuration into Globus services. This includes display names, descriptions, keywords, tags, messages, and other free-text fields, plus structured configuration such as permission rules and saved requests. By service, this includes:

- **Transfer and Globus Connect:** endpoint, storage gateway, and collection display names; descriptions; keywords; contact organization information; transfer and delete task labels; bookmark names and paths; guest collection permission rules, and the custom notification messages sent when sharing.
- **Groups:** group names, descriptions, terms and conditions, and custom invitation or membership messages.
- **Timers:** timer names, and the transfer or flow request stored with each timer, including its paths and labels.
- **Compute:** endpoint names and descriptions, function names and source code, and function arguments.
- **Flows:** flow titles, descriptions, keywords, definitions, and input schemas; run labels and tags; and run inputs.
- **Search:** index names and descriptions, ingested documents, and queries.
- **Auth:** project names, app (client) names, and policy names and descriptions.

Globus Compute results

Globus Compute runs functions on customer-operated Compute endpoints. The hosted service passes tasks and results between the submitting client and the endpoint. The service serializes the arguments passed to a function and the return values or exceptions it produces. Because the service stores and transmits whatever a function returns, customers control what data reaches Globus through how they design their functions. For example, if a function reads file contents on an endpoint and returns them as its result, that content will pass through the Compute service and be stored there temporarily. In CMMC environments, CUI must not appear in function source code, arguments, return values, or exceptions.

Globus Flow run state and action output

Globus Flows automates multi-step tasks (e.g., start a transfer, run a Compute function, then send a notification). When you use Globus Flows, it will store the definition of the multi-step workflow and metadata about the executions of that workflow. For example, Globus Flows stores the output from a step, the step status, identities allowed to read or make modifications, start and completion times, and step specific result details. If a flow run fails and Globus Flows catches the exception, the error information is also stored by Globus Flows. In CMMC environments, CUI must not appear in any of these fields.

Operational and log data

Globus services generate operational records and logs as part of running the service. These include:

- The transfer task records and event logs described above
- IP addresses of clients that connect to Globus services
- IP addresses of Globus Connect Server, Globus Connect Personal, and Globus Compute endpoints that communicate with Globus services
- Select system information reported by endpoints, such as operating system and OpenSSL version
- Notification emails sent to the address associated with a user's identity
- Log data and cookies collected on Globus websites, as described in the Globus Privacy Notice

Data not stored or accessed by Globus

- **File contents**. Files transferred and shared with Globus Transfer and Globus Connect stay on storage systems that customers provide and control. Their contents never reside on Globus infrastructure and do not pass through it, even temporarily, during transfer. Because Globus Transfer does not store file contents, files may contain CUI as this will not be processed by Transfer. CUI should still be kept out of metadata.
- **Institutional credentials.** To act on a user's behalf, Globus uses only temporary credentials, in the form of delegated, revocable OAuth 2.0 tokens. Users never enter their passwords or long-term site credentials into Globus services. Users can review and revoke the consents they have granted to applications at auth.globus.org/consents.
- **Globus Connect and Compute Endpoint audit logs.** Globus Connect and Compute Endpoint write audit logs directly to the customer's storage system. The customer is responsible for log access, encryption, and retention.
- **Endpoint deployment keys.** Globus Connect Server deployment requires the generation of a deployment key that encrypts the endpoint configuration that is backed up to the cloud. The encryption key is managed by the customer and not accessible to Globus.
- **Data Transfer Encryption Keys.** Session keys are generated for each data channel connection to encrypt files in transit. Globus does not have access to these keys.

Globus continues to monitor evolving CMMC requirements and DoD guidance. To discuss your organization's compliance needs, contact support@globus.org.

Additional Resources

- Globus Documentation
- Globus Security and Compliance Overview
- High Assurance Security Overview
- High Assurance Eligible Services
- Admin Guide for Sensitive Data
- Sensitive Data Transfer and Sharing User Guide
- Globus Connect Personal FIPS Cryptography Support
- FAQs: Security