Enterprise Mission Assurance Support Service (eMASS)

eMASS REST API (v3.7)

Documentation

December 15, 2022

Table of Contents

REVISION HISTORY

Version	Date	Description
1.0	November 16, 2017	Initial availability of the eMASS API. Deployed in eMASS v5.5.0.4 release.
1.1	March 5, 2018	Added fields to Systems endpoint: • Organization Name • Secondary Organization • Cross Domain Ticket • Security Plan Approval Status • Security Plan Approval Date • RMF Activity Deployed in eMASS v5.5.1.4 release.
1.2	April 12, 2018	Added fields to Controls endpoint: • Criticality • Frequency • Method • Reporting • Tracking • SLCM Comments Deployed in eMASS v5.5.2.0 release.
1.3	August 17, 2018	Added parameter to Systems endpoint: • Include DITPR Metrics Added fields to Systems endpoint: • DITPR-DON ID • Contingency Plan Tested • Contingency Plan Tested Date • Security Review Date • Has Open POA&M Item • Between 90 and 120 Days Past SCD • Greater than 120 Days Past SCD Deployed in eMASS v5.5.3.4 release.
2.0	August 23, 2018	Added user-uid header for actionable requests. Added fields to Controls endpoint: • Residual Risk Level • Likelihood • Relevance of Threat • Impact • Impact Description Renamed field in Controls endpoint: • Vulnerability Severity → Severity • Control Risk Level → Residual Risk Level • Criticality → SLCM Criticality • Frequency → SLCM Frequency • Method → SLCM Method • Reporting → SLCM Reporting • Tracking → SLCM Tracking

		Added fields to POA&Ms endpoint: • Mitigation • Residual Risk Level • Likelihood • Relevance of Threat • Impact • Impact Description • Recommendations Renamed fields in POA&Ms endpoint: • Raw Severity Value → Raw Severity • Severity Value → Severity Deployed in eMASS v5.5.4.0 release.
2.1	July 25, 2019	Added parameter to Artifacts endpoint: • Compress Deployed in eMASS v5.6.3.2 release.
2.2	January 16, 2020	Added fields to Systems endpoint: • Description • Terms For Auth • Is Public Facing • System Ownership • Authorization Length • Security Review Date • Geographical Association Added parameter to Systems endpoint: • Include Decommissioned Added System Roles endpoint. Deployed in eMASS v5.7.0.6 release.
2.3	December 10, 2020	Added fields to Systems endpoint: • Impact • Has CUI • Has PII • Has PHI • PPSM Registry Number • Interconnected Information System and Identifiers • Is PIA Required • PIA Status • PIA Date • User-defined Fields 1-5 • Current RMF Lifecycle Step • Other Information • Connectivity • CCSD Number Added parameter to System Roles endpoint: • Include Decommissioned Added field to PAC endpoint: • Days at Current Stage Deployed in eMASS v5.8.0.2 release.
3.0	April 29, 2021	Changed endpoint routes:

		- /register → /api-key - /systemrole → /system-roles - /testresults → /test-results - /poam → /poams - /artifactsexport → /artifacts-export Added field to Controls endpoint: - Test Method Renamed field in Controls endpoint: - Comments → Implementation Narrative Added field to POA&M endpoint: - Display POA&M ID Renamed fields in PAC endpoint: - Workflow Name → Workflow - Current Role → Current Stage Name - Current Step → Current Stage - Total Steps → Total Stages Removed field from PAC endpoint: - Type Deployed in eMASS v5.9.0.0 release.
3.1	July 7, 2021	Added CMMC Assessments endpoint. Deployed in eMASS v5.9.1.0 release.
3.2	October 21, 2021	Added Static Code Scans endpoint. Added Workflow Definitions endpoint. Added Workflow Instances endpoint. Added parameter to Systems endpoint: - Reports for Scorecard Deployed in eMASS v5.9.2.0 release.
3.3	March 16, 2022	Renamed field in Systems endpoint: - ContingencyPlanTestedDate → ContingencyPlanTestDate Changed endpoint routes: - /workflow-definitions → /workflows/definitions - /systems/{systemId}/workflow-instances → /workflows/instances Added Cloud Resource Results endpoint. Added Container Scan Results endpoint. Deployed in eMASS v5.9.4.0 release.
3.4	June 27, 2022	Added field to Systems endpoint: - Highest System Data Classification - [NISP Only] Overall Classification Renamed field in Systems endpoint: - [VA Only] DITPR ID → VASI ID Added Dashboards endpoint. Deployed in eMASS v5.10.0.0 release.

3.5	July 28, 2022	Added fields to Systems endpoint: • Is HVA Deployed in eMASS v5.10.0.1 release.
3.6	September 15, 2022	Added fields to Systems endpoint: • Is Financial Management • Is Reciprocity • Reciprocity Exemption • Cloud Computing • Cloud Type • Is SaaS • Is PaaS • Is IaaS • Other Service Models • Need Date • Overall Risk Score • Is HRR • ATC Status • ATC Date • ATC Termination Date • System Development Lifecycle • Is FISMA Reportable Added fields to CMMC Assessments endpoint: • Highest Level Order Cage Code • Certification Unique ID • POAM • Overall Score • OSC Assessment Official Last Name • OSC Assessment Official First Name • OSC Assessment Official Email • OSC Assessment Official Title Renamed fields in CMMC Assessments endpoint: • Unique Entity Identifier -> UEI • CageCodes → CageCodesInScope • CertificateID → AssessmentID Removed field from CMMC Assessments endpoint: • DUNS Added Artifacts Dashboard endpoints. Deployed in eMASS v5.10.1.0 release.
3.7	December 15, 2022	Added field to Systems endpoint: • Instance Renamed field in Systems endpoint: • Organization Name → Owning Organization • [Army Only] DITPR ID → APMS ID Removed field from Systems endpoint: • System Owner Added parameter to Dashboards endpoint: • excludeInherited Deployed in eMASS v5.10.2.0 release.

1.0 INTRODUCTION

The Enterprise Mission Assurance Support Service (eMASS) Representational State Transfer (REST) Application Programming Interface (API) enables users to perform assessments and complete actions associated with system records. This document will provide an outline of all eMASS objects and their associated endpoints to include business rules that pertain to each.

2.0 GETTING STARTED

2.1 REGISTER EXTERNAL APPLICATION

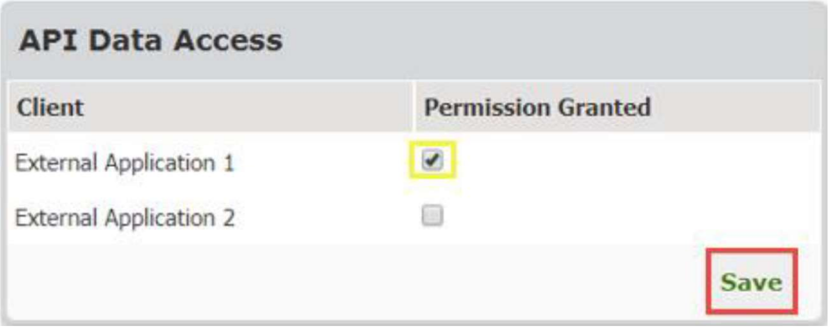
New users will need to register an API key with the eMASS development team prior to accessing the site for the first time. The eMASS API requires a client certificate (SSL/TLS, PKI only) where {url}/api/api-key (POST) is used to register the client certificate.

Every call to the eMASS API will require the use of the agreed upon public key certificate and API key. The API key must be provided in the request header for all endpoint calls (api-key). If the service receives an untrusted certificate or API key, a 401-error response code will be returned along with an error message.

2.2 APPROVE API CLIENT FOR ACTIONABLE REQUESTS

Users are required to log-in to eMASS and grant permissions for a client to update data within eMASS on their behalf. This is only required for actionable requests (PUT, POST, DELETE). The Registration endpoint and all GET requests can be accessed without completing this process with the correct permissions. Please note that leaving a field parameter blank (for PUT/POST requests) has the potential to clear information in the active eMASS records.

Users can grant permissions for the client from their eMASS User Profile in the *API Data Access* section by selecting a checkbox for the applicable client and clicking **[Save]**.



API Data Access

Client	Permission Granted
External Application 1	☑
External Application 2	☐

Once saved, the client can begin completing actionable requests in eMASS.

3.0 VERSIONING

Versioning will be specified through a query string parameter (?api-version=1.0) or request header (api-version:1.0). If no version is specified, then the system will default to the latest version. Available versions will follow the format #.0 and include the latest update from that version. E.g. using api-version:1.0 will return results from 1.2 or the latest available corresponding 1.# version. All responses will include headers with information about any deprecated versions. A deprecated API version will be maintained for 6 months before the version is no longer available for use.

The following deprecated API versions are currently available:

- Version 2.3

3.1 REQUEST HEADERS

Available request headers are depicted in the following table:

Available Request Headers

Key	**Example Value**	**Description**
api-key	f32516cc-57d3-43f5-9e16-8f86780a4cce	This API key must be provided in the request header for all endpoint calls.
user-uid	1647389405	This User unique identifier key must be provided in the request header for all PUT, POST, and DELETE endpoint calls. **Note:** For DoD users this is the DoD ID Number (EIDIPI) on their DoD CAC.

3.2 RESPONSE NOTIFICATIONS & ERROR CODES

If a request to the eMASS API is successful, it will return a structured JSON response envelope. If unsuccessful, it will return an error code and any relevant error messages.

Response envelope (success)

```
{
    "meta": {
        "code": 200
    },
    "data": {
        ...
    },
    "pagination": {
        "totalCount": "5000",
        "totalPages": "20",
        "prevPageUrl": "...",
        "nextPageUrl": "..."
    }
}
```

Response envelope (error)

```
{
    "meta": {
        "code": 500
        "errorMessage": "..."
    }
}
```

The eMASS REST API will adhere to standard HTTP Status Codes as much as possible. The following table provides a small list of commonly used codes within the API; however, this list may not be fully comprehensive of all possible response notifications.

HTTP Status Code	Description/Likely Causes
200: OK	Request has succeeded. Applicable to partial successes and the response body depends on the request method.
201: Created	Request was fulfilled and resulted in on or more new resources being successfully created on the server.
400: Bad Request	Request could not be understood by the server due to incorrect syntax or an unexpected format.
401: Unauthorized	Request has failed to provide suitable authentication from the client (see section 2.0 Getting Started).
403: Forbidden	Request was blocked by the application due to a lack of client permissions to the API or to a specific endpoint.
404: Not Found	Request has failed because the URL provided in the request did not match any available endpoint locations.

405: Method Not Allowed	Request was made with a verb (GET, POST, etc.) that is not permitted for the endpoint.
411: Length Required	Request was of type POST and failed to provide the server information about the data/content length being submitted.
490: API Rule Failed	Request has failed because too much data was requested in a single batch. This error is specific to eMASS.
500: Internal Server Error	Server encountered an unexpected condition which prevented it from fulfilling the request.

The sample response below is an example of a response from a POST request to the Test Result Endpoint. The first object was created successfully. The second object was created successfully but has additional warnings for consideration. The third object failed and supplies the reasons why in the errors field. Please note that leaving a field parameter blank has the potential to clear information in the active eMASS records.

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "cci": "002110",
            "success": true,
            "systemId": 1
        },
        {
            "cci": "002107",
            "success": true,
            "systemId": 1,
            "warnings": [
                "You have entered a Non-Compliant Test Result. You
                 must create a POA&M Item for this Control and/or AP
                 if one does not already exist."
            ]
        },
        {
            "cci": "002108",
            "success": false,
            "systemId": 1,
            "errors": [
                "The Status is required."
            ]
        }
    ]
}
```

4.0 ENDPOINTS

The eMASS REST API exposes the following endpoints:

- Test Connection
- Registration
- Systems
- System Roles
- Controls
- Test Results
- POA&Ms
- Milestones
- Artifacts
- Artifacts Export
- PAC
- CAC
- CMMC Assessments
- Static Code Scans
- Workflow Definitions
- Workflow Instances
- Cloud Resource Results
- Container Scan Results
- Dashboards

Each set of endpoints will have an example provided in curl for development purposes only. Please ensure you follow your system's architecture and security requirements.

Endpoints are defined by parameter, data type, details, and presence of an associated business rule. The data types for each parameter are defined by the following table:

BOOLEAN	Logical Boolean type with accepted values true, false.
INTEGER	Signed [-+] number composed of numeric values 0-9
DATE	Denoted by Unix Time in the format 1499891128
STRING	Sequence of characters

A master list of DoD-defined business rules, parameters, and fields for each endpoint can be found in Appendices A and B.

Endpoints that can receive multiple objects will accept a response body of up to 1000 unique objects. Requests with larger than 1000 objects will be rejected, and the client is required to break the request body into multiple requests.

4.1 TEST CONNECTION ENDPOINT

The Test Connection endpoint provides the ability to verify connection to the web service.

GET	/api *Test connection to the API*

Curl Example

```
curl -L "[URL]/api" --cert .\cert.cer --key .\private.key
```

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": {
        "success": true
    }
}
```

4.2 REGISTRATION ENDPOINT

The Registration endpoint provides the ability to register a certificate & obtain an API-key.

Notes:

- This API-key must be provided in the request header for all endpoint calls.
- Example header: api-key: f0126b6b-f232-45c9-a8de-01d5f003deda

POST	/api/api-key *Register certificate and obtain API key*

Curl Example

```
curl -X POST -d -L "[URL]/api/api-key" --cert .\cert.cer --key .\private.key
```

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": {
        "apikey": "f0126b6b-f232-45c9-a8de-01d5f003deda"
    }
}
```

4.3 SYSTEMS ENDPOINTS

The Systems endpoints provide the ability to view system information.

Notes:

- If a system is dual-policy enabled, the returned system details defaults to the RMF policy information unless otherwise specified for an individual system.
- Certain fields are instance specific and may not be returned in GET request.

GET	**/api/systems** *Get system information*

Curl Example

```
curl -L "[URL]/api/systems" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.cer --key .\private.key
```

Available Query String Parameters

Name	**Type**	**Example**
coamsId	String	30498
ditprId	String	93054
includeDecommissioned	Boolean	true, false If no value is specified, the default returns true to include decommissioned systems.
includeDitprMetrics	Boolean	true, false This query string parameter cannot be used in conjunction with the following parameters: • includePackage • ditprId • coamsId If no value is specified, the default returns false to not include DITPR Metrics.
includePackage	Boolean	true, false If no value is specified, the default returns false to not include package information.
policy	String	Accepts single value from the following options: • diacap • rmf • reporting If no value is specified, the default returns RMF policy information for dual-policy systems.

registrationType	String	Accepts multiple comma-separated values including the following options: • assessAndAuthorize • assessOnly • guest • regular • functional • cloudServiceProvider • commonControlProvider
reportsForScorecard	Boolean	true, false Used to filter results to only return systems that report to the DoD Cyber Hygiene Scorecard.

Sample Response
(includePackage=true, includeDecommissioned=false)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "secondaryOrganization": "Test Organization",
            "description": "Test System Description",
            "isNSS": true,
            "coamsId": null,
            "isTypeAuthorization": false,
            "securityPlanApprovalStatus": "Approved",
            "securityPlanApprovalDate": 1622234497.6,
            "missionCriticality": "Mission Critical (MC)",
            "governingMissionArea": "Warfighting MA (WMA)",
            "primaryFunctionalArea": "Allies",
            "secondaryFunctionalArea": "Intelligence",
            "appliedOverlays": "Classified Information,Privacy",
            "rmfActivity": "Maintain ATO and conduct reviews",
            "crossDomainTicket": "Test Cross Domain Ticket",
            "termsForAuth": "Terms/Conditions for Authorization",
            "isPublicFacing": false,
            "systemOwnership": "DoD-Partnered System",
            "package": [
                {
                    "workflow": "RMF Step 1: Security Category",
                    "name": "Test Package Name",
                    "currentStageName": "Submit Categorization",
                    "currentStage": 2,
                    "totalStages": 3,
                    "daysAtCurrentStage": 7.4
                }
            ],
            "authorizationLength": 730,
            "highestSystemDataClassification": "Unclassified",
            "isFinancialManagement": true,
            "isReciprocity": true,
        "reciprocityExemption": null,
        "cloudComputing": true,
        "cloudType": "Public",
        "atcStatus": null,
        "isSaaS": false,
        "isPaaS": true,
        "isIaaS": false,
        "otherServiceModels": "Test Other Service",
        "needDate": null,
        "overallRiskScore": "Moderate",
        "isHRR": null,
        "atcDate": null,
        "atcTerminationDate": null,
        "systemId": 27,
        "registrationType": "Assess and Authorize",
        "name": "eMASS API Example System",
        "acronym": "eMASS API-ES",
        "instance": "Navy",
        "owningOrganization": "Test Organization",
        "versionReleaseNo": "5.9.1.0",
        "policy": "RMF",
        "systemType": "IS Major Application",
        "ditprId": "Test DITPR ID",
        "authorizationStatus": "Authorization to Operate (ATO)",
        "authorizationDate": 1622061697.6,
        "authTerminationDate": 1685133697.6,
        "primaryControlSet": "NIST SP 800-53 Revision 4",
        "confidentiality": "Moderate",
        "integrity": "Moderate",
        "availability": "High",
        "securityReviewDate": 1622048629.307,
        "contingencyPlanTested": true,
        "contingencyPlanTestDate": 1622048629.307,
        "impact": "High",
        "hasCUI": false,
        "hasPII": false,
        "hasPHI": false,
        "ppsmRegistryNumber": "Test PPSM Registry Number",
        "interconnectedInformationSystemsAndIdentifiers": "Test",
        "isPiaRequired": true,
        "piaStatus": "Completed",
        "piaDate": 1622048629.307,
        "userDefinedField1": "Test User-defined Field 1",
        "userDefinedField2": "Test User-defined Field 2",
        "userDefinedField3": "Test User-defined Field 3",
        "userDefinedField4": "Test User-defined Field 4",
        "userDefinedField5": "Test User-defined Field 5",
        "currentRmfLifecycleStep": "1 - Categorize",
        "otherInformation": "Additional Comments",
        "reportsForScorecard": true,
        "connectivityCcsd": [
            {
                "ccsdNumber": "CCSD Number",
                "connectivity": "Test Connectivity"
            }
        ]
    },
    ]
}
```

Sample Response
(includeDitprMetrics=true)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "ditprDonId": "5910,1234,5678",
            "hasOpenPOAMItem": true,
            "between90and120PastScheduledCompletionDate": false,
            "greaterThan120PastScheduledCompletionDate": false,
            "systemId": 27,
            "registrationType": "Assess and Authorize",
            "name": "eMASS API Example System",
            "acronym": "eMASS API-ES",
            "instance": "Navy",
            "owningOrganization": "Test Organization",
            "versionReleaseNo": "5.9.1.0",
            "policy": "RMF",
            "systemType": "IS Major Application",
            "ditprId": "Test DITPR ID",
            "authorizationStatus": "Authorization to Operate (ATO)",
            "authorizationDate": 1622061697.6,
            "authTerminationDate": 1685133697.6,
            "confidentiality": "Moderate",
            "integrity": "Moderate",
            "availability": "High",
            "securityReviewDate": 1622048629.307,
            "contingencyPlanTested": true,
            "contingencyPlanTestDate": 1622048629.307,
            "impact": "High",
            "hasCUI": false,
            "hasPII": false,
            "hasPHI": false,
            "ppsmRegistryNumber": "Test PPSM Registry Number",
            "interconnectedInformationSystemsAndIdentifiers": "Test",
            "isPiaRequired": true,
            "piaStatus": "Completed",
            "piaDate": 1622048629.307,
            "userDefinedField1": "Test User-defined Field 1",
            "userDefinedField2": "Test User-defined Field 2",
            "userDefinedField3": "Test User-defined Field 3",
            "userDefinedField4": "Test User-defined Field 4",
            "userDefinedField5": "Test User-defined Field 5",
            "currentRmfLifecycleStep": "1 - Categorize",
            "otherInformation": "Additional Comments",
            "reportsForScorecard": false,
            "connectivityCcsd": [
                {
                    "ccsdNumber": "CCSD Number",
                    "connectivity": "Test Connectivity"
                }
            ]
        },
    ]
}
```

GET	/api/systems/{systemId} *Get system information for a specific system*

Curl Example

```
curl -L "[URL]/api/systems/27" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.cer --key .\private.key
```

Available Query String Parameters

Name	**Type**	**Example**
includePackage	Boolean	true, false If no value is specified, the default returns false to not include package information.
policy	String	Accepts single value from the following options: • diacap • rmf • reporting If no value is specified, the default returns RMF policy information for dual-policy systems.

Sample Response
(includePackage=false, policy=reporting)

```
{
    "meta": {
        "code": 200
    },
    "data": {
        "secondaryOrganization": "Test Organization",
        "description": "Test System Description",
        "isNSS": true,
        "coamsId": null,
        "isTypeAuthorization": false,
        "securityPlanApprovalStatus": "Approved",
        "securityPlanApprovalDate": 1622234497.6,
        "missionCriticality": "Mission Critical (MC)",
        "governingMissionArea": "Warfighting MA (WMA)",
        "primaryFunctionalArea": "Allies",
        "secondaryFunctionalArea": "Intelligence",
        "rmfActivity": "Maintain ATO and conduct reviews",
        "crossDomainTicket": "Test Cross Domain Ticket",
        "termsForAuth": "Terms/Conditions for Authorization",
        "isPublicFacing": false,
        "systemOwnership": "DoD-Partnered System",
        "package": [],
        "authorizationLength": 730,
        "systemId": 27,
        "registrationType": "Assess and Authorize",
        "name": "eMASS API Example System",
        "acronym": "eMASS API-ES",
        "instance": "Navy",
        "owningOrganization": "Test Organization",
        "versionReleaseNo": "5.9.1.0",
        "policy": "RMF",
        "systemType": "IS Major Application",
        "ditprId": "Test DITPR ID",
        "authorizationStatus": "Authorization to Operate (ATO)",
        "authorizationDate": 1622061697.6,
        "authTerminationDate": 1685133697.6,
        "primaryControlSet": "NIST SP 800-53 Revision 4",
        "confidentiality": "Moderate",
        "integrity": "Moderate",
        "availability": "High",
        "securityReviewDate": 1622048629.307,
        "contingencyPlanTested": true,
        "contingencyPlanTestDate": 1622048629.307,
        "impact": "High",
        "hasCUI": false,
        "hasPII": false,
        "hasPHI": false,
        "ppsmRegistryNumber": "Test PPSM Registry Number",
        "interconnectedInformationSystemsAndIdentifiers": "Test",
        "isPiaRequired": true,
        "piaStatus": "Completed",
        "piaDate": 1622048629.307,
        "userDefinedField1": "Test User-defined Field 1",
        "userDefinedField2": "Test User-defined Field 2",
        "userDefinedField3": "Test User-defined Field 3",
        "userDefinedField4": "Test User-defined Field 4",
        "userDefinedField5": "Test User-defined Field 5",
        "currentRmfLifecycleStep": "1 - Categorize",
        "otherInformation": "Additional Comments",
        "reportsForScorecard": true,
        "connectivityCcsd": [
            {
                "ccsdNumber": "CCSD Number",
                "connectivity": "Test Connectivity"
            }
        ]
    }
}
```

4.4 SYSTEM ROLES ENDPOINTS

The System Roles endpoints provides the ability to access user data assigned to systems.

Notes:

- The endpoint can access three different role categories: PAC, CAC, and Other.
- If a system is dual-policy enabled, the returned system role information will default to the RMF policy information unless otherwise specified.

GET	**/api/system-roles** *Get available roles*

Curl Example

```
curl -L "[URL]/api/system-roles" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.cer --key .\private.key
```

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "roleCategory": "PAC",
            "role": "SCA"
        },
        {
            "roleCategory": "PAC",
            "role": "AO"
        },
        {
            "roleCategory": "PAC",
            "role": "ISSM"
        },
        {
            "roleCategory": "CAC",
            "role": "Validator”
        },
        {
            "roleCategory": "Other",
            "role": "User Rep (View Only)"
        },
        {
            "roleCategory": "Other",
            "role": "Auditor"
        },
        {
            "roleCategory": "Other",
            "role": "Artifact Manager"
        }
    ]
}
```

GET	/api/system-roles/{roleCategory} *Get system roles*

Curl Example

```
curl -L "[URL]/api/system-roles/pac?role=SCA" -H "api-key: 0a60a84d-3fc1-
433c-b39f-507adb1f8bec" --cert .\cert.cer --key .\private.key
```

Available Query String Parameters

Name	Type	Example
role	String	**Required parameter.** Accepts single value from options available at base system-roles endpoint e.g., SCA.
policy	String	Accepts single value from the following options: • diacap • rmf • reporting If no value is specified, the default returns RMF policy information for dual-policy systems.

Sample Response
(role=SCA)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "systemId": 27,
            "systemName": "eMASS API Example System",
            "systemAcronym": "eMASS API-ES",
            "roles": [
                {
                    "roleCategory": "PAC",
                    "role": "SCA",
                    "users": [
                        {
                            "firstName": "John",
                            "lastName": "Doe",
                            "email": "john.doe.ctr@mail.mil"
                        },
                        {
                            "firstName": "Jane",
                            "lastName": "Doe",
                            "email": "jane.doe.ctr@mail.mil"
                        }
                    ]
                }
            ]
        },
        {
            "systemId": 29,
            "systemName": "eMASS Test System",
            "systemAcronym": "eMASS TS",
            "roles": [
                {
                    "roleCategory": "PAC",
                    "role": "SCA",
                    "users": [
                        {
                            "firstName": "John",
                            "lastName": "Doe",
                            "email": "john.doe.ctr@mail.mil"
                        }
                    ]
                }
            ]
        }
    ]
}
```

4.5 CONTROLS ENDPOINTS

The Controls endpoints provide the ability to view, add, and update Security Control information to a system for both the Implementation Plan and Risk Assessment.

GET	**/api/systems/{systemId}/controls** *Get control information in a system for one or many controls*

Curl Example

```
curl -L "[URL]/api/systems/27/controls" -H "api-key: 0a60a84d-3fc1-433c-
b39f-507adb1f8bec" --cert .\cert.cer --key .\private.key
```

Available Query String Parameters

Name	Type	Example
acronyms	String	AC-3,PM-6

Sample Response
(acronyms=AC-2(3))

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "systemId": 27,
            "name": "Disable Inactive Accounts",
            "acronym": "AC-2(3)",
            "ccis": "000017,000217",
            "isInherited": false,
            "includedStatus": "Baseline",
            "complianceStatus": "UA",
            "modifiedByOverlays": "Privacy",
            "responsibleEntities": "Test Responsible Entities",
            "implementationStatus": "Planned",
            "controlDesignation": "Common",
            "estimatedCompletionDate": 1622065680.1599998,
            "implementationNarrative": "Test Imp. Narrative",
            "testMethod": "Test, Examine",
            "slcmCriticality": "CRWG White Criticality Control",
            "slcmFrequency": "Monthly",
            "slcmMethod": "Automated",
            "slcmReporting": "Test Reporting",
            "slcmTracking": "Test Tracking",
            "slcmComments": "Test SLCM Comments"
        }
    ]
}
```

PUT	/api/systems/{systemId}/controls *Update control information in a system for one or many controls*

Sample Request Body

```
[
    {
        "acronym": "AC-1",
        "responsibleEntities": "Test Responsible Entities",
        "implementationStatus": "Not Applicable",
        "commonControlProvider": "DoD",
        "naJustification": "Test NA Justification",
        "controlDesignation": "Common",
        "testMethod": "Test",
        "estimatedCompletionDate": 1509375108,
        "implementationNarrative": "Test Imp. Narrative",
        "slcmCriticality": "Test Criticality",
        "slcmFrequency": "Daily",
        "slcmMethod": "Automated",
        "slcmReporting": "Test Reporting",
        "slcmTracking": "Test Tracking",
        "slcmComments": "Test SLCM Comments",
        "severity": "Moderate",
        "vulnerabilitySummary": "Test Vulnerability Summary",
        "recommendations": "Test Recommendations",
        "relevanceOfThreat": "Very Low",
        "likelihood": "Low",
        "impact": "Moderate",
        "impactDescription": "Test Impact Description",
        "residualRiskLevel": "High"
    }
]
```

4.5.1 Controls Endpoints Fields

Field	Type	Detail	Associated Business Rule?
systemId	Integer	[Required] Unique eMASS system identifier.	
name	String	[Read-Only] Name of control as defined in NIST SP 800-53 Revision 4.	
acronym	String	[Required] Required to match the NIST SP 800-53 Revision 4.	
ccis	String	[Read-Only] Comma separated list of CCIs associated with the control.	
isInherited	Boolean	[Read-Only] Indicates whether a control is inherited.	

modifiedByOverlays	String	[Read-Only] List of overlays that affect the control. An example would be the privacy overlay.	
includedStatus	String	[Read-Only] Indicates the manner by which a control was included in the system's categorization.	
complianceStatus	String	[Read-Only] Compliance status of the control.	
responsibleEntities	String	[Required] Include written description of Responsible Entities that are responsible for the Security Control. Character Limit = 2,000.	✓
implementationStatus	String	[Optional] Implementation Status of the Security Control for the information system. Values include the following options: • Planned • Implemented • Inherited • Not Applicable • Manually Inherited	✓
commonControlProvider	String	[Conditional] Indicate the type of Common Control Provider for an "Inherited" Security Control. Values include the following options: • DoD • Component • Enclave	✓
naJustification	String	[Conditional] Provide justification for Security Controls deemed Not Applicable to the system.	✓
controlDesignation	String	[Required] Values include the following options: • Common • System-Specific • Hybrid	✓
estimatedCompletionDate	Date	[Required] Field is required for Implementation Plan	✓

implementationNarrative	String	[Required] Includes Security Control comments. Character Limit = 2,000.	✓
slcmCriticality	String	[Conditional] Criticality of Security Control regarding SLCM. Character Limit = 2,000	✓
slcmFrequency	String	[Conditional] Values include the following options: • Constantly • Daily • Weekly • Monthly • Quarterly • Semi-Annually • Annually • Every Two Years • Every Three Years • Undetermined	✓
slcmMethod	String	[Conditional] Values include the following options: • Automated • Semi-Automated • Manual • Undetermined	✓
slcmReporting	String	[Conditional] Method for reporting Security Controls for SLCM. Character Limit = 2,000	✓
slcmTracking	String	[Conditional] How Non-Compliant Security Controls will be tracked for SLCM. Character Limit = 2,000	✓
slcmComments	String	[Conditional] Additional comments for Security Control regarding SLCM. Character Limit = 4,000	✓
severity	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High	

		• Very High	
vulnerabilitySummary	String	[Optional] Include vulnerability summary. Character Limit = 2,000.	
recommendations	String	[Optional] Include recommendations. Character Limit = 2,000.	
relevanceOfThreat	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	
likelihood	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	
impact	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	
impactDescription	String	[Optional] Include description of Security Control's impact.	
residualRiskLevel	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	
testMethod	String	[Optional] Identifies the assessment method / combination that will determine if the security	

		requirements are implemented correctly. Values include the following options: • Test • Interview • Examine • Test, Interview • Test, Examine • Interview, Examine • Test, Interview, Examine	

4.6 TEST RESULTS ENDPOINTS

The Test Results endpoints provide the ability to view and add test results for a system's Assessment Procedures (CCIs) which determine Security Control compliance.

GET	**/api/systems/{systemId}/test-results** *Get one or many test results in a system*

Available Query String Parameters

Name	Type	Example
controlAcronyms	String	AC-3,PM-6
ccis	String	002667,002619
latestOnly	Boolean	true, false

Sample Response (ccis=002667,002619)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "systemId": 6,
            "control": "SI-4(10)",
            "cci": "002667",
            "isInherited": false,
            "testedBy": "John Smith",
            "testDate": 1615305256.763,
            "description": "Test Results Text",
            "type": "Self-Assessment",
            "complianceStatus": "Non-Compliant"
        },
        {
            "systemId": 6,
            "control": "SI-3",
            "cci": "002619",
            "isInherited": false,
            "testedBy": "John Smith",
            "testDate": 1615305256.763,
            "description": "Test Results Text",
            "type": "Self-Assessment",
            "complianceStatus": "Non-Compliant"
        }
    ]
}
```

POST	**/api/systems/{systemId}/test-results** *Add one or many test results in a system*

Sample Request Body

```
[
  {
    "cci": "002107",
    "testedBy": "Smith, John",
    "testDate": 1497883526.177,
    "description": "NC test result from POST",
    "complianceStatus": "Non-Compliant"
  },
  {
    "cci": "002108",
    "testedBy": "Smith, John",
    "testDate": 1497883999,
    "description": "C test result from POST",
    "complianceStatus": "Compliant"
  }
]
```

4.6.1 Test Results Endpoints Fields

Field	**Type**	**Details**	**Associated Business Rule?**
systemId	Integer	[Required] Unique eMASS system identifier.	
control	String	[Read-Only] Control acronym associated with the test result. NIST SP 800-53 Revision 4 defined.	
cci	String	[Required] CCI associated with the test result.	
isInherited	Boolean	[Read-Only] Indicates whether a test result is inherited.	
testedBy	String	[Required] Last Name, First Name. Character Limit = 100.	✓
testDate	Date	[Required] Unix time format.	✓
description	String	[Required] Include description of test result. Character Limit = 4,000.	✓

type	String	[Read-Only] Indicates the location in the Control Approval Chain when the test result is submitted.	
complianceStatus	String	[Required] Values include the following options: • Compliant • Non-Compliant • Not Applicable	✓

4.7 POA&MS ENDPOINTS

The POA&Ms endpoints provide the ability to view, add, update, and remove Plan of Action and Milestones (POA&M) items and associated milestones for a system.

GET	/api/systems/{systemId}/poams *Get one or many POA&M items in a system*

Available Query String Parameters

Name	Type	Example
scheduledCompletionDateStart	Date	1499644800
scheduledCompletionDateEnd	Date	1499990400
controlAcronyms	String	AC-3,PM-6
ccis	String	000123,000069
systemOnly	String	true, false If no value is specified, the default returns false to include control and AP level artifacts as well.

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "externalUid": null,
            "systemId": 27,
            "poamId": 71,
            "displayPoamId": 101003238,
            "isInherited": false,
            "controlAcronym": null,
            "cci": null,
            "severity": "Very Low",
            "rawSeverity": "I",
            "status": "Completed",
            "reviewStatus": "Not Approved",
            "scheduledCompletionDate": 1622054028.83,
            "completionDate": 1622054028.83,
            "extensionDate": null,
            "pocOrganization": "Office/Organization",
            "pocLastName": "Last Name",
            "pocFirstName": "First Name",
            "pocEmail": "john.doe.ctr@mail.mil",
            "pocPhoneNumber": "1112223333",
            "vulnerabilityDescription": "Vulnerability Description",
            "mitigation": "Mitigations",
            "comments": "Comments",
            "resources": "Resources",
            "sourceIdentVuln": "Source Identifying Vulnerability",
            "securityChecks": null,
            "relevanceOfThreat": "Low",
            "likelihood": "Very Low",
            "impact": "Moderate",
            "impactDescription": "Impact Description",
            "residualRiskLevel": "Low",
            "recommendations": "Recommendations",
            "milestones": [
                {
                    "systemId": 27,
                    "milestoneId": 85,
                    "poamId": 71,
                    "description": "Milestone 1",
                    "scheduledCompletionDate": 1622054028.83,
                    "reviewStatus": "Not Approved"
                },
                {
                    "systemId": 27,
                    "milestoneId": 86,
                    "poamId": 71,
                    "description": "Milestone 2",
                    "scheduledCompletionDate": 1622054028.83,
                    "reviewStatus": "Not Approved"
                }
            ]
        }
    ]
}
```

GET	/api/systems/{systemId}/poams/{poamId} *Get POA&M item by ID in a system*

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": {
        "externalUid": null,
        "systemId": 27,
        "poamId": 73,
        "displayPoamId": 101003239,
        "isInherited": true,
        "controlAcronym": "AC-2(1)",
        "cci": null,
        "severity": "Very Low",
        "rawSeverity": "II",
        "status": "Risk Accepted",
        "reviewStatus": "Not Approved",
        "scheduledCompletionDate": null,
        "completionDate": null,
        "extensionDate": null,
        "pocOrganization": "Office/Organization",
        "pocLastName": "Last",
        "pocFirstName": "First",
        "pocEmail": "New@email.com",
        "pocPhoneNumber": "9998887777",
        "vulnerabilityDescription": "Test Risk Accepted",
        "mitigation": "Mitigations",
        "comments": "Comments",
        "resources": "Resources",
        "sourceIdentVuln": "Source Identifying Vulnerability",
        "securityChecks": null,
        "relevanceOfThreat": "Very Low",
        "likelihood": "Low",
        "impact": "Very Low",
        "impactDescription": "Impact Description",
        "residualRiskLevel": "Very Low",
        "recommendations": "Recommendations",
        "milestones": []
    }
}
```

POST	/api/systems/{systemId}/poams *Add one or many POA&M items in a system*

Sample Request Body

```
[
    {
        "externalUId": "Test External Id",
        "controlAcronym": "AC-1",
        "cci": "002107",
        "severity": "Low",
        "rawSeverity": "I",
        "status": "Ongoing",
        "scheduledCompletionDate": 1505915077,
        "completionDate": null,
        "pocOrganization": "Test Organization",
        "pocLastName": "Doe",
        "pocFirstName": "John",
        "pocEmail": "john.doe.ctr@mail.mil",
        "pocPhoneNumber": "555-555-5555",
        "vulnerabilityDescription": "Test Vulnerability Description",
        "mitigation": "Mitigation text.",
        "comments": "Comments text.",
        "resources": "Resources text.",
        "sourceIdentVuln": "Test Source Identifying Vulnerability",
        "securityChecks": "SV-12345_r1234,SV-12346_r1234",
        "recommendations": "Test Recommendations",
        "relevanceOfThreat": "High",
        "likelihood": "Moderate",
        "impact": "High",
        "impactDescription": "Impact Description text",
        "residualRiskLevel": "Moderate",
        "milestones": [
            {
                "description": "Description text.",
                "scheduledCompletionDate": 1505915077
            }
        ]
    }
]
```

PUT	**/api/systems/{systemId}/poams** *Update one or many POA&M items in a system*

Sample Request Body

```
[
    {
        "externalUId": "External Id",
        "controlAcronym": "AC-1",
        "cci": "002107",
        "severity": "Low",
        "rawSeverity": "I",
        "status": "Ongoing",
        "scheduledCompletionDate": 1509375108,
        "completionDate": null,
        "pocOrganization": "Test Organization",
        "pocLastName": "Doe",
        "pocFirstName": "John",
        "pocEmail": "john.doe.ctr@mail.mil",
        "pocPhoneNumber": "555-555-5555",
        "vulnerabilityDescription": "Test Vulnerability Description",
        "mitigation": "Test Mitigation",
        "comments": "Test Comments",
        "resources": "Test Resources",
        "sourceIdentVuln": "Test Source Identifying Vulnerability",
        "securityChecks": "SV-12345_r1234,SV-12346_r1234",
        "recommendations": "Test Recommendations",
        "relevanceOfThreat": "High",
        "likelihood": "Moderate",
        "impact": "High",
        "impactDescription": "Impact Description text",
        "residualRiskLevel": "Moderate",
        "milestones": [
            {
                "description": "Test Milestone Description",
                "scheduledCompletionDate": 1505915077,
                "isActive": true
            }
        ]
    }
]
```

Note: To prevent uploading duplicate/undesired milestones through the POA&M PUT you must include an “isActive” field for the milestone and set it to equal to false.

DELETE	**/api/systems/{systemId}/poams** *Remove one or many POA&M items in a system*

Sample Request Body

```
[
    {
        "poamId": 74
    }
]
```

4.7.1 POA&Ms Endpoints Fields

Field	**Type**	**Details**	**Associated Business Rule?**
systemId	Integer	[Required] Unique eMASS system identifier.	
poamId	Integer	[Required] Unique identifier representing the nth POAM item entered into the site's database.	
displayPoamId	Integer	[Required] Globally unique identifier for individual POA&M Items, seen on the front-end as "ID".	
isInherited	Boolean	[Read-Only] Indicates whether a POA&M Item is inherited.	
externalUid	String	[Optional] Unique identifier external to the eMASS application for use with associating POA&M Items. Character Limit = 100.	
controlAcronym	String	[Optional] Control acronym associated with the POA&M Item. NIST SP 800-53 Revision 4 defined.	
cci	String	[Optional] CCI associated with POA&M Item.	
status	String	[Required] Values include the following: • Ongoing • Risk Accepted • Completed • Not Applicable	✓
reviewStatus	String	[Read-Only] Values include the following options: • Not Approved • Under Review • Approved	✓

vulnerabilityDescription	String	[Required] Provide a description of the POA&M Item. Character Limit = 2,000.	
sourceIdentVuln	String	[Required] Include Source Identifying Vulnerability text. Character Limit = 2,000.	
securityChecks	String	[Optional] Security Checks that are associated with the POA&M.	
milestones	JSON	[Conditional] Please see Milestone Endpoint for more details.	
pocOrganization	String	[Required] Organization/Office represented. Character Limit = 100.	✓
pocFirstName	String	[Conditional] First name of POC. Character Limit = 100.	✓
pocLastName	String	[Conditional] Last name of POC. Character Limit = 100.	✓
pocEmail	String	[Conditional] Email address of POC. Character Limit = 100. If a POC email is supplied, the application will attempt to locate a user already registered within the application and pre-populate any information not explicitly supplied in the request. If no such user is found, these fields are required within the request.	✓
pocPhoneNumber	String	[Conditional] Phone number of POC. Character Limit = 100.	✓
severity	String	[Conditional] Required for approved items. Values include the following options:	

		• Very Low • Low • Moderate • High • Very High	
rawSeverity	String	[Optional] Values include the following options: • I • II • III	
resources	String	[Required] List of resources used. Character Limit = 250.	✓
relevanceOfThreat	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	
likelihood	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	
impact	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	
impactDescription	String	[Optional] Include description of Security Control’s impact.	
residualRiskLevel	String	[Optional] Values include the following options: • Very Low • Low • Moderate	

		• High • Very High	
recommendations	String	[Optional] Include recommendations. Character Limit = 2,000.	
scheduledCompletionDate	Date	[Conditional] Required for ongoing and completed POA&M items. Unix time format.	✓
completionDate	Date	[Conditional] Field is required for completed POA&M items. Unix time format.	✓
extensionDate	Date	[Read-Only] Value returned for a POA&M Item with review status “Approved” and has a milestone with a scheduled completion date that extends beyond the POA&M Item’s scheduled completion date.	
comments	String	[Conditional] Field is required for completed and risk accepted POA&M items. Character Limit = 2000.	✓
mitigation	String	[Optional] Include mitigation explanation. Character Limit = 2000.	✓
isActive	Boolean	[Conditional] Optionally used in PUT to prevent uploading new duplicate/undesired milestones. Include an “isActive” field for the milestone and set it to false to prevent creating a new milestone.	

4.8 MILESTONES ENDPOINTS

The Milestones endpoints provide the ability to view, add, update, and remove milestones that are associated with Plan of Action and Milestones (POA&M) items for a system.

GET	/api/systems/{systemId}/poams/{poamId}/milestones *Get milestones in one or many POA&M items in a system*

Available Query String Parameters

Name	Type	Example
scheduledCompletionDateStart	Date	1499644800
scheduledCompletionDateEnd	Date	1499990400

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "systemId": 27,
            "milestoneId": 89,
            "poamId": 74,
            "description": "Test Milestone Description 1",
            "scheduledCompletionDate": 1622234174.597,
            "reviewStatus": "Under Review"
        },
        {
            "systemId": 27,
            "milestoneId": 90,
            "poamId": 74,
            "description": "Test Milestone Description 2",
            "scheduledCompletionDate": 1622161400.033,
            "reviewStatus": "Not Approved"
        }
    ]
}
```

GET	/api/systems/{systemId}/poams/{poamId}/milestones/{milestoneId} *Get milestone by ID in POA&M item in a system*

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": {
        "systemId": 27,
        "milestoneId": 89,
        "poamId": 74,
        "description": "Test Milestone Description",
        "scheduledCompletionDate": 1622234174.597,
        "reviewStatus": "Not Approved"
    }
}
```

POST	/api/systems/{systemId}/poams/{poamId}/milestones *Add milestones to one or many POA&M items in a system*

Sample Request Body

```
[
    {
        "description": "Description text.",
        "scheduledCompletionDate": 1505919280
    }
]
```

PUT	/api/systems/{systemId}/poams/{poamId}/milestones *Update milestones in a system for one or many POA&M items*

Sample Request Body

```
[
    {
        "milestoneId": 20268,
        "description": "Description text edit.",
        "scheduledCompletionDate": 1505919280
    }
]
```

DELETE	**/api/systems/{systemId}/poams/{poamId}/milestones** *Remove milestones in a system for one or many POA&M items*

Sample Request Body

```
[
    {
        "milestoneId": 20268
    }
]
```

4.8.1 Milestones Endpoints Fields

Field	**Type**	**Details**	**Associated Business Rule?**
systemId	Integer	[Required] Unique system identifier.	
milestoneId	Integer	[Required] Unique milestone identifier.	
poamId	Integer	[Required] Unique POA&M item identifier.	
description	String	[Required] Provide a description of the milestone. Character Limit = 2,000.	
scheduledCompletionDate	Date	[Required] Unix date format.	✓

Note: Business rules associated with Milestones endpoints fields will be located within the POA&Ms Endpoints table in Appendix A.

4.9 ARTIFACTS ENDPOINTS

The Artifacts endpoints provide the ability to view, add, update, and remove artifacts (supporting documentation/evidence) and associated files for a system.

GET	/api/systems/{systemId}/artifacts *Get one or many artifacts in a system*

Available Query String Parameters

Name	Type	Example
filename	String	sample.pdf
controlAcronyms	String	AC-3,PM-6
ccis	String	000123,000069
systemOnly	Boolean	true, false

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "systemId": 27,
            "filename": "HardwareSoftwareFirmware.pdf",
            "isInherited": false,
            "description": "Test Hardware Software Firmware",
            "isTemplate": false,
            "type": "Diagram",
            "category": "Hardware Software Firmware Diagram",
            "refPageNumber": null,
            "controls": "AC-1",
            "ccis": "002107",
            "mimeContentType": "application/pdf",
            "fileSize": "369 KB",
            "artifactExpirationDate": 1622506488.4629998,
            "lastReviewedDate": null
        },
        {
            "systemId": 27,
            "filename": "RiskAssessment.pdf",
            "isInherited": false,
            "description": "Test E-Authentication Risk Assessment",
            "isTemplate": true,
            "type": "Document",
            "category": "E-Authentication Risk Assessment",
            "refPageNumber": "Test Ref Page Num 2",
            "controls": "IA-2,IA-8",
            "ccis": "000764",
            "mimeContentType": "application/pdf",
            "fileSize": "555 KB",
            "artifactExpirationDate": 1622506488.4629998,
            "lastReviewedDate": 1619914488.4629998
        }
    ]
}
```

POST	**/api/systems/{systemId}/artifacts** *Add one or many artifacts in a system*

Information

The body of a request through the Artifacts POST endpoint accepts a single binary file with extension ".zip" only. This .zip file should contain one or more files corresponding to existing artifacts or new artifacts that will be created upon successful receipt. Filename uniqueness within an eMASS system will be enforced by the API.

Upon successful receipt of a file, if a file within the .zip is matched via filename to an artifact existing within the application, the file associated with the artifact will be updated. If no artifact is matched via filename to the application, a new artifact will be created with the following default values. Any values not specified below will be null.

- isTemplate: false
- type: other
- category: evidence

To update values other than the file itself, please submit a PUT request.

PUT	**/api/systems/{systemId}/artifacts** *Update one or many artifacts in a system*

Sample Request Body

```
[
  {
    "filename": "AuthorizationGuidance.pdf",
    "isTemplate": true,
    "type": "Document",
    "category": "Evidence",
    "refPageNumber": "Page 100",
    "controls": "AC-1,AC-2",
    "ccis": "000005"
  }
]
```

DELETE	**/api/systems/{systemId}/artifacts** *Remove one or many artifacts in a system*

Sample Request Body

```
[
  {
    "filename": "AuthorizationGuidance.pdf"
  }
]
```

4.9.1 Artifacts Endpoints Fields

Field	**Type**	**Details**	**Associated Business Rule?**
filename	String	[Required] File name should match exactly one file within the provided zip file. Character Limit = 1,000.	✓
filename	Binary	[Required] Application/zip file. Max 30MB per artifact.	✓
systemId	Integer	[Required] Unique system identifier.	
isInherited	Boolean	[Read-Only] Indicates whether an artifact is inherited.	
isTemplate	Boolean	[Required] Indicates whether an artifact is a template.	✓
type	String	[Required] Values include the following options: • Procedure • Diagram • Policy • Labor • Document • Image • Other • Scan Result • Auditor Report May also accept custom artifact type values set by system administrators.	✓
category	String	[Required] Values include the following options: • Implementation Guidance • Evidence May also accept custom artifact category values set by system administrators.	✓
description	String	[Optional] Artifact description. Character Limit = 2,000.	✓

refPageNumber	String	[Optional] Artifact reference page number. Character Limit = 50.	
ccis	String	[Optional] CCIs associated with artifact.	
controls	String	[Optional] Control acronym associated with the artifact. NIST SP 800-53 Revision 4 defined.	
mimeContentType	String	[Read-Only] Standard MIME content type derived from file extension.	
fileSize	String	[Read-Only] File size of attached artifact.	
artifactExpirationDate	Date	[Optional] Date artifact expires and requires review. Unix date format.	
lastReviewDate	Date	[Optional] Date artifact was last reviewed. Unix date format.	✓

4.10 ARTIFACTS EXPORT ENDPOINT

The Artifacts Export endpoint provides the ability to download artifact files for a system.

GET	/api/systems/{systemId}/artifacts-export *Get the file of an artifact in a system*	
Available Query String Parameters		
Name	**Type**	**Example**
filename	String	**Required parameter.** sample.pdf
compress	Boolean	true, false
Sample Response		
Binary file associated with given filename. If "compress" parameter is specified, zip archive of binary file associated with given filename.		

4.11 PAC ENDPOINTS

The Package Approval Chain (PAC) endpoints provide the ability to view the status of existing workflows and initiate new workflows for a system.

Notes:

- If the indicated system has any active workflows, the response will include information such as the workflow type and the current stage of each workflow.
- If there are no active workflows, then a null data member will be returned.

GET	/api/systems/{systemId}/approval/pac *Get status of active workflows in a system*

Sample Response 1 – Active Workflow

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "workflow": "RMF Step 1: Security Category",
            "name": "Test Package Name",
            "currentStageName": "Submit Categorization",
            "currentStage": 2,
            "totalStages": 3,
            "daysAtCurrentStage": 0.2
        }
    ]
}
```

Sample Response 2 – No Active Workflow

```
{
    "meta": {
        "code": 200
    },
    "data": null
}
```

POST	/api/systems/{systemId}/approval/pac *Initiate system workflow for review*

Sample Request Body

```
[
    {
        "workflow": "Security Plan Approval",
        "name": "Test Package Name",
        "comments": "Test workflow initiation comments."
    }
]
```

4.11.1 PAC Endpoints Fields

Field	**Type**	**Details**	**Associated Business Rule?**
systemId	Integer	[Required] Unique system identifier.	
workflow	String	[Required] Values include the following: • Assess and Authorize • Assess Only • Security Plan Approval	
name	String	[Required] Package name. Character Limit = 100.	
currentStageName	String	[Read-Only] Name of the current stage in the active workflow.	
currentStage	Integer	[Read-Only] Number of the current stage in the active workflow.	
totalStages	Integer	[Read-Only] Total number of stages in the active workflow.	
comments	String	[Required] Comments submitted upon initiation of the indicated workflow. Character Limit = 4,000.	✓

4.12 CAC ENDPOINTS

The Control Approval Chain (CAC) endpoints provide the ability to view the status of Security Controls and submit them to the second stage in the Control Approval Chain.

Notes:

- POST requests will only yield successful results if the Security Control is at the first stage of the CAC. If the control is not at the first stage, an error will be returned.

GET	**/api/systems/{systemId}/approval/cac** *Get location of one or many controls in CAC*

Available Query String Parameters

Name	Type	Example
controlAcronyms	String	AC-3,PM-6

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "systemId": 27,
            "controlAcronym": "AC-1",
            "complianceStatus": "Not Applicable",
            "currentStageName": "Validator",
            "currentStage": 2,
            "totalStages": 2
        },
        {
            "systemId": 27,
            "controlAcronym": "AC-2",
            "complianceStatus": "Unassessed",
            "currentStageName": "ISO",
            "currentStage": 1,
            "totalStages": 2
        }
    ]
}
```

POST	**/api/systems/{systemId}/approval/cac** *Submit control to second stage of CAC*

Sample Request Body

```
[
    {
        "controlAcronym": "AC-2(1)",
        "comments": "Test control submission comments."
    }
]
```

4.12.1 CAC Endpoints Fields

Field	Type	Details	Associated Business Rule?
systemId	Integer	[Required] Unique system identifier.	
controlAcronym	String	[Required] Control acronym associated with the CAC. NIST SP 800-53 Revision 4 defined.	
complianceStatus	String	[Read-Only] Compliance status of the control.	
currentStageName	String	[Read-Only] Role in current stage.	
currentStage	Integer	[Read-Only] Current stage in the Control Approval Chain.	
totalStages	Integer	[Read-Only] Total number of stages in Control Approval Chain.	
comments	String	[Conditional] Character Limit = 10,000.	✓

4.13 CMMC ASSESSMENTS ENDPOINT

The Cybersecurity Maturity Model Certification (CMMC) Assessments endpoint provides the ability to view CMMC assessment information. It is available to CMMC eMASS only.

GET	**/api/cmmc-assessments** *Get CMMC assessment information*	
Available Query String Parameters		
Name	**Type**	**Example**
sinceDate	Date	**Required parameter.** Unix date format.
Sample Response (sinceDate=1611776337)		

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "operation": "UPDATED",
            "hqOrganizationName": "Umbrella Corporation",
            "uei": "9809123",
            "cageCodesInScope": "89ED9; 99D8B",
            "oscName": "UC Labs",
            "scope": "Non-Enterprise",
            "scopeDescription": "Assessment of UC's Lab",
            "awardedCMMCLevel": "Level 2",
            "expirationDate": 1682450360.0,
            "assessmentId": "41b89528-a7a8-470a-90f4-c3fd1267d6f7",
            "modelVersion": "1.12",
            "highestLevelOrderCageCode": "99D8B",
            "certificationUniqueId": "L20000003",
            "poam": true,
            "overallScore": 110,
            "oscAssessmentOfficialLastName": "Doe",
            "oscAssessmentOfficialFirstName": "John",
            "oscAssessmentOfficialEmail": "john.doe.ctr@mail.mil",
            "oscAssessmentOfficialTitle": null,
            "ssps": [
                {
                    "sspName": "UC Lab",
                    "sspVersion": "1.2",
                    "sspDate": 1449775097.707
                },
                {
                    "sspName": "AC Lab",
                    "sspVersion": "2.1",
                    "sspDate": 1578286800.0
                },
                {
                    "sspName": "UL Lab",
                    "sspVersion": "4.3.0",
                    "sspDate": 1589760000.0
                },
                {
                    "sspName": "FE Lab",
                    "sspVersion": "1.0",
                    "sspDate": 1627935145.983
                }
            ]
        },
        {
            "operation": "ADDED",
            "hqOrganizationName": "Test Labs",
            "uei": null,
            "cageCodesInScope": null,
            "oscName": "Test Engineering Systems",
            "scope": null,
            "scopeDescription": null,
            "awardedCMMCLevel": "Not Certified",
            "expirationDate": null,
            "assessmentId": null,
            "modelVersion": null,
            "highestLevelOrderCageCode": null,
            "certificationUniqueId": null,
            "poam": false,
            "overallScore": null,
            "oscAssessmentOfficialLastName": null,
            "oscAssessmentOfficialFirstName": null,
            "oscAssessmentOfficialEmail": null,
            "oscAssessmentOfficialTitle": null,
            "ssps": []
        }
    ]
}
```

4.13.1 CMMC Assessments Endpoint Fields

Field	Type	Details	Associated Business Rule?
operation	String	[Read-Only] Indicates the action that should be taken on the assessment record since the provided sinceDate. Values include the following options: • ADDED • UPDATED • DELETED	
hqOrganizationName	String	[Read-Only] The name of the DIB Company.	

uei	String	[Read-Only] The Unique Entity Identifier assigned to the DIB Company.	
cageCodesInScope	String	[Read-Only] The five position code(s) associated with the Organization Seeking Certification (OSC).	
oscName	String	[Read-Only] The name of the Organization Seeking Certification.	
scope	String	[Read-Only] The scope of the OSC assessment. Values include the following options: - Enterprise - Non-Enterprise	
scopeDescription	String	[Read-Only] Brief description of the scope of the OSC assessment.	
awardedCMMCLevel	String	[Read-Only] Values include the following options: - Not Certified - Level 1 - Level 2 - Level 3 - Level 4 - Level 5	
expirationDate	Date	[Read-Only] Expiration date of the awarded CMMC certification. Unix date format.	
assessmentId	String	[Read-Only] Unique identifier for the assessment/certificate. “41b89528-a7a8-470a-90f4-c3fd1267d6f7”	
modelVersion	String	[Read-Only] Version of the CMMC Model used as part of the assessment.	
highestLevelOrderCageCode	String	[Read-Only] Identifies the highest-level CAGE Code	

		associated with a given organization.	
certificationUniqueId	String	[Read-Only] Identifies the unique ID that is associated with a given CMMC certification for an organization.	
poam	Boolean	[Read-Only] Identifies whether any security requirements received a POA&M during the assessment.	
overallScore	Integer	[Read-Only] Identifies the overall calculated score for the assessment based on the assigned values to each applicable security requirement.	
oscAssessmentOfficialLastName	String	[Read-Only] Last name of the company official contracting with the C3PAO for the assessment.	
oscAssessmentOfficialFirstName	String	[Read-Only] First name of the company official contracting with the C3PAO for the assessment.	
oscAssessmentOfficialEmail	String	[Read-Only] Email of the company official contracting with the C3PAO for the assessment.	
oscAssessmentOfficialTitle	String	[Read-Only] Title of the company official contracting with the C3PAO for the assessment.	
sspName	String	[Read-Only] Name of the System Security Plan.	
sspVersion	String	[Read-Only] Version of the System Security Plan.	
sspDate	Date	[Read-Only] Date of the System Security Plan. Unix date format.	

4.14 STATIC CODE SCANS ENDPOINT

The Static Code Scans endpoint provides the ability to upload application scan findings into a system's assets module. Application findings can also be cleared from the system.

POST	/api/systems/{systemId}/static-code-scans *Upload static code scans*

Sample Request Body

```
[
    {
        "application": {
            "applicationName": "Artemis",
            "version": "Version 5.0"
        },
        "applicationFindings": [
            {
                "rawSeverity": "Critical",
                "codeCheckName": "Redundant Check",
                "count": 28,
                "scanDate": 1625070000,
                "cweId": "155"
            },
            {
                "rawSeverity": "Medium",
                "codeCheckName": "Hidden Field",
                "count": 54,
                "scanDate": 1625070000,
                "cweId": "125"
            }
        ]
    }
]
```

POST	/api/systems/{systemId}/static-code-scans *Clear static code scans*

Sample Request Body

```
[
    {
        "application": {
            "applicationName": "Artemis",
            "version": "Version 5.0"
        },
        "applicationFindings": [
            {
                "clearFindings": true
            }
        ]
    }
]
```

Note: To clear an application's findings, use only the field clearFindings and set it to true.

4.14.1 Static Code Scans Endpoint Fields

Field	**Type**	**Details**	**Associated Business Rule?**
applicationName	String	[Required] Name of the software application that was assessed.	
cweId	String	[Required] The Common Weakness Enumerator (CWE) identifier.	
clearFindings	Boolean	[Optional] When used by itself, can clear out all application findings for a single application/version pairing.	
codeCheckName	String	[Required] Name of the software vulnerability or weakness.	
count	Integer	[Required] Number of instances observed for a specified finding.	
rawSeverity	String	[Optional] Values include the following options: • Low • Medium • Moderate • High • Critical Note: In eMASS, values of "Critical" will appear as "Very High", and values of "Medium" will appear as "Moderate" Note: Any values not listed as options in the list above will map to "Unknown" and appear as blank values.	
scanDate	Date	[Required] Unix date format.	
version	String	[Required] The version of the application.	

4.15 WORKFLOW DEFINITIONS ENDPOINT

The Workflow Definitions endpoint provides the ability to view all workflow schemas available on the eMASS instance. Every transition for each workflow stage is included.

GET	/api/workflows/definitions *Get workflow definitions in a site*

Available Query String Parameters

Name	Type	Example
includeInactive	Boolean	true, false If no value is specified, the default returns false to not include outdated or disabled workflows.
registrationType	String	Accepts multiple comma-separated values including the following options: • assessAndAuthorize • assessOnly • guest • regular • functional • cloudServiceProvider • commonControlProvider For example: If the guest value is used, only workflows available to systems with a guest registration type will be returned.

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "workflowUid": "0ab0c7db-f985-4b98-a6f9-adc9cb245fed",
            "workflow": "RMF Step 1: Security Category",
            "version": 3,
            "description": "Initiate a workflow to complete, review,
                             and approve the system security
                             categorization for RMF Step 1.",
            "isActive": true,
            "stages": [
                {
                    "name": "Not Started",
                    "transitions": [
                        {
                            "endStage": "Categorize System",
                            "description": "Initiate Workflow",
                            "roles": [
                                "PM/ISO",
                                "System Admin",
                                "eMASS System Admin"
                            ]
                        }
                    ]
                },
                {
                    "name": "Categorize System",
                    "transitions": [
                        {
                            "endStage": "Submit Categorization",
                            "description": "Approve",
                            "roles": [
                                "PM/ISO",
                                "System Admin",
                                "eMASS System Admin",
                                "ISSE",
                                "ISSM",
                                "IO"
                            ]
                        },
                        {
                            "endStage": "Submit Categorization",
                            "description": "Disapprove and Move
                                            Forward",
                            "roles": [
                                "PM/ISO",
                                "System Admin",
                                "eMASS System Admin",
                                "ISSE",
                                "ISSM",
                                "IO"
                            ]
                        },
                        {
                            "endStage": "Cancelled",
                            "description": "Cancel",
                            "roles": [
                                "PM/ISO",
                                "System Admin",
                                "eMASS System Admin",
                                "ISSE",
                                "ISSM",
                                "IO"
                            ]
                        }
                    ]
                },
                {
                    "name": "Submit Categorization",
                    "transitions": [
                        ...
                    ]
                },
                {
                    "name": "Approval",
                    "transitions": [
                        ...
                    ]
                },
                {
                    "name": "Complete",
                    "transitions": [
                        {
                            "endStage": "Complete",
                            "description": "Approve",
                            "roles": [
                                ...
                            ]
                        },
                        {
                            "endStage": "Complete",
                            "description": "Deny",
                            "roles": [
                                ...
                            ]
                        }
                    ]
                },
                {
                    "name": "Cancelled",
                    "transitions": []
                }
            ]
        },
        ...
    ]
}
```

Note: Ellipses (...) were used to shorten the example output for simplicity.

4.15.1 Workflow Definitions Endpoint Fields

Field	Type	Details	Associated Business Rule?
description	String	[Read-Only] Description of the workflow or the stage transition.	
endStage	String	[Read-Only] The landing stage that is active after performing a transition.	
isActive	String	[Read-Only] Returns true if the workflow is available to the site. Note: Unless using the includeInactive parameter, workflow definitions set to false for isActive will be excluded.	

		Note: If an admin disables the workflow in the Administration module, it will be set to false for isActive. Note: If a workflow definition is updated, all prior versions will automatically be set to false for isActive.	
name	String	[Read-Only] Name of the workflow stage. Note: For older workflows, this will match the user assigned to the stage.	
version	Integer	[Read-Only] Version of the workflow definition.	
workflow	String	[Read-Only] The workflow type.	
workflowUid	String	[Read-Only] Unique workflow definition identifier. Note: Unique for the workflow & version (ex. POA&M Approval, version 2).	

4.16 WORKFLOW INSTANCES ENDPOINT

The Workflow Instances endpoint provides the ability to view detailed information on all active and historical workflows for an eMASS instance.

GET	/api/workflows/instances *Get workflow instances in a site*	
Available Query String Parameters		
Name	**Type**	**Example**
includeComments	Boolean	true, false If no value is specified, the default returns true to include transition comments. Note: Corresponds to the Comments textbox that is required at most workflow transitions. Does not include other text input fields such as Terms / Conditions for Authorization.
pageIndex	Integer	If no value is specified, the default returns results from the first page with an index of 0. Note: Pages contain 1000 workflow instances.
sinceDate	Date	Unix Date format. Note: Filters off the lastEditedDate field. Note: The authorization/assessment decisions on completed workflows can be edited for up to 30 days after the initial decision is made.
status	String	Values include the following options: • active • inactive • all If no value is specified, the default returns all to include both active and inactive workflows. Note: Any workflows at a current stage of Complete or Canceled are inactive. Legacy workflows with a current stage of Authorized, Approved, or Denied are also inactive. Ongoing workflows currently at other stages are active.
Sample Response (sinceDate=1631130832)		

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "workflowUid": "0ab0c7db-f985-4b98-a6f9-adc9cb245fed",
            "systemId": 13,
            "systemName": "John A&A System 1",
            "workflowInstanceId": 28,
            "packageName": "Test RMF Step 1 package",
            "createdDate": 1630428572.36,
            "lastEditedDate": 1631130837.303,
            "lastEditedBy": "john.doe.ctr@mail.mil",
            "workflow": "RMF Step 1: Security Category",
            "version": 1,
            "currentStage": "Complete",
            "transitions": [
                {
                    "description": "Approve",
                    "startStage": "Approval",
                    "endStage": "Complete",
                    "comments": "Approved the categorization.",
                    "createdDate": 1631130837.303,
                    "createdBy": "john.doe.ctr@mail.mil"
                },
                {
                    "description": "Approve",
                    "startStage": "Submit Categorization",
                    "endStage": "Approval",
                    "comments": "Submitted the categorization.",
                    "createdDate": 1631130832.3969998,
                    "createdBy": "john.doe.ctr@mail.mil"
                },
                {
                    "description": "Approve",
                    "startStage": "Categorize System",
                    "endStage": "Submit Categorization",
                    "comments": "Categorized the system as HMM.",
                    "createdDate": 1630443388.583,
                    "createdBy": "john.doe.ctr@mail.mil"
                },
                {
                    "description": "Initiate Workflow",
                    "startStage": "Not Started",
                    "endStage": "Categorize System",
                    "comments": null,
                    "createdDate": 1630428572.53,
                    "createdBy": "john.doe.ctr@mail.mil"
                }
            ]
        },
        {
            "workflowUid": "6f810301-5b3b-4f89-81e7-587fef9142a9",
            "systemId": 14,
            "systemName": "John A&A System 2",
            "workflowInstanceId": 123,
            "packageName": "Test POA&M Approval",
            "createdDate": 1636124623.4429998,
            "lastEditedDate": 1636124641.1629999,
            "lastEditedBy": "john.doe.ctr@mail.mil",
            "workflow": "POA&M Approval",
            "version": 3,
            "currentStage": "Echelon II",
            "transitions": [
                {
                    "description": "Submit New Package",
                    "startStage": "PM/ISO",
                    "endStage": "Echelon II",
                    "comments": "Selected POA&M Items.",
                    "createdDate": 1636124641.1629999,
                    "createdBy": "john.doe.ctr@mail.mil"
                },
                {
                    "description": "Initiate Workflow",
                    "startStage": "Not Started",
                    "endStage": "PM/ISO",
                    "comments": null,
                    "createdDate": 1636124623.633,
                    "createdBy": "john.doe.ctr@mail.mil"
                }
            ]
        }
    ],
    "pagination": {
        "totalCount": 12,
        "totalPages": 1,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

GET	/api/workflows/instances/{workflowInstanceId} *Get workflow instance by ID*

Available Query String Parameters

Name	Type	Example

Sample Response

```
{
    "meta": {
        "code": 200
    },
    "data": {
        "workflowUid": "6f810301-5b3b-4f89-81e7-587fef9142a9",
        "systemName": "John A&A System",
        "workflowInstanceId": 123,
        "packageName": "Test POA&M Approval",
        "createdDate": 1636124623.4429998,
        "lastEditedDate": 1636124641.1629999,
        "lastEditedBy": "john.doe.ctr@mail.mil",
        "workflow": "POA&M Approval",
        "version": 3,
        "currentStage": "Echelon II",
        "transitions": [
            {
                "description": "Submit New Package",
                "startStage": "PM/ISO",
                "endStage": "Echelon II",
                "comments": "Selected POA&M Items.",
                "createdDate": 1636124641.1629999,
                "createdBy": "john.doe.ctr@mail.mil"
            },
            {
                "description": "Initiate Workflow",
                "startStage": "Not Started",
                "endStage": "PM/ISO",
                "comments": null,
                "createdDate": 1636124623.633,
                "createdBy": "john.doe.ctr@mail.mil"
            }
        ]
    }
}
```

4.16.1 Workflow Instances Endpoint Fields

Field	**Type**	**Details**	**Associated Business Rule?**
comments	String	[Read-Only] Comments entered by the user when performing the transition.	
createdBy	String	[Read-Only] User that performed the workflow transition.	
createdDate	Date	[Read-Only] Date the workflow instance or the workflow transition was created.	
currentStage	String	[Read-Only] Name of the current stage.	
description	String	[Read-Only] Description of the stage transition. This matches the action dropdown that appears for PAC users.	
endStage	String	[Read-Only] The landing stage that is active after performing a transition.	
lastEditedBy	String	[Read-Only] User that last acted on the workflow.	
lastEditedDate	Date	[Read-Only] Date the workflow was last acted on.	
packageName	String	[Read-Only] The package name.	
startStage	String	[Read-Only] The beginning stage that is active before performing a transition.	

systemId	String	[Read-Only] Unique system identifier.	
systemName	String	[Read-Only] The system name.	
version	Integer	[Read-Only] Version of the workflow definition.	
workflow	String	[Read-Only] The workflow type.	
workflowInstanceId	Integer	[Read-Only] Unique workflow instance identifier.	
workflowUid	String	[Read-Only] Unique workflow definition identifier. Note: Unique for the workflow & version (ex. POA&M Approval, version 2).	

4.17 CLOUD RESOURCE RESULTS ENDPOINT

The Cloud Resource Results endpoint provides the ability to add, update, and remove cloud resources and their scan results in the assets module for a system.

POST	/api/systems/{systemId}/cloud-resource-results *Add one or many cloud resources and their scan results*

Sample Request Body

```
[
    {
        "provider": "azure",
        "resourceId":
                      "/subscriptions/123456789/sample/resource/names
                      pace/default",
        "resourceName": "Storage Resource",
        "resourceType": "Microsoft.storage.table",
        "initiatedBy": "john.doe.ctr@mail.mil",
        "cspAccountId": "123456789",
        "cspRegion": "useast2",
        "isBaseline": true,
        "tags": {
            "test": "testtag"
        },
        "complianceResults": [
            {
                "cspPolicyDefinitionId":
                                         "/providers/sample/policy/nam
                                         espace/au11_policy",
                "policyDefinitionTitle": "AU-11 - Audit Record
                                         Retention",
                "complianceCheckTimestamp": 1644003780,
                "isCompliant": false,
                "control": "AU-11",
                "assessmentProcedure": "000167,000168",
                "complianceReason": "retention period not configured",
                "policyDeploymentName": "testDeployment",
                "policyDeploymentVersion": "1.0.0",
                "severity": "High"
            }
        ]
    }
]
```

4.17.1 Cloud Resource Results Endpoint Fields

Field	**Type**	**Details**	**Associated Business Rule?**
assessmentProcedure	String	[Optional] Comma separated correlation to Assessment Procedure (i.e. CCI number for DoD Control Set). Character Limit = 100.	
complianceCheckTimestamp	Date	[Optional] Unix date format.	
complianceReason	String	[Optional] Reason/comments for compliance result. Character Limit = 1,000.	
control	String	[Optional] Comma separated correlation to Security Control (e.g. exact NIST Control acronym). Character Limit = 100.	
cspAccountId	String	[Optional] System/owner's CSP account ID/number. Character Limit = 100.	
cspPolicyDefinitionId	String	[Required] Unique identifier/compliance namespace for CSP/Resource's policy definition/compliance check. Character Limit = 500.	
cspRegion	String	[Optional] CSP region of system. Character Limit = 100.	
initiatedBy	String	[Optional] Email of POC. Character Limit = 100.	
isBaseline	Boolean	[Optional] True/false flag for providing results as baseline. If true, all existing compliance results for the resourceId will be replaced by results in the current call.	
isCompliant	Boolean	[Required] Compliance status of the policy for the identified cloud resource.	
policyDefinitionTitle	String	[Required] Friendly policy/compliance check title. Recommend short title.	

		Character Limit = 2,000.	
policyDeploymentName	String	[Optional] Name of policy deployment. Character Limit = 500.	
policyDeploymentVersion	String	[Optional] Version of policy deployment. Character Limit = 50.	
provider	String	[Required] Cloud service provider name. Character Limit = 100.	
resourceId	String	[Required] Unique identifier/resource namespace for policy compliance result. Character Limit = 500.	
resourceName	String	[Required] Friendly name of Cloud resource. Character Limit = 500.	
resourceType	String	[Required] Type of Cloud resource. Character Limit = 100.	
severity	String	[Optional] Values include the following options: • Low • Medium • High • Critical	
tags	String	[Optional] Informational tags associated to results for other metadata.	

4.18 CONTAINER SCAN RESULTS ENDPOINT

The Container Scan Results endpoint provides the ability to add, update, and remove containers and their scan results in the assets module for a system.

POST	/api/systems/{systemId}/container-scan-results *Add one or many containers and their scan results*

Sample Request Body

```
[
    {
        "containerId": "command-control",
        "containerName": "command-control",
        "podName": "command-control-955596ffc",
        "podIp": "1.1.1.101",
        "namespace": "command-control",
        "time": 1648217219,
        "tags": {
            "test": "test"
        },
        "benchmarks": [
            {
                "benchmark": "RHEL_8_STIG",
                "isBaseline": false,
                "results": [
                    {
                        "ruleId": "SV-230221r743913_rule",
                        "status": "pass",
                        "lastSeen": 1648217219,
                        "message": "test message"
                    },
                    {
                        "ruleId": "SV-230222r627750_rule",
                        "status": "pass",
                        "lastSeen": 1648217219,
                        "message": ""
                    },
                    {
                        "ruleId": "SV-230223r627750_rule",
                        "status": "fail",
                        "lastSeen": 1648217219,
                        "message": ""
                    },
                    {
                        "ruleId": "SV-230224r627750_rule",
                        "status": "fail",
                        "lastSeen": 1648217219,
                        "message": ""
                    }
                ]
            }
        ]
    }
]
```

4.18.1 Container Scan Results Endpoint Fields

Field	Type	Details	Associated Business Rule?
benchmark	String	[Required] Identifier of the benchmark/grouping of compliance results. (e.g. for STIG results, provide the benchmark id for the STIG technology). Character Limit = 100.	
containerId	String	[Required] Unique identifier of the container. Character Limit = 500.	
containerName	String	[Required] Friendly name of the container. Character Limit = 500.	
isBaseline	Boolean	[Optional] True/false flag for providing results as baseline. If true, all existing compliance results for the provided *benchmark* within the *container* will be replaced by results in the current call.	
lastSeen	Date	[Required] Unix date format.	
message	String	[Optional] Comments for the result. Character Limit = 1,000.	
namespace	String	[Optional] Namespace of container in container orchestration (e.g. Kubernetes namespace). Character Limit = 100.	
podIp	String	[Optional] IP address of pod (e.g. Kubernetes assigned IP) Character Limit = 100.	
podName	String	[Optional] Name of pod (e.g. Kubernetes pod). Character Limit = 100.	
ruleId	String	[Required] Identifier for the compliance result, vulnerability, etc. the result is for. (e.g. for STIGs, use the SV-XXXrXX identifier; for CVEs, the CVE-XXXX-XXX identifier, etc.).	

status	String	[Required] Values include the following options: • Pass • Fail • Other • Not Reviewed • Not Checked • Not Applicable	
tags	String	[Optional] Informational tags associated to results for other metadata.	
time	Date	[Required] Datetime of scan/result. Unix date format.	

4.19 DASHBOARDS ENDPOINTS

The Dashboards endpoints provide the ability to view data contained in dashboard exports. In the eMASS front end, these dashboard exports are generated as Excel exports.

The following reference is provided as an example only and may not be the exact fields. Each dashboard dataset available from the API is automatically updated with the current configuration of the dashboard and the instance of eMASS as the dashboard changes.

Organization-specific fields may differ. Organization-specific Dashboards should only be used by that organization (e.g., VA [dashboard name] should be used by VA).

Dashboard Quick Reference

4.19.1 System Status Details

GET	**/api/dashboards/system-status-details** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-status-details?orgId=1&pageIndex=0" -H
"api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	**Type**	**Example/Details**
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization Name": "Test Org",
            "Organization Hierarchy": "Army > Test Org",
            "System Acronym": "John A&A System",
            "System Name": "John Assess and Authorize System",
            "System ID": "4",
            "Version / Release Number": "5.10.1.0",
            "Registration Completion Date": "1655489975",
            "Registration Type": "Assess and Authorize",
            "System Type": "IS Major Application",
            "Special Type": "-",
            "Special Type Description": "-",
            "DITPR ID": "1234",
            "Highest System Data Classification": "-",
            "System Policy": "RMF",
            "National Security System": "No",
            "Financial Management System": "No",
            "Reciprocity System": "Yes",
            "Cloud Computing": "No",
            "Public Facing Component / Presence": "-",
            "Controlled Unclassified Information (CUI)": "-",
            "Personally Identifiable Information (PII)": "-",
            "Protected Health Information (PHI)": "-",
            "Mission Criticality": "-",
            "Governing Mission Area": "-",
            "Mission Portfolio": "-",
            "MAC": "-",
            "DoD Confidentiality": "-",
            "Confidentiality": "Moderate",
            "Integrity": "Moderate",
            "Availability": "Moderate",
            "Impact": "Moderate",
            "Applied Overlays": "-",
            "Lifecycle/Acquisition Phase": "Pre-Milestone A (Material
                                            Solution Analysis)",
            "Need Date": "-",
            "Authorization Status": "Not Yet Authorized",
            "Authorization Date": "-",
            "ATD": "-",
            "Terms / Conditions for Authorization": "-",
            "Overall Risk Score": "-",
            "Days to ATD": "-",
            "Current AO": "-",
            "RMF Activity": "Initiate and plan cybersecurity
                             Assessment Authorization",
            "Package Type": "-",
            "Package Created": "-",
            "Location in PAC": "Not Yet Initiated",
            "Package Days at Role": "-",
            "Days to Annual Review": "-",
            "ATC Decision": "-",
            "ATC Decision Date": "-",
            "ATC Termination Date": "-",
            "Reported Policy": "RMF",
            "Reported Authorization Status": "Not Yet Authorized",
            "Reported Authorization Date": "-",
            "Reported ATD": "-",
            "Days to Reported ATD": "-"
        },
        {
            "Organization Name": "Army",
            "Organization Hierarchy": "Army",
            "System Acronym": "Jane A&A System",
            "System Name": "Jane Assess & Authorize System",
            "System ID": "5",
            "Version / Release Number": "1.0",
            "Registration Completion Date": "1657738026",
            "Registration Type": "Assess and Authorize",
            "System Type": "IS Major Application",
            "Special Type": "-",
            "Special Type Description": "-",
            "DITPR ID": "TBD",
            "Highest System Data Classification": "Secret",
            "System Policy": "RMF",
            "National Security System": "No",
            "Financial Management System": "No",
            "Reciprocity System": "Yes",
            "Cloud Computing": "No",
            "Public Facing Component / Presence": "-",
            "Controlled Unclassified Information (CUI)": "-",
            "Personally Identifiable Information (PII)": "No",
            "Protected Health Information (PHI)": "No",
            "Mission Criticality": "-",
            "Governing Mission Area": "-",
            "Mission Portfolio": "-",
            "MAC": "-",
            "DoD Confidentiality": "-",
            "Confidentiality": "Moderate",
            "Integrity": "Moderate",
            "Availability": "Moderate",
            "Impact": "Moderate",
            "Applied Overlays": "-",
            "Lifecycle/Acquisition Phase": "Post-Milestone C
                                            (Production and
                                            Deployment)",
            "Need Date": "-",
            "Authorization Status": "Authorization to Operate (ATO-
                                    ConMon)",
            "Authorization Date": "1659373591",
            "ATD": "1690909592",
            "Terms / Conditions for Authorization": "asdf",
            "Overall Risk Score": "Low",
            "Days to ATD": "351",
            "Current AO": " Smith, John",
            "RMF Activity": "Initiate and plan cybersecurity
                             Assessment Authorization",
            "Package Type": "POA&M Approval; Change Request",
            "Package Created": "(POA&M Approval) 13-Jul-2022; (Change
                                Request) 29-Jul-2022",
            "Location in PAC": "(POA&M Approval) ISO/PM; (Change
                                Request) ISO/PM",
            "Package Days at Role": "(POA&M Approval) 13.0; (Change
                                     Request) 17.3",
            "Days to Annual Review": "351",
            "ATC Decision": "-",
            "ATC Decision Date": "-",
            "ATC Termination Date": "-",
            "Reported Policy": "RMF",
            "Reported Authorization Status": "Authorization to Operate
                                              (ATO-ConMon)",
            "Reported Authorization Date": "1659373591",
            "Reported ATD": "1690909592",
            "Days to Reported ATD": "351"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.2 System Control Compliance Summary

GET	/api/dashboards/system-control-compliance-summary *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-control-compliance-
summary?orgId=1&pageIndex=0" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "Test Org",
            "Organization Hierarchy": "USN > Test Org",
            "System Acronym": "John A&A System",
            "System Name": "John Assess & Authorize System",
            "System ID": "1",
            "Registration Completion Date": "1647639989",
            "Policy": "RMF",
            "Registration Type": "Assess and Authorize",
            "System Type": "IS Major Application",
            "Impact": "Moderate",
            "Authorization Status": " Authorization to Operate (ATO)",
            "Not Applicable Controls": "0",
            "Compliant Controls": "5",
            "Non-Compliant Controls": "2",
            "Unassessed Controls": "413",
            "Non-Compliant Red Criticality Controls": "0",
            "Non-Compliant Yellow Criticality Controls": "1",
            "Non-Compliant White Criticality Controls": "1",
            "Implementation Plan: Implemented Controls": "0",
            "Implementation Plan: Planned Controls": "417",
            "Implementation Plan: Not Applicable Controls": "0",
            "Implementation Plan: Inherited Controls": "2",
            "Implementation Plan: Manually Inherited Controls": "1",
            "Implementation Plan: Not Implemented Controls": "0",
            "Implementation Plan: Compensated Controls": "0"
        },
        {
            "Organization": "USN",
            "Organization Hierarchy": "USN",
            "System Acronym": "Jane Guest System",
            "System Name": "Jane Guest System",
            "System ID": "2",
            "Registration Completion Date": "1648063729",
            "Policy": "RMF",
            "Registration Type": "Guest",
            "System Type": "IS Major Application",
            "Impact": "Low",
            "Authorization Status": "EXPIRED",
            "Not Applicable Controls": "0",
            "Compliant Controls": "0",
            "Non-Compliant Controls": "0",
            "Unassessed Controls": "1",
            "Non-Compliant Red Criticality Controls": "0",
            "Non-Compliant Yellow Criticality Controls": "0",
            "Non-Compliant White Criticality Controls": "0",
            "Implementation Plan: Implemented Controls": "0",
            "Implementation Plan: Planned Controls": "1",
            "Implementation Plan: Not Applicable Controls": "0",
            "Implementation Plan: Inherited Controls": "0",
            "Implementation Plan: Manually Inherited Controls": "0",
            "Implementation Plan: Not Implemented Controls": "0",
            "Implementation Plan: Compensated Controls": "0"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.3 System Security Controls Details

GET	/api/dashboards/system-security-controls-details *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-security-controls-details?orgId=1&pageIndex=0" -H "api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "USN",
            "System ID": "1",
            "System Name": "John Assess & Authorize System",
            "System Acronym": "John A&A System",
            "System Type": "IS Major Application",
            "Control": "AC-1",
            "Name": "Access Control Policy And Procedures",
            "Criticality": "White",
            "Security Control Designation": "Common",
            "Test Method": "-",
            "Implementation Status": "Inherited",
            "Implementation Narrative": "-",
            "N/A Justification": "-",
            "Compliance Status": "Compliant",
            "Estimated Completion Date": "-",
            "Severity": "-",
            "Relevance of Threat": "-",
            "Likelihood": "-",
            "Impact": "-",
            "Residual Risk Level": "-",
            "Recommended Residual Risk Level": "-",
            "Attached Evidence": "No",
            "Inherited": "Yes",
            "Inherited Status": "Inherited",
            "Inheritable Status": "Inheritable",
            "Revalidation Date": "Unspecified",
            "Days to Revalidation": "N/A"
        },
        {
            "Organization": "USN",
            "System ID": "1",
            "System Name": "John Assess & Authorize System",
            "System Acronym": "John A&A System",
            "System Type": "IS Major Application",
            "Control": "AC-2",
            "Name": "Account Management",
            "Criticality": "Yellow",
            "Security Control Designation": "Hybrid",
            "Test Method": "-",
            "Implementation Status": "Manually Inherited",
            "Implementation Narrative": "-",
            "N/A Justification": "-",
            "Compliance Status": "Non-Compliant",
            "Estimated Completion Date": "1653329494",
            "Severity": "Very Low",
            "Relevance of Threat": "Very High",
            "Likelihood": "Very High",
            "Impact": "Moderate",
            "Residual Risk Level": "Moderate",
            "Recommended Residual Risk Level": "Moderate",
            "Attached Evidence": "Yes",
            "Inherited": "Yes",
            "Inherited Status": "Hybrid",
            "Inheritable Status": "Not Provided",
            "Revalidation Date": "Unspecified",
            "Days to Revalidation": "N/A"
        }
    ],
    "pagination": {
        "totalCount": 17964,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.4 System Assessment Procedures Details

GET	**/api/dashboards/system-assessment-procedures-details** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-assessment-procedures-details?orgId=1"
-H "api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	**Type**	**Example**
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.

pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "USN",
            "System ID": "1",
            "System Name": "John Assess & Authorize System",
            "System Acronym": "John A&A System",
            "System Type": "IS Major Application",
            "Control": "AC-1",
            "Name": "Access Control Policy And Procedures",
            "AP Acronym": "AC-1.1",
            "CCI Number": "002107",
            "CCI Definition": "The organization defines the personnel
                               or roles to be recipients of the
                               access control policy necessary to
                               facilitate the implementation of the
                               access control policy and associated
                               access controls.",
            "Procedure": "The organization being inspected/assessed is
                          automatically compliant with this CCI
                          because they are covered at the DoD level.
                          DoD has defined the personnel or roles as
                          all personnel.",
            "Implementation Guidance": "DoD has defined the personnel
                                        or roles as all personnel.",
            "Recommended Compelling Evidence": "Automatically
                                                compliant",
            "Source": "John CCP",
            "Compliance Status": "Compliant",
            "Date Tested": "1652292687",
            "Tested By": "John Smith",
            "Test Results": "C",
            "Type": "Self-Assessment",
            "Created By": "Smith, John",
            "Created Date": "1652292688",
            "Attached Evidence": "No",
            "Inherited": "Yes",
            "Inherited Status": "Inherited",
            "Inheritable Status": "Not Provided"
        },
        {
            "Organization": "USN",
            "System ID": "1",
            "System Name": "John Assess & Authorize System",
            "System Acronym": "John A&A System",
            "System Type": "IS Major Application",
            "Control": "AC-1",
            "Name": "Access Control Policy And Procedures",
            "AP Acronym": "AC-1.2",
            "CCI Number": "002108",
            "CCI Definition": "The organization defines the personnel
                               or roles to be recipients of the
                               procedures necessary to facilitate the
                               implementation of the access control
                               policy and associated access
                               controls.",
            "Procedure": "The organization being inspected/assessed is
                          automatically compliant with this CCI
                          because they are covered at the DoD level.
                          DoD has defined the personnel or roles as
                          all personnel.",
            "Implementation Guidance": "DoD has defined the personnel
                                        or roles as all personnel.",
            "Recommended Compelling Evidence": "Automatically
                                                compliant",
            "Source": "John CCP",
            "Compliance Status": "Compliant",
            "Date Tested": "1652292687",
            "Tested By": "John Smith",
            "Test Results": "C",
            "Type": "Self-Assessment",
            "Created By": "Smith, John",
            "Created Date": "1652292688",
            "Attached Evidence": "No",
            "Inherited": "Yes",
            "Inherited Status": "Inherited",
            "Inheritable Status": "Not Provided"
        }
    ],
    "pagination": {
        "totalCount": 69764,
        "totalPages": 4,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": "[URL]/api/dashboards/system-assessment-
                        procedures-
                        details?orgid=1&pageIndex=1&pageSize=20000"
```

4.19.5 System POA&M Summary

GET	**/api/dashboards/system-poam-summary** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-poam-summary?orgId=1&pageIndex=0" -H
"api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
excludeInherited	Boolean	true, false If no value is specified, the default returns false to include inherited data.
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "USN",
            "System Acronym": "John Import",
            "System Name": "John Import",
            "System ID": "99",
            "Registration Completion Date": "1654194808",
            "Policy": "RMF",
            "System Type": "IS Major Application",
            "Authorization Status": "Authorization to Operate (ATO)",
            "Ongoing POA&M Items": "3",
            "Risk Accepted POA&M Items": "1",
            "Overdue POA&M Items": "3",
            "Completed POA&M Items": "1",
            "Low or Very Low Residual Risk POA&M Items": "2",
            "Moderate Residual Risk POA&M Items": "0",
            "High or Very High Residual Risk POA&M Items": "0",
            "Low or Very Low Severity POA&M Items": "5",
            "Moderate Severity POA&M Items": "0",
            "High or Very High Severity POA&M Items": "0",
            "Unassigned Residual Risk POA&M Items": "3",
            "Unassigned Severity POA&M Items": "0"
        },
        {
            "Organization": "NAVSEA",
            "System Acronym": "Jane NNPI Test 6",
            "System Name": "Jane NNPI Test 6",
            "System ID": "40",
            "Registration Completion Date": "1650563063",
            "Policy": "RMF",
            "System Type": "IS Major Application",
            "Authorization Status": "Not Yet Authorized",
            "Ongoing POA&M Items": "1077",
            "Risk Accepted POA&M Items": "41",
            "Overdue POA&M Items": "1077",
            "Completed POA&M Items": "0",
            "Low or Very Low Residual Risk POA&M Items": "123",
            "Moderate Residual Risk POA&M Items": "876",
            "High or Very High Residual Risk POA&M Items": "115",
            "Low or Very Low Severity POA&M Items": "123",
            "Moderate Severity POA&M Items": "876",
            "High or Very High Severity POA&M Items": "115",
            "Unassigned Residual Risk POA&M Items": "4",
            "Unassigned Severity POA&M Items": "4"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.6 System POA&M Details

GET	**/api/dashboards/system-poam-details** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-poam-details?orgId=1&pageIndex=0" -H
"api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
excludeInherited	Boolean	true, false If no value is specified, the default returns false to include inherited data.

orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "USN",
            "System ID": "1",
            "System Name": "John Assess & Authorize System",
            "System Acronym": "John A&A System",
            "System Type": "IS Major Application",
            "Policy": "RMF",
            "ID": "1010032150",
            "POA&M URL":
                       "[URL]/App/CA/DisplayVulnerability/1010032150",
            "Control/AP": "AC-17(2).1",
            "Control Title": "Protection Of Confidentiality /
                             Integrity Using Encryption",
            "Control Criticality": "Yellow",
            "Control Implementation Status": "Planned",
            "POA&M Item Status": "Completed",
            "POA&M Item Review Status": "Approved",
            "Scheduled Completion Date": "1653067732",
            "Pending Extension Date": "-",
            "Extension Date": "-",
            "Completion Date": "1653067829",
            "Security Checks": "SV-96481r1_rule",
            "Vulnerability Description": "Failed scan or manual review
                                         for: [SV-96481r1_rule
                                         (Moderate) - Apple iOS must
                                         not include applications
                                         with the following
                                         characteristics: Siri when
                                         the device is locked. (1)
                                         resource affected].",
            "Devices Affected": "Test Devices",
            "Predisposing Conditions": "Test Conditions",
            "Raw Severity": "II",
            "Severity": "Very Low",
            "Relevance Of Threat": "Very Low",
            "Threat Descriptions": "Test Threat",
            "Likelihood": "Very Low",
            "Recommended Likelihood": "Very Low",
            "Impact": "Very Low",
            "Impact Description": "Test Impact",
            "Residual Risk": "Very Low",
            "Recommended Residual Risk": "Very Low",
            "Mitigations": "Test Mitigations",
            "Resulting Residual Risk Level after Proposed
             Mitigations": "Very Low",
            "Recommendations": "Test Recommendations",
            "Source Identifying Vulnerability": "Identified by DISA
                                                 STIG Viewer: CMRS
                                                 manual review on 06-
                                                 May-2022.",
            "Resources": "Test Resources",
            "Comments": "[SV-96481r1_rule failed on Apple iOS 12]. ",
            "Artifact Attachments": "1",
            "POC": "John Smith",
            "Source": "Not Inherited",
            "Created Date": "1653067732",
            "Last Modified Date": "1653067828",
            "Modified By": "Smith, John",
            "Latest Milestone Description": "Test Milestone",
            "Milestone Scheduled Completion Date": "1653067732",
            "Milestone Created Date": "1653067732",
            "Milestone Review Status": "Approved"
        },
        {
            "Organization": "NAVSEA",
            "System ID": "40",
            "System Name": "Jane Assess and Authorize Test ",
            "System Acronym": "Jane A&A Test",
            "System Type": "IS Major Application",
            "Policy": "RMF",
            "ID": "1010032193",
            "POA&M URL":
                       "[URL]/App/CA/DisplayVulnerability/1010032193",
            "Control/AP": "System",
            "Control Title": "-",
            "Control Criticality": "-",
            "Control Implementation Status": "-",
            "POA&M Item Status": "Ongoing",
            "POA&M Item Review Status": "Under Review",
            "Scheduled Completion Date": "1614793549",
            "Pending Extension Date": "-",
            "Extension Date": "-",
            "Completion Date": "-",
            "Security Checks": "SV-84993r1_rule",
            "Vulnerability Description": "At least one tester must be
                                          designated to test for
                                          security flaws in addition
                                          to functional testing.",
            "Devices Affected": "-",
            "Predisposing Conditions": "-",
            "Raw Severity": "-",
            "Severity": "Moderate",
            "Relevance Of Threat": "Moderate",
            "Threat Descriptions": "-",
            "Likelihood": "Moderate",
            "Recommended Likelihood": "Moderate",
            "Impact": "Moderate",
            "Impact Description": "Description of magnitude of
                                   potential harm from the
                                   exploitation of this
                                   vulnerability.",
            "Residual Risk": "Moderate",
            "Recommended Residual Risk": "Moderate",
            "Mitigations": "Description of the mitigations in place
                            (if any) to counter this vulnerability.",
            "Resulting Residual Risk Level after Proposed
            Mitigations": "-",
            "Recommendations": "Summary of the recommended actions
                                that will further address/reduce the
                                risk of this vulnerability.",
            "Source Identifying Vulnerability":
                              "Application_Security_Development_STIG",
            "Resources": "Resources required to correct the identified
                          vulnerability.",
            "Comments": "Description of any relevant information not
                         captured by the other fields.",
            "Artifact Attachments": "0",
            "POC": "-",
            "Source": "Not Inherited",
            "Created Date": "1654019161",
            "Last Modified Date": "1654019161",
            "Modified By": "Smith, John",
            "Latest Milestone Description": "Milestone A",
            "Milestone Scheduled Completion Date": "1614793549",
            "Milestone Created Date": "1654019162",
            "Milestone Review Status": "Under Review"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.7 System Artifacts Summary

GET	**/api/dashboards/system-artifacts-summary** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-artifacts-summary?orgId=1" -H "api-key:
0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
excludeInherited	Boolean	true, false If no value is specified, the default returns false to include inherited data.
orgId	Integer	1 This value will be provided by eMASS Support.

Sample Response
(orgId=1, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "Test Org",
            "Organization Hierarchy": "Army > Test Org",
            "System Name": "John Assess & Authorize System",
            "System Acronym": "John A&A System",
            "System ID": "4",
            "Policy": "RMF",
            "Registration Type": "Assess and Authorize",
            "Authorization Status": "Authorization to Operate (ATO)",
            "Authorization Termination Date": "1692204393",
            "Inherited Artifacts": "0",
            "Total Artifacts": "5",
            "Expiring Artifacts": "0",
            "Expired Artifacts": "0",
            "Artifacts w/o Control/AP Associations": "3"
        },
        {
            "Organization": "Army",
            "Organization Hierarchy": "Army",
            "System Name": "Jane Assess & Authorize System",
            "System Acronym": "Jane A&A System",
            "System ID": "5",
            "Policy": "RMF",
            "Registration Type": "Assess and Authorize",
            "Authorization Status": "EXPIRED",
            "Authorization Termination Date": "1657567243",
            "Inherited Artifacts": "1",
            "Total Artifacts": "35",
            "Expiring Artifacts": "0",
            "Expired Artifacts": "4",
            "Artifacts w/o Control/AP Associations": "31"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.8 System Artifacts Details

GET	/api/dashboards/system-artifacts-details *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-artifacts-details?orgId=1&pageIndex=0"
-H "api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	**Type**	**Example**
excludeInherited	Boolean	true, false If no value is specified, the default returns false to include inherited data.
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "Test Org",
            "Organization Hierarchy": "Army > Test Org",
            "System Name": "John Assess & Authorize System",
            "System Acronym": "John A&A System",
            "System ID": "4",
            "Policy": "RMF",
            "Registration Type": "Assess and Authorize",
            "Authorization Status": "Authorization to Operate (ATO)",
            "Authorization Termination Date": "1692204393",
            "Artifact Name": "E-Authentication Assessment",
            "Description": "The assessment of new and existing
                            electronic transactions within the system
                            to ensure that authentication processes
                            provide the appropriate level of
                            assurance.",
            "Filename": "RiskAssessment.pdf",
            "Type": "Document",
            "Category": "E-Authentication Risk Assessment",
            "Inherited From": "-",
            "Control Association(s)": "IA-2,IA-8",
            "AP Association(s)": "-",
            "Template": "No",
            "Reference": "-",
            "Last Modified": "1660667649",
            "Last Reviewed": "-",
            "Signed Date": "1659803645",
            "Expiration Date": "1691339645",
            "Created By": "SSO, Admin",
            "Created Date": "1660667649",
            "Download URL":
                          "[URL]/App/CA/DownloadArtifactFile/147/8541"
        },
        {
            "Organization": "Army",
            "Organization Hierarchy": "Army",
            "System Name": "Jane Assess & Authorize System",
            "System Acronym": "Jane A&A System",
            "System ID": "5",
            "Policy": "RMF",
            "Registration Type": "Assess and Authorize",
            "Authorization Status": "Not Yet Authorized",
            "Authorization Termination Date": "-",
            "Artifact Name": "Configuration Management Plan",
            "Description": "A comprehensive description of the roles,
                            responsibilities, policies, and
                            procedures that apply when managing the
                            configuration of products and systems.",
            "Filename": "Assessment.xlsx",
            "Type": "Other",
            "Category": "Configuration Management Plan",
            "Inherited From": "-",
            "Control Association(s)": "-",
            "AP Association(s)": "-",
            "Template": "No",
            "Reference": "-",
            "Last Modified": "1660071054",
            "Last Reviewed": "-",
            "Signed Date": "1660071053",
            "Expiration Date": "1691607053",
            "Created By": "SSO, Admin",
            "Created Date": "1660071054",
            "Download URL":
                          "[URL]/App/CA/DownloadArtifactFile/134/8541"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.9 System Hardware Summary

GET	/api/dashboards/system-hardware-summary *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-hardware-summary?orgId=1&pageIndex=0" -H "api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "Test Org",
            "Organization Hierarchy": "USN > Test Org",
            "System Acronym": "John A&A System",
            "System Name": "John Assess & Authorize System",
            "System ID": "1",
            "Registration Completion Date": "1647639989",
            "Policy": "RMF",
            "Authorization Status": "Authorization to Operate (ATO)",
            "Hardware Matching Criteria": "0",
            "Total Hardware Assets": "2"
        },
        {
            "Organization": "USN",
            "Organization Hierarchy": "USN",
            "System Acronym": "Jane Guest System",
            "System Name": "Jane Guest System",
            "System ID": "2",
            "Registration Completion Date": "1648063729",
            "Policy": "RMF",
            "Authorization Status": "Authority to Connect (ATC)",
            "Hardware Matching Criteria": "0",
            "Total Hardware Assets": "0"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.10 System Hardware Details

GET	/api/dashboards/system-hardware-details *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-hardware-details?orgId=1&pageIndex=0" -
H "api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "USN",
            "System ID": "29",
            "System Name": "Jane Assess and Authorize Test",
            "System Acronym": "Jane A&A Test",
            "System Type": "IS Major Application",
            "Component Type": "Web Server",
            "Machine Name": "test34126",
            "Nickname": "-",
            "IP Address": "100.00.00.34126",
            "Virtual Asset": "No",
            "Manufacturer": "Test Manufacturer ",
            "Model Number": "T-34925",
            "Serial Number": "00034126",
            "OS/iOS/FW Version": "Windows 2016 Server",
            "Memory Size / Type": "-",
            "Location": "-",
            "Approval Status": "-",
            "Critical Asset": "No",
            "POC Office/Organization": "-",
            "POC First Name": "-",
            "POC Last Name": "-",
            "POC Phone Number": "-",
            "POC Email": "-",
            "Date Reviewed / Updated": "-",
            "Reviewed / Updated By": "-"
        },
        {
            "Organization": "USN",
            "System ID": "29",
            "System Name": "Jane Assess and Authorize Test",
            "System Acronym": "Jane A&A Test",
            "System Type": "IS Major Application",
            "Component Type": "Web Server",
            "Machine Name": "test34127",
            "Nickname": "-",
            "IP Address": "100.00.00.34127",
            "Virtual Asset": "No",
            "Manufacturer": "Test Manufacturer",
            "Model Number": "T-34926",
            "Serial Number": "00034127",
            "OS/iOS/FW Version": "Windows 2016 Server",
            "Memory Size / Type": "-",
            "Location": "-",
            "Approval Status": "-",
            "Critical Asset": "No",
            "POC Office/Organization": "-",
            "POC First Name": "-",
            "POC Last Name": "-",
            "POC Phone Number": "-",
            "POC Email": "-",
            "Date Reviewed / Updated": "-",
            "Reviewed / Updated By": "-"
        }
    ],
    "pagination": {
        "totalCount": 60360,
        "totalPages": 4,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": "https://[URL]/api/dashboards/system-hardware-
                        details?orgid=1&pageIndex=1&pageSize=20000"
    }
}
```

4.19.11 System Associations Details

GET **/api/dashboards/system-associations-details**
Get dashboard information

Curl Example

```
curl -L "[URL]/api/dashboards/system-associations-
details?orgId=1&pageIndex=0" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "USN",
            "System ID": "2",
            "System Name": "John Assess and Authorize System",
            "System Acronym": "John A&A System",
            "Relationship Type": "relates to",
            "Associated System ID": "3",
            "Associated System Acronym": "John CCP",
            "Associated System Name": "John Common Control Provider",
            "Owning Organization": "USN",
            "Authorization Status": "Not Yet Authorized",
            "Authorization Termination Date": "-",
            "Relationship Description": "Test Relationship",
            "External System": "No",
            "Controls Received": "-",
            "APs Received": "-",
            "Controls Provided": "-",
            "APs Provided": "-",
            "System Type": "IS Major Application",
            "Date Established": "1655477694"
        },
        {
            "Organization": "USN",
            "System ID": "3",
            "System Name": "John Common Control Provider",
            "System Acronym": "John CCP",
            "Relationship Type": "provides inheritance to",
            "Associated System ID": "5",
            "Associated System Acronym": "Jane A&A System",
            "Associated System Name": "Jane A&A System",
            "Owning Organization": "USN",
            "Authorization Status": "Interim Authorization to Test -
                                     Not Connected (IATT-NC)",
            "Authorization Termination Date": "1661955140",
            "Relationship Description": "This association was
                                         automatically created by the
                                         established inheritance
                                         relationship.",
            "External System": "No",
            "Controls Received": "0",
            "APs Received": "0",
            "Controls Provided": "1",
            "APs Provided": "4",
            "System Type": "IS Major Application",
            "Date Established": "1659108397"
        },
        {
            "Organization": "USN",
            "System ID": "5",
            "System Name": "Jane A&A System",
            "System Acronym": "Jane A&A System",
            "Relationship Type": "receives inheritance from",
            "Associated System ID": "3",
            "Associated System Acronym": "John CCP",
            "Associated System Name": "John Common Control Provider",
            "Owning Organization": "USN",
            "Authorization Status": "Not Yet Authorized",
            "Authorization Termination Date": "-",
            "Relationship Description": "This association was
                                         automatically created by the
                                         established inheritance
                                         relationship.",
            "External System": "No",
            "Controls Received": "1",
            "APs Received": "4",
            "Controls Provided": "1",
            "APs Provided": "4",
            "System Type": "IS Major Application",
            "Date Established": "1659108397"
        }
    ],
    "pagination": {
        "totalCount": 3,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
        }
}
```

4.19.12 User System Assignments Details

GET	**/api/dashboards/user-system-assignments-details** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/user-system-assignments-
details?orgId=1&pageIndex=0" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "User ID": "2",
            "Status": "Active",
            "Last Name": "Smith",
            "First Name": "John",
            "Home Organization": "DISA",
            "Email": "200@mail.mil",
            "Phone": "200200200",
            "Role": "AO, AODR Rep",
            "System Name": "John Assess and Authorize System",
            "System Acronym": "John A&A System",
            "System ID": "1",
            "System Policy": "RMF",
            "Organization": "Test Org",
            "Organization Hierarchy": "DISA > Test Org"
        },
        {
            "User ID": "2",
            "Status": "Active",
            "Last Name": "Smith",
            "First Name": "John",
            "Home Organization": "DISA",
            "Email": "200@mail.mil ",
            "Phone": "200200200",
            "Role": "AO",
            "System Name": "Jane CCP System",
            "System Acronym": "Jane CCP System",
            "System ID": "18",
            "System Policy": "RMF",
            "Organization": "DISA",
            "Organization Hierarchy": "DISA"
        },
        {
            "User ID": "7",
            "Status": "Active",
            "Last Name": "Doe",
            "First Name": "Jane",
            "Home Organization": "DISA",
            "Email": "195@emass.com",
            "Phone": "9998887777",
            "Role": "ISSO/PM/SM",
            "System Name": "Jane CCP System",
            "System Acronym": "Jane CCP System",
            "System ID": "18",
            "System Policy": "RMF",
            "Organization": "DISA",
            "Organization Hierarchy": "DISA"
        },
        {
            "User ID": "9",
            "Status": "Inactive",
            "Last Name": "Johnson",
            "First Name": "Steven",
            "Home Organization": "DISA",
            "Email": "117@mail.mil",
            "Phone": "117117117117",
            "Role": "AO, AODR Rep, Directorate ISSM, ISSO, ISSO/PM/SM,
                     Organizational Director, SCA, SCA Team",
            "System Name": "Test System 1",
            "System Acronym": "Test 1",
            "System ID": "48",
            "System Policy": "RMF",
            "Organization": "DISA",
            "Organization Hierarchy": "DISA"
        }
    ],
    "pagination": {
        "totalCount": 4,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.13 System Privacy Summary

GET	/api/dashboards/system-privacy-summary *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/system-privacy-summary?orgId=1&pageIndex=0" -H
"api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "Test Org",
            "Organization Hierarchy": "DISA > Test Org",
            "System Acronym": "John A&A System",
            "System Name": "John Assess and Authorize System",
            "System ID": "1",
            "Registration Completion Date": "1655488771",
            "Policy": "RMF",
            "Registration Type": "Assess and Authorize",
            "System Type": "IS Major Application",
            "Authorization Status": "Authorization to Operate (ATO)",
            "System Life Cycle / Acquisition Phase": "Post-Milestone C
                                                      (Production and
                                                     Deployment)",
            "PTA Completed": "Yes",
            "PTA Date": "1655491804",
            "PIA Required": "Yes",
            "PIA Status": "Completed",
            "PIA Date": "1655491804",
            "Controlled Unclassified Information (CUI)": "No",
            "Personally Identifiable Information (PII)": "Yes",
            "Protected Health Information (PHI)": "Yes",
            "ATOs in Current FY": "1",
            "Privacy Overlay Applied": "Yes",
            "HIPAA Coverage": "Yes",
            "Privacy Overlays Responses": "Does the information system
                                           contain PII? (Yes); Does
                                           the Exception of the
                                           Business Rolodex
                                           Information Apply? (No);
                                           Is the PII confidentiality
                                           impact level low,
                                           moderate, or high?
                                           (Moderate); Is your
                                           organization a covered
                                           entity or business
                                           associate under HIPAA?
                                           (Yes); Is the PII in the
                                           information system PHI?
                                           (Yes)",
            "System of Records Notice Required": "Yes"
        },
        {
            "Organization": "DISA",
            "Organization Hierarchy": "DISA",
            "System Acronym": "Jane CCP System",
            "System Name": "Jane CCP System",
            "System ID": "18",
            "Registration Completion Date": "1657638316",
            "Policy": "RMF",
            "Registration Type": "Common Control Provider",
            "System Type": "Platform IT System",
            "Authorization Status": "Interim Authorization to Test -
                                     Not Connected (IATT-NC)",
            "System Life Cycle / Acquisition Phase": "Pre-Milestone A
                                                      (Material
                                                      Solution
                                                      Analysis)",
            "PTA Completed": "-",
            "PTA Date": "-",
            "PIA Required": "-",
            "PIA Status": "-",
            "PIA Date": "-",
            "Controlled Unclassified Information (CUI)": "-",
            "Personally Identifiable Information (PII)": "-",
            "Protected Health Information (PHI)": "-",
            "ATOs in Current FY": "0",
            "Privacy Overlay Applied": "No",
            "HIPAA Coverage": "-",
            "Privacy Overlays Responses": "-",
            "System of Records Notice Required": "-"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.14 VA OMB FISMA SAOP Summary

GET **/api/dashboards/va-omb-fisma-saop-summary**

Get dashboard information

Curl Example

```
curl -L "[URL]/api/dashboards/va-omb-fisma-saop-summary?orgId=1&pageIndex=0"
-H "api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Geographical Association": "Unassigned",
            "Identifiable Systems VA": "0",
            "Identifiable Systems Non-VA": "0",
            "Identifiable Systems Requiring PIA VA": "0",
            "Identifiable Systems Requiring PIA Non-VA": "0",
            "Identifiable Systems w/ Current PIA VA": "0",
            "Identifiable Systems w/ Current PIA Non-VA": "0",
            "Identifiable Systems Requiring SORN VA": "0",
            "Identifiable Systems Requiring SORN Non-VA": "0",
            "Identifiable Systems w/ Current SORN VA": "0",
            "Identifiable Systems w/ Current SORN Non-VA": "0"
        },
        {
            "Geographical Association": "EO",
            "Identifiable Systems VA": "1",
            "Identifiable Systems Non-VA": "0",
            "Identifiable Systems Requiring PIA VA": "1",
            "Identifiable Systems Requiring PIA Non-VA": "0",
            "Identifiable Systems w/ Current PIA VA": "0",
            "Identifiable Systems w/ Current PIA Non-VA": "0",
            "Identifiable Systems Requiring SORN VA": "1",
            "Identifiable Systems Requiring SORN Non-VA": "0",
            "Identifiable Systems w/ Current SORN VA": "1",
            "Identifiable Systems w/ Current SORN Non-VA": "0"
        },
        {
            "Geographical Association": "Region 1",
            "Identifiable Systems VA": "3",
            "Identifiable Systems Non-VA": "2",
            "Identifiable Systems Requiring PIA VA": "2",
            "Identifiable Systems Requiring PIA Non-VA": "1",
            "Identifiable Systems w/ Current PIA VA": "1",
            "Identifiable Systems w/ Current PIA Non-VA": "0",
            "Identifiable Systems Requiring SORN VA": "2",
            "Identifiable Systems Requiring SORN Non-VA": "0",
            "Identifiable Systems w/ Current SORN VA": "1",
            "Identifiable Systems w/ Current SORN Non-VA": "2"
        },
        {
            "Geographical Association": "Region 2",
            "Identifiable Systems VA": "0",
            "Identifiable Systems Non-VA": "0",
            "Identifiable Systems Requiring PIA VA": "0",
            "Identifiable Systems Requiring PIA Non-VA": "0",
            "Identifiable Systems w/ Current PIA VA": "0",
            "Identifiable Systems w/ Current PIA Non-VA": "0",
            "Identifiable Systems Requiring SORN VA": "0",
            "Identifiable Systems Requiring SORN Non-VA": "0",
            "Identifiable Systems w/ Current SORN VA": "0",
            "Identifiable Systems w/ Current SORN Non-VA": "0"
        },
        {
            "Geographical Association": "Region Other",
            "Identifiable Systems VA": "1",
            "Identifiable Systems Non-VA": "0",
            "Identifiable Systems Requiring PIA VA": "0",
            "Identifiable Systems Requiring PIA Non-VA": "0",
            "Identifiable Systems w/ Current PIA VA": "0",
            "Identifiable Systems w/ Current PIA Non-VA": "0",
            "Identifiable Systems Requiring SORN VA": "0",
            "Identifiable Systems Requiring SORN Non-VA": "0",
            "Identifiable Systems w/ Current SORN VA": "0",
            "Identifiable Systems w/ Current SORN Non-VA": "0"
        }
    ],
    "pagination": {
        "totalCount": 8,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
        }
}
```

4.19.15 VA System A&A Summary

GET	/api/dashboards/va-system-aa-summary *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/va-system-aa-summary?orgId=1&pageIndex=0" -H
"api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
excludeInherited	Boolean	true, false If no value is specified, the default returns false to include inherited data.
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization Name": "VA",
            "System ID": "1",
            "System Acronym": "John A&A System",
            "System Name": "John Assess and Authorize System",
            "Registration Completion Date": "1655490034",
            "Registration Type": "Assess and Authorize",
            "System Type": "IS Major Application",
            "Special Type": "-",
            "Special Type Description": "-",
            "Portfolio/Product Line": "Not Applicable",
            "Geographical Association": "EO",
            "Entity Type": "Information System",
            "FISMA Reportable": "Yes",
            "VA Exhibit 300 ID": "1",
            "System Ownership / Controlled": "VA Partnered System",
            "System Development Life Cycle":
                                              "Implementation/Assessment",
            "Cloud Computing": "No",
            "Cloud Type": "-",
            "Data Hosting": "Internal to VA Network",
            "Quantity of Data (GB)": "-",
            "Unique Records": "-",
            "Impact": "Moderate",
            "High Value Asset": "No",
            "Current RMF Step": "6 - Monitor",
            "Days In Current RMF Step": "7",
            "Need Date": "-",
            "Authorization Status": "Authorization to Operate (ATO)",
            "Authorization Date": "1660078033",
            "ATD": "1693514586",
            "Authorization Length": "387",
            "Authorization Expiration Status": "Continous Monitoring",
            "# of previous ATO w/Conditions": "0",
            "Overall Risk Score": "Moderate",
            "Type Authorization": "No",
            "Package Type(s)": "POA&M Approval; Change Request",
            "Current Workflow Stage": "(POA&M Approval) ISSO; (Change
                                           Request) ISSO",
            "Days in Current Workflow Stage": "(POA&M Approval) 10.9;
                                                   (Change Request) 15.1",
            "% of Workflow Completed": "(POA&M Approval) 20.00%;
                                            (Change Request) 20.00%",
            "Compliant Controls": "0",
            "Non-Compliant Controls": "0",
            "Not Applicable Controls": "0",
            "Unassessed Controls": "276",
            "Compliant APs": "0",
            "Non-Compliant APs": "0",
            "Not Applicable APs": "0",
            "Unassessed APs": "1281",
            "Ongoing POA&M Items": "1",
            "Risk Accepted POA&M Items": "1",
            "Last AO to Provide Authorization": "Smith, John",
            "System Steward": "Smith, John",
            "ISSO": "Smith, John",
            "Current AO": "Smith, John",
            "System Owner": "Smith, John"
        },
        {
            "Organization Name": "VA",
            "System ID": "2",
            "System Acronym": "Jane A&A System",
            "System Name": "Jane Assess & Authorize System",
            "Registration Completion Date": "1657304286",
            "Registration Type": "Assess and Authorize",
            "System Type": "IS Major Application",
            "Special Type": "-",
            "Special Type Description": "-",
            "Portfolio/Product Line": "-",
            "Geographical Association": "EO",
            "Entity Type": "Information System",
            "FISMA Reportable": "Yes",
            "VA Exhibit 300 ID": "1",
            "System Ownership / Controlled": "VA Partnered System",
            "System Development Life Cycle": "Initiation",
            "Cloud Computing": "No",
            "Cloud Type": "-",
            "Data Hosting": "Internal to VA Network",
            "Quantity of Data (GB)": "1",
            "Unique Records": "1",
            "Impact": "High",
            "High Value Asset": "No",
            "Current RMF Step": "-",
            "Days In Current RMF Step": "0",
            "Need Date": "1657567244",
            "Authorization Status": "EXPIRED",
            "Authorization Date": "1657567243",
            "ATD": "1657567243",
            "Authorization Length": "0",
            "Authorization Expiration Status": "Expired",
            "# of previous ATO w/Conditions": "0",
            "Overall Risk Score": "High",
            "Type Authorization": "Yes",
            "Package Type(s)": "POA&M Approval",
            "Current Workflow Stage": "ISSO",
            "Days in Current Workflow Stage": "33.8",
            "% of Workflow Completed": "20.00%",
            "Compliant Controls": "0",
            "Non-Compliant Controls": "2",
            "Not Applicable Controls": "1",
            "Unassessed Controls": "273",
            "Compliant APs": "0",
            "Non-Compliant APs": "2",
            "Not Applicable APs": "21",
            "Unassessed APs": "1258",
            "Ongoing POA&M Items": "3",
            "Risk Accepted POA&M Items": "2",
            "Last AO to Provide Authorization": "-",
            "System Steward": "Doe, Jane",
            "ISSO": "Doe, Jane",
            "Current AO": "Doe, Jane",
            "System Owner": "Doe, Jane"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.16 VA System A2.0 Summary

GET	/api/dashboards/va-system-a2-summary *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/va-system-a2-summary?orgId=1&pageIndex=0" -H
"api-key: 0a60a84d-3fc1-433c-b39f-507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	Type	Example
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "System ID": "1",
            "System Name": "John Assess and Authorize System",
            "Registration Completion Date": "1655490034",
            "Confidentiality": "Moderate",
            "Integrity": "Moderate",
            "Availability": "Moderate",
            "FISMA Reportable": "Yes",
            "PII": "No",
            "PHI": "No",
            "Public Facing Presence (Externally Facing)": "-",
            "Portfolio/Product Line": "Not Applicable",
            "High Value Asset": "No",
            "Customer and Veteran Experience User Base (Total Number
                                                  of Users)": "-",
            "Mission Critical Single Point of Failure": "No",
            "Overall Risk Score": "Moderate",
            "Type Authorization": "No",
            "Compliant Controls": "0",
            "Non-Compliant Controls": "0",
            "Not Applicable Controls": "0",
            "Unassessed Controls": "276",
            "Compliant Controls without Evidence": "0",
            "Inherited Controls": "1",
            "Controls Provided as Inheritable": "0",
            "Ongoing POA&Ms": "1",
            "Risk Accepted POA&Ms": "1",
            "Overdue POA&Ms": "1",
            "Completed POA&Ms": "0",
            "Low or Very Low Severity Ongoing POA&Ms": "1",
            "Moderate Severity Ongoing POA&Ms": "0",
            "High or Very High Severity Ongoing POA&Ms ": "0",
            "Low or Very Low Residual Risk Ongoing POA&Ms": "0",
            "Moderate Residual Risk Ongoing POA&Ms": "1",
            "High or Very High Residual Risk Ongoing POA&Ms": "0"
        },
        {
            "System ID": "2",
            "System Name": "Jane Assess & Authorize System",
            "Registration Completion Date": "1657304286",
            "Confidentiality": "Moderate",
            "Integrity": "Moderate",
            "Availability": "Moderate",
            "FISMA Reportable": "No",
            "PII": "No",
            "PHI": "No",
            "Public Facing Presence (Externally Facing)": "No",
            "Portfolio/Product Line": "-",
            "High Value Asset": "No",
            "Customer and Veteran Experience User Base (Total Number
                                                    of Users)": "12",
            "Mission Critical Single Point of Failure": "No",
            "Overall Risk Score": "-",
            "Type Authorization": "No",
            "Compliant Controls": "1",
            "Non-Compliant Controls": "0",
            "Not Applicable Controls": "0",
            "Unassessed Controls": "275",
            "Compliant Controls without Evidence": "1",
            "Inherited Controls": "0",
            "Controls Provided as Inheritable": "0",
            "Ongoing POA&Ms": "1",
            "Risk Accepted POA&Ms": "0",
            "Overdue POA&Ms": "1",
            "Completed POA&Ms": "0",
            "Low or Very Low Severity Ongoing POA&Ms": "0",
            "Moderate Severity Ongoing POA&Ms": "1",
            "High or Very High Severity Ongoing POA&Ms ": "0",
            "Low or Very Low Residual Risk Ongoing POA&Ms": "0",
            "Moderate Residual Risk Ongoing POA&Ms": "1",
            "High or Very High Residual Risk Ongoing POA&Ms": "0"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.17 VA System P.L. 109 Reporting Summary

GET	**/api/dashboards/va-system-pl-109-reporting-summary** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/va-system-pl-109-reporting-
summary?orgId=1&pageIndex=0" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	**Type**	**Example**
excludeInherited	Boolean	true, false If no value is specified, the default returns false to include inherited data.
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "Test Org",
            "Organization Hierarchy": "VA > Test Org",
            "System Acronym": "John A&A System",
            "System Name": "John Assess and Authorize System",
            "System ID": "1",
            "Registration Completion Date": "1657303069",
            "Registration Type": "Assess and Authorize",
            "Entity Type": "Facility",
            "Geographical Association": "EO",
            "Impact": "Moderate",
            "Authorization Status": "Not Yet Authorized",
            "System Development Life Cycle": "Initiation",
            "Ongoing (Overall)": "7",
            "Risk Accepted (Overall)": "4",
            "Completed (Overall)": "5",
            "Total (Overall)": "16",
            "% Completed (Overall) POA&M Items": "31%",
            "Ongoing (Management)": "0",
            "Risk Accepted (Management)": "0",
            "Completed (Management)": "0",
            "Total (Management)": "0",
            "% Completed (Management)": "-",
            "Ongoing (Technical)": "4",
            "Risk Accepted (Technical)": "3",
            "Completed (Technical)": "4",
            "Total (Technical)": "11",
            "% Completed (Technical)": "36%",
            "Ongoing (Operational)": "2",
            "Risk Accepted (Operational)": "1",
            "Completed (Operational)": "1",
            "Total (Operational)": "4",
            "% Completed (Operational)": "25%",
            "Ongoing (Privacy)": "0",
            "Risk Accepted (Privacy)": "0",
            "Completed (Privacy)": "0",
            "Total (Privacy)": "0",
            "% Completed (Privacy)": "-",
            "Ongoing (Unassigned)": "1",
            "Risk Accepted (Unassigned)": "0",
            "Completed (Unassigned)": "0",
            "Total (Unassigned)": "1",
            "% Completed (Unassigned)": "0%",
            "Installation Name/Owning Org": "Location 1",
            "Country": "United States",
            "State": "Virginia",
            "City": "Herndon",
            "Street Address": "123 Herndon Dr.",
            "Building Number": "-",
            "Room Number": "-",
            "Zip Code": "12341"
        {
            "Organization": "VA",
            "Organization Hierarchy": "VA",
            "System Acronym": "Jane A&A System",
            "System Name": "Jane Assess & Authorize System",
            "System ID": "9",
            "Registration Completion Date": "1657304286",
            "Registration Type": "Assess and Authorize",
            "Entity Type": "Information System",
            "Geographical Association": "Region 3",
            "Impact": "Moderate",
            "Authorization Status": "Not Yet Authorized",
            "System Development Life Cycle":
                                          "Implementation/Assessment",
            "Ongoing (Overall)": "3",
            "Risk Accepted (Overall)": "2",
            "Completed (Overall)": "0",
            "Total (Overall)": "5",
            "% Completed (Overall) POA&M Items": "0%",
            "Ongoing (Management)": "0",
            "Risk Accepted (Management)": "0",
            "Completed (Management)": "0",
            "Total (Management)": "0",
            "% Completed (Management)": "-",
            "Ongoing (Technical)": "2",
            "Risk Accepted (Technical)": "1",
            "Completed (Technical)": "0",
            "Total (Technical)": "3",
            "% Completed (Technical)": "0%",
            "Ongoing (Operational)": "0",
            "Risk Accepted (Operational)": "1",
            "Completed (Operational)": "0",
            "Total (Operational)": "1",
            "% Completed (Operational)": "0%",
            "Ongoing (Privacy)": "0",
            "Risk Accepted (Privacy)": "0",
            "Completed (Privacy)": "0",
            "Total (Privacy)": "0",
            "% Completed (Privacy)": "-",
            "Ongoing (Unassigned)": "1",
            "Risk Accepted (Unassigned)": "0",
            "Completed (Unassigned)": "0",
            "Total (Unassigned)": "1",
            "% Completed (Unassigned)": "0%",
            "Installation Name/Owning Org": "123",
            "Country": "United States",
            "State": "Vermont",
            "City": "Victory",
            "Street Address": "123123",
            "Building Number": "-",
            "Room Number": "-",
            "Zip Code": "12345"
        }
    ],
    "pagination": {
        "totalCount": 2,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

4.19.18 VA System FISMA Inventory Summary

GET	**/api/dashboards/va-system-fisma-inventory-summary** *Get dashboard information*

Curl Example

```
curl -L "[URL]/api/dashboards/va-system-fisma-inventory-
summary?orgId=1&pageIndex=0" -H "api-key: 0a60a84d-3fc1-433c-b39f-
507adb1f8bec" --cert .\cert.pem
```

Available Query String Parameters

Name	**Type**	**Example**
orgId	Integer	1 This value will be provided by eMASS Support.
pageIndex	Integer	0 If no value is specified, the default returns results from the first page with an index of 0.
pageSize	Integer	20000 If no value is specified, the default returns up to 20,000 results per page. Exceeding this value is prohibited and will default back to 20,000.

Sample Response
(orgId=1, pageIndex=0, pageSize=20000)

```
{
    "meta": {
        "code": 200
    },
    "data": [
        {
            "Organization": "Test Org",
            "Organization Hierarchy": "VA > Test Org",
            "System Acronym": "John A&A System",
            "System Name": "John Assess and Authorize System",
            "System ID": "1",
            "Registration Completion Date": "1655490034",
            "VASI ID": "200",
            "VA EPS Number": "-",
            "Registration Type": "Assess and Authorize",
            "System Description": "Test Description",
            "System Type": "IS Major Application",
            "VA System Type": "Financial",
            "Special Type": " COVID-19 Priority",
            "Special Type Description": "Test Special Type
                                         Description",
            "Portfolio/Product Line": "Not Applicable",
            "Entity Type": "Information System",
            "Geographical Association": "Region Other",
            "FISMA Reportable": "Yes",
            "Authorization Status": "Authorization to Operate (ATO)",
"Type Authorization": "Yes",
"Current RMF Step": "6 - Monitor",
"Days In Current RMF Step": "0",
"Confidentiality": "Moderate",
"Integrity": "Moderate",
"Availability": "Moderate",
"Impact": "Moderate",
"Authorized Confidentiality": "Moderate",
"Authorized Integrity": "Moderate",
"Authorized Availability": "Moderate",
"Security Review Completed": "Yes",
"Security Review Date": "1660667933",
"Days Since Last Annual Review": "0",
"Contingency Plan Tested": "Yes",
"Contingency Plan Test Date": "1659717245",
"Days Since Last Contingency Plan Test": "11",
"Alternate Processing Site (Contingency)": "VA - Dulles,
                                            VA - Ashburn",
"Contingency Plan Test Type": "Functional (restore from
                               backup)",
"Incident Response Test Date": "1659890045",
"Disaster Recovery Test Date": "1660062845",
"Alternate Processing Site (Disaster Recovery)": "VA -
                                                 Ashburn",
"System Development Life Cycle": "Initiation",
"System Ownership / Controlled": "VA Owned and VA Operated
                                  IS",
"Cloud Computing": "Yes",
"Cloud Type": "Private",
"Quantity of Data (GB)": "500",
"Unique Records": "1000",
"Data Loss Prevention (DLP) Protected": "Yes",
"Data Rights Management (DRM) Protected": "Yes",
"Encryption of Data": "Data at Rest; Data in Transit; Data
                       in Use",
"Data Encryption Barrier": "-",
"Data Encryption Barrier (Other)": "-",
"Data Retention Length": "6 months",
"Permanent Data": "No",
"Replica Data": "Yes",
"External User Access": "Yes",
"National Essential Function (NEF)": "Yes",
"NEF Description": "Defending the United States against
                    all enemies, foreign and domestic, and
                    preventing or interdicting attacks
                    against the United States or its
                    people, property, or interest.;
                    Ensuring the continued functioning of
                    our form of government under the
                    United States Constitution, including
                    the functioning of the three separate
                    branches of government.",
"Mission Essential Function (MEF)": "Yes",
"MEF Description": "Acquisition support (OALC); Account
                    for employees (HRA)",
"Primary Mission Essential Function (PMEF)": "Yes",
            "PMEF Description": "Provide medical and hospital services
                                 for Veterans, and during a disaster
                                 or emergency, for civilian victims as
                                 appropriate. (VHA)",
            "Maximum Tolerable Downtime": "48 hours",
            "Recovery Time Objective": "Mission Critical: 12 hours",
            "Recovery Point Objective": "Essential Support: 72 hours",
            "BIA Required": "Yes",

            "BIA Last Reviewed Date": "1656707876",
            "Contingency Plan Required": "Yes",
            "Contingency Plan Last Reviewed Date": "1656794282",
            "Incident Response Plan Required": "Yes",
            "Incident Response Plan Last Reviewed Date": "1656880688",
            "Disaster Recovery Plan Required": "Yes",
            "Disaster Recovery Plan Last Reviewed Date": "1656967094",
            "Threat Model Required": "Yes",
            "Threat Model Status": "Completed",
            "Threat Model Last Completed": "1660336553",
            "Remaining Medium Unmitigated Vulnerabilities": "5",
            "Remaining High Unmitigated Vulnerabilities": "3",
            "Threat Model Last Reviewed Date": "1657139904",
            "Configuration Management Plan Required": "Yes",
            "Configuration Management Plan Last Reviewed Date":
                                                         "1657053626",
            "Privacy Threshold Analysis Required": "Yes",
            "Privacy Threshold Analysis Last Reviewed Date":
                                                         "1657226310",
            "Privacy Impact Assessment Required": "Yes",
            "Privacy Impact Assessment Last Reviewed Date":
                                                         "1657312721",
            "PIV Status": "Enabled",
            "MFA Details (Internal Users)": "System enforces an MFA
                                             credential that is
                                             verifier impersonation-
                                             resistant (e.g., mutual
                                             TLS, or Web
                                             Authentication) as a
                                             required authentication
                                             mechanism for internal
                                             users",
            "MFA Barrier": "Technology",
            "MFA Barrier (Other)": "-",
            "Network Access PIV Required": "-",
            "Periodic Password Changes": "-",
            "External Federated IDP Trust (Internal Users)": "-",
            "Complex Password Composition": "-",
            "Compromised/Weak Password Checks": "-",
            "External User Accounts": "Yes",
            "MFA Details (External Users)": "System enforces (not
                                             optional) an MFA
                                             credential that is
                                             verifier impersonation-
                                             resistant (e.g., mutual
                                             TLS, or Web
                                             Authentication) as a
                                             required authentication
                                             mechanism.",
            "External Federated IDP Trust (External Users)": "-",
            "PII": "No",
            "PHI": "No",
            "Data Hosting": "Internal to VA Network",
            "Mission Critical Single Point of Failure": "Yes",
            "Mission Critical Description": "Test Point of Failure",
            "System Environment": "Test Environment",
            "Acquisition Contract": "Yes",
            "Contract Name": "Test Contract",
            "Contract Number": "H3128452",
            "Contract Term Length": "3 years",
            "Contract Award / Execution Date": "1659371816",
            "Contract Termination Date": "1754066216",
            "Critical Software Overlay Applied": "Yes",
            "Elevated Privilege": "Yes",
            "Privileged Network/Computing Access": "Yes",
            "Controls Access to Data/Operational Technology": "Yes",
            "Performs Critical Trust Function": "Yes",
            "Privileged Access Beyond Normal Trust": "Yes",
            "System Steward": "Smith, John",
            "Information System Security Officer": "Smith, John",
            "Information System Owner": "Smith, John",
            "Authorizing Official": "Smith, John"
        }
    ],
    "pagination": {
        "totalCount": 1,
        "totalPages": 1,
        "pageIndex": 0,
        "pageSize": 20000,
        "prevPageUrl": "",
        "nextPageUrl": ""
    }
}
```

APPENDIX A – BUSINESS RULES

This appendix contains a table of business rules associated with each defined eMASS endpoint.

CONTROLS ENDPOINTS – RISK ASSESSMENT

Business Rule	**Associated Parameter/Field**
Risk Assessment information cannot be updated if a Security Control is “Inherited.”	N/A
Risk Assessment information cannot be updated for a DIACAP system record.	N/A
Risk Assessment information cannot be updated if Security Control does not exist in the system record.	N/A

CONTROLS ENDPOINTS – IMPLEMENTATION PLAN

Business Rule	**Associated Parameter/Field**
Implementation Plan cannot be updated if a Security Control is “Inherited” except for the following fields: • Common Control Provider • Security Control Designation	commonControlProvider controlDesignation
Security Control with Planned Implementation Status cannot be saved if the following fields are missing data: • Implementation Status • Security Control Designation • Estimated Completion Date • Responsible Entities (if system is Type Authorization) • Criticality • Frequency • Method • Reporting • Tracking • SLCM Comments	implementationStatus controlDesignation estimatedCompletionDate responsibleEntities slcmCriticality slcmFrequency slcmMethod slcmReporting slcmTracking slcmComments
Security Control with Implemented Implementation Status cannot be saved if the following fields are missing data: • Implementation Status	implementationStatus controlDesignation estimatedCompletionDate responsibleEntities

• Security Control Designation • Estimated Completion Date • Responsible Entities (if system is Type Authorization) • Criticality • Frequency • Method • Reporting • Tracking • SLCM Comments	slcmCriticality slcmFrequency slcmMethod slcmReporting slcmTracking slcmComments
Security Control with Not Applicable Implementation Status cannot be saved if the following fields are missing data: • Implementation Status • N/A Justification • Security Control Designation • Responsible Entities (if system is Type Authorization)	implementationStatus naJustification controlDesignation responsibleEntities
Security Control with Manually Inherited Implementation Status cannot be saved if the following fields are missing data: • Implementation Status • Common Control Provider • Security Control Designation • Estimated Completion Date • Responsible Entities (if system is Type Authorization) • Criticality • Frequency • Method • Reporting • Tracking • SLCM Comments	implementationStatus commonControlProvider controlDesignation estimatedCompletionDate responsibleEntities slcmCriticality slcmFrequency slcmMethod slcmReporting slcmTracking slcmComments
Implementation Plan information cannot be saved if the fields below exceed the following character limits: • N/A Justification – 2,000 characters • Responsible Entities – 2,000 characters • Implementation Narrative – 2,000 characters • Criticality – 2,000 characters • Reporting – 2,000 characters	naJustification responsibleEntities implementationNarrative slcmCriticality slcmFrequency slcmMethod slcmReporting slcmTracking slcmComments

- Tracking – 2,000 characters - SLCM Comments – 2,000 characters	
Implementation Plan information cannot be updated if Security Control does not exist in the system record.	N/A

TEST RESULTS ENDPOINTS

Business Rule	**Associated Parameter/Field**
Tests Results cannot be saved if the "Test Date" is in the future.	testDate
Test Results cannot be saved if a Security Control is "Inherited" in the system record.	description
Test Results cannot be saved if an Assessment Procedure is "Inherited" in the system record.	description
Test Results cannot be saved if the AP does not exist in the system.	description
Test Results cannot be saved if the control is marked "Not Applicable" by an Overlay.	description
Test Results cannot be saved if the control is required to be assessed as "Applicable" by an Overlay.	description
Test Results cannot be saved if the Tests Results entered is greater than 4,000 characters.	description
Test Results cannot be saved if the following fields are missing data: - complianceStatus - testDate - testedBy - description	complianceStatus testDate testedBy description

POA&MS ENDPOINTS

Business Rule	**Associated Parameter/Field**
POA&M Item cannot be saved if associated Security Control or AP is inherited.	N/A

POA&M Item cannot be created manually if a Security Control or AP is Not Applicable.	N/A
Completed POA&M Item cannot be saved if Completion Date is in the future.	completionDate
POA&M Item cannot be saved if the Point of Contact (POC) fields exceed 100 characters: • Office / Organization • First Name • Last Name • Email • Phone Number	pocOrganization pocFirstName pocLastName pocEmail pocPhoneNumber
POA&M Item cannot be saved if Mitigation field exceeds 2,000 characters.	mitigation
Completed POA&M Item cannot be saved if Completion Date is in the future.	completionDate
POA&M Item cannot be saved if Source Identifying Vulnerability field exceeds 2,000 characters.	sourceIdentVuln
POA&M Item cannot be saved if Comments field exceeds 2,000 characters.	comments
POA&M Item cannot be saved if Resources field exceeds 250 characters.	resources
Risk Accepted POA&M Item cannot be saved with a Scheduled Completion Date or Milestones.	scheduledCompletionDate
Risk Accepted POA&M Item cannot be saved for a Compliant Control or AP.	controlAcronym cci
POA&M Item cannot be saved if the following fields are missing data: • Status • Scheduled Completion Date • Completion Date (Completed POA&M Item only) • Office / Organization • First Name (only if Last Name, Email, or Phone Number have data) • Last Name (only if First Name, Email, or Phone Number have data) • Email (only if First Name, Last Name, or Phone Number have data)	status scheduledCompletionDate completionDate pocOrganization pocFirstName pocLastName pocEmail pocPhoneNumber comments resources vulnerabilityDescription sourceIdentVuln severity* relevanceOfThreat* likelihood*

• Phone Number (only if First Name, Last Name, or Email have data) • Comments (Completed or Risk Accepted POA&M Items only) • Resources • Vulnerability Description • Source Identifying Vulnerability *Note: Certain eMASS instances also require the Risk Analysis fields to be populated: • Severity • Relevance of Threat • Likelihood • Impact • Residual Risk Level • Mitigations	impact* residualRiskLevel* mitigation*
POA&M Item with a review status of “Not Approved” cannot be saved if Milestone Scheduled Completion Date exceeds POA&M Item Scheduled Completion Date.	status
POA&M Item with a review status of “Approved” can be saved if Milestone Scheduled Completion Date exceeds POA&M Item Scheduled Completion Date.	status
POA&M Items that have a status of “Completed” and a status of “Ongoing” cannot be saved without Milestones.	status
POA&M Items cannot be saved if Milestone Description exceeds 2,000 characters.	description
POA&M Items that have a status of “Risk Accepted” cannot have milestones.	status
POA&M Items with a review status of “Approved” that have a status of “Completed” and “Ongoing” cannot update Scheduled Completion Date.	status
POA&M Items that have a review status of “Approved” are required to have a Severity Value assigned.	status
POA&M Items cannot be updated if they are included in an active package.	N/A
Archived POA&M Items cannot be updated.	N/A

POA&M Items with a status of "Not Applicable" will be updated through test result creation.	N/A
If the Security Control or Assessment Procedure does not exist in the system, we may have to just import POA&M Item at the System Level.	N/A

ARTIFACTS ENDPOINT

Business Rule	**Associated Parameter/Field**
Artifact cannot be saved if the fields below exceed the following character limits: • File Name – 1,000 characters • Description – 2,000 characters • Reference Page Number – 50 characters	fileName description refPageNumber
Artifact cannot be saved if the file does not have an allowable file extension/type.	file
Artifact version cannot be saved if an Artifact with the same file name already exist in the system.	fileName
Artifact cannot be saved if the file size exceeds 30MB.	file
Artifact cannot be saved if the following fields are missing data: • File Name • Template • Type • Category	fileName isTemplate type category
Artifact cannot be saved if the Last Review Date is set in the future.	lastReviewDate

CAC ENDPOINT

Business Rule	**Associated Parameter/Field**
Comments are not required at the first role of the CAC but are required at the second role of	comments

the CAC. Comments cannot exceed 10,000 characters.	

APPENDIX B – ENDPOINT PARAMETER/FIELD MASTER LIST

This appendix contains a master list of all parameters and fields found in the eMASS API. Please note that this list can be updated to reflect as future versions of the system.

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Systems	includePackage	Boolean	true, false If no value is specified, the default returns false to not include package information.	P
Systems	registrationType	String	Accepts multiple comma separated values including the following options: • assessAndAuthorize • assessOnly • guest • regular • functional • cloudServiceProvider • commonControlProvider	P/F
Systems	ditprId	String	93054	P
Systems	coamsId	String	SystemABC ID 8495	P
Systems	policy	String	Accepts single value from the following options: • diacap • rmf • reporting If no value is specified, the default returns RMF policy information for dual-policy systems.	P
Systems	includeDitprMetrics	Boolean	true, false If no value is specified, the default returns false to not include DITPR Metrics.	P
Systems	includeDecommissioned	Boolean	true, false If no value is specified, the default returns true to include decommissioned systems.	P
Systems	reportsForScorecard	Boolean	true, false	P

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			Used to filter results to only return systems that report to the DoD Cyber Hygiene Scorecard.	
Systems	systemId	Integer	[Read-Only] Unique system record identifier.	F
Systems	policy	String	[Read-Only] RMF/DIACAP Policy identifier for the system record. Values include the following options: • RMF • DIACAP	F
Systems	registrationType	String	[Read-Only] Registration type of the system record. Values include the following options: • Assess and Authorize • Assess Only • Guest • Regular • Functional • Cloud Service Provider	F
Systems	name	String	[Read-Only] Name of the system record.	F
Systems	acronym	String	[Read-Only] Acronym of the system record.	F
Systems	description	String	[Read-Only] Description of the system record.	F
Systems	instance	String	[Read-Only] Name of the top-level component that owns the system.	F
Systems	owningOrganization	String	[Read-Only] Owning organization of the system record. Values match the eMASS instance Organizational Hierarchy.	F
Systems	secondaryOrganization	String	[Read-Only] Secondary Organization that owns the system record.	F
Systems	versionReleaseNo	String	[Read-Only] Version/Release Number of system record.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Systems	systemType	String	[Read-Only] Type of the system record. RMF values include the following options: • IS Major Application • IS Enclave • Platform IT System DIACAP values include the following options: • Platform IT Interconnection • AIS Application • Outsourced IT-Based Process (DoD-controlled) • Enclave • Outsourced IT-Based Process (service provider shared)	F
Systems	isNSS	Boolean	[Read-Only] Is the system record a National Security System?	F
Systems	isPublicFacing	Boolean	[Read-Only] Does the system record have a public facing component/presence.	F
Systems	coamsId	Integer	[Read-Only] Corresponding Cyber Operational Attributes Management System (COAMS) identifier for the system record.	F
Systems	isTypeAuthorization	Boolean	[Read-Only] Identifies if system is a Type Authorization.	F
Systems	ditprId	String	[Read-Only] DITPR ID of the system record.	F
Systems	apmsId	String	[Read-Only] Same field as ditprId but displays as apmsId for Army only.	F
Systems	vasiId	String	[Read-Only] Same field as ditprId but displays as vasiId for VA only.	F
Systems	authorizationStatus	String	[Read-Only] Authorization Status of the system record. RMF values include the following options*:	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			• Authorization to Operate (ATO) • Authorization to Operate with Conditions (ATO w/Conditions) • Interim Authorization to Test (IATT) • Denied Authorization to Operate (DATO) • Not Yet Authorized • Decommissioned DIACAP values include the following options: • Authorization to Operate (ATO) • Interim Authorization to Operate (IATO) • Interim Authorization to Test (IATT) • Denied Authorization to Operate (DATO) • Unaccredited • Decommissioned *Some eMASS instances have custom Authorization Status values not captured in this list.	
Systems	authorizationDate	Date	[Read-Only] Authorization Date of the system record.	F
Systems	authorizationTerminationDate	Date	[Read-Only] Authorization Termination Date of the system record.	F
Systems	authorizationLength	String	[Read-Only] Length of system's Authorization. Calculated based from Authorization Date & Authorization Termination Date	F
Systems	termsForAuth	String	[Read-Only] Terms/Conditions for receiving and maintaining the system's Authorization. Assigned by the Authorizing Official.	F
Systems	securityPlanApprovalStatus	String	[Read-Only] Status of the approval of the system's RMF Security Plan. Values include the following options:	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			• Approved • Denied • Not Yet Approved	
Systems	securityPlanApprovalDate	Date	[Read-Only] Approval date of the system's RMF Security Plan.	F
Systems	missionCriticality	String	[Read-Only] Mission Criticality of the system record.	F
Systems	geographicalAssociation	String	[Read-Only] Geographical Association of the system record.	F
Systems	systemOwnership	String	[Read-Only] Ownership of the system record.	F
Systems	governingMissionArea	String	[Read-Only] Governing Mission Area of the system record.	F
Systems	primaryFunctionalArea	String	[Read-Only] Primary functional area of the system record.	F
Systems	secondaryFunctionalArea	String	[Read-Only] Secondary functional area of the system record.	F
Systems	primaryControlSet	String	[Read-Only] Primary Control Set of the system record. RMF values include the following options: • NIST SP 800-53 Revision 4 DIACAP values include the following options: • DoDI 8500.2	F
Systems	confidentiality	String	[Read-Only] Confidentiality of the system record. RMF values include the following options: • High • Moderate • Low	F
Systems	integrity	String	[Read-Only] Integrity of the system record. RMF values include the following options: • High • Moderate	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			• Low	
Systems	availability	String	[Read-Only] Availability of the system record. RMF values include the following options: • High • Moderate • Low	F
Systems	appliedOverlays	String	[Read-Only] Overlays applied to the system record.	F
Systems	rmfActivity	String	[Read-Only] RMF Activity of the system record.	F
Systems	crossDomainTicket	String	[Read-Only] Cross Domain Tickets of the system record.	F
Systems	ditprDonId	String	[Read-Only] DITPR-DON identifier of the system record.	F
Systems	mac	String	[Read-Only] MAC level of the system record. DIACAP values include the following options: • I • II • III	F
Systems	dodConfidentiality	String	[Read-Only] DoD Confidentiality level of the system record. DIACAP values include the following options: • Public • Sensitive • Classified	F
Systems	contingencyPlanTested	Boolean	[Read-Only] Has the system record's Contingency Plan been tested?	F
Systems	contingencyPlanTestDate	Date	[Read-Only] Date the system record's Contingency Plan was tested.	F
Systems	securityReviewDate	Date	[Read-Only] Date the system record's Annual Security Review was conducted.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Systems	hasOpenPoamItem	Boolean	[Read-Only] Does the system record have an Ongoing or Risk Accepted POA&M Item?	F
Systems	hasOpenPoamItem90to120PastScheduledCompletionDate	Boolean	[Read-Only] Does the system record have an Ongoing or Risk Accepted POA&M Item 90 to 120 days past its Scheduled Completion Date?	F
Systems	hasOpenPoamItem120PlusPastScheduledCompletionDate	Boolean	[Read-Only] Does the system record have an Ongoing or Risk Accepted POA&M Item 120 days past its Scheduled Completion Date?	F
Systems	impact	String	[Read-Only] Values include the following options: • Low • Moderate • High	F
Systems	hasCUI	Boolean	[Read-Only] Does the system record contain and/or process Controlled Unclassified information?	F
Systems	hasPII	Boolean	[Read-Only] Does the system record contain and/or process Personally Identifiable Information?	F
Systems	hasPHI	Boolean	[Read-Only] Does the system record contain and/or process Personal Health Information?	F
Systems	ppsmRegistryNumber	String	[Read-Only] Unique identifier for the DoD's Ports, Protocols, and Services Management Registry system.	F
Systems	interconnectedInformationSystemAndIdentifiers	String	[Read-Only] Identify the interconnected information systems and corresponding identifiers within control CA-3.	F
Systems	isPiaRequired	Boolean	[Read-Only] Does the system require a Privacy Impact Assessment?	F
Systems	piaStatus	String	[Read-Only] Status of the PIA.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			Values include the following options: - Not Started - In Progress - Completed Conditional on "isPiaRequired" being True.	
Systems	piaDate	Date	[Read-Only] Date in which the system's PIA took place. Conditional on "isPiaRequired" being True.	F
Systems	userDefinedField1	String	[Read-Only] User-defined field to augment Ad Hoc Reporting.	F
Systems	userDefinedField2	String	[Read-Only] User-defined field to augment Ad Hoc Reporting.	F
Systems	userDefinedField3	String	[Read-Only] User-defined field to augment Ad Hoc Reporting.	F
Systems	userDefinedField4	String	[Read-Only] User-defined field to augment Ad Hoc Reporting.	F
Systems	userDefinedField5	String	[Read-Only] User-defined field to augment Ad Hoc Reporting.	F
Systems	currentRmfLifecycleStep	String	[Read-Only] Displays the system's current step within the RMF Lifecycle. Values include the following options: - 1 – Categorize - 2 – Select - 3 – Implement - 4 – Assess - 5 – Authorize - 6 – Monitor	F
Systems	otherInformation	String	[Read-Only] Include any additional information required by the organization.	F
Systems	reportsForScorecard	Boolean	[Read-Only] Indicates if the system reports to the DoD Cyber Hygiene Scorecard.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Systems	ccsdNumber	String	[Read-Only] Identifier for specific connections to the system.	F
Systems	connectivity	String	[Read-Only] Choose connection type for the system.	F
Systems	highestSystemDataClassification	String	[Read-Only] The overall classification level of information that the System is approved to collect, process, store, and/or distribute.	F
Systems	overallClassification	String	[Read-Only] Same field as highestSystemDataClassification, but displays as overallClassification for NISP only.	F
Systems	isHVA	Boolean	[Read-Only] Indicates if the system contains High Value Assets. Does not display if value is null.	F
Systems	isFinancialManagement	Boolean	[Read-Only] Per OMB Circular A-127, a financial management system includes the core financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, and controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. The following are examples of financial management systems: core financial systems, procurement systems, loan systems, grants systems, payroll systems, budget formulation systems, billing systems, and travel systems.	F
Systems	isReciprocity	Boolean	[Read-Only] A reciprocity system is any information system that is part of a mutual agreement among participating organizations to	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.	
Systems	reciprocityExemption	String	[Read-Only] The following justifications are acceptable for exemption from reciprocity: (a) the existence of the system is classified (not the data, but the existence of the system) or (b) the system's authorization to operate is in the process of being pulled (e.g. DATO, Decommission).	F
Systems	cloudComputing	Boolean	[Read-Only] Is this a cloud-based IS?	F
Systems	cloudType	String	[Read-Only] Values include the following: • Hybrid • Private • Public	F
Systems	atcStatus	String	[Read-Only] The Authority to Connect decision. Values include the following: • Authority to Connect (ATC) • Denial of Authority to Connect (DATC) • Not Yet Connected • Decommissioned	F
Systems	isSaaS	Boolean	[Read-Only] Software as a Service (SaaS) cloud service model.	F
Systems	isPaaS	Boolean	[Read-Only] Platform as a Service (PaaS) cloud service model.	F
Systems	isIaaS	Boolean	[Read-Only] Infrastructure as a Service (IaaS) cloud service model.	F
Systems	otherServiceModels	String	[Read-Only] Free text field to include other cloud service models.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Systems	needDate	Date	[Read-Only] Indicates the date by which the System needs to be deployed to a production environment.	F
Systems	overallRiskScore	String	[Read-Only] The overall risk score of the system.	F
Systems	isHRR	Boolean	[Read-Only] Identifies whether a System has been designated as High Risk Review. Applicable to USCG and Navy only.	F
Systems	atcDate	Date	[Read-Only] The Connectivity Authorization Date.	F
Systems	atcTerminationDate	Date	[Read-Only] The Connectivity Authorization Termination Date.	F
Systems	systemDevelopmentLifeCycle	String	[Read-Only] Indicate the date by which the System needs to be deployed to a production environment. VA only.	F
Systems	isFISMAReportable	Boolean	[Read-Only] Is this IS reportable per Federal Information Security Management Act (FISMA) established requirements? VA only.	F
System Roles	role	String	Required parameter. Accepts single value from options available at base system-roles endpoint e.g., SCA.	P
System Roles	policy	String	Accepts single value from the following options: • diacap • rmf • reporting If no value is specified and more than one policy is available, the default returns the RMF policy information.	P
Controls	acronyms	String	AC-3,PM-6	P

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Controls	systemId	Integer	[Required] Unique system identifier.	F
Controls	name	String	[Read-Only] Name of control as defined in NIST SP 800-53 Revision 4.	F
Controls	acronym	String	[Required] Acronym of control as defined in the NIST SP 800-53 Revision 4.	F
Controls	ccis	String	[Read-Only] Comma separated list of CCIs associated with the control.	F
Controls	isInherited	Boolean	[Read-Only] Indicates whether a control is inherited.	F
Controls	modifiedByOverlays	String	[Read-Only] List of overlays that affect the control. An example would be the privacy overlay.	F
Controls	includedStatus	String	[Read-Only] Indicates the manner in which a control was included in the system's categorization.	F
Controls	complianceStatus	String	[Read-Only] Compliance status of the control.	F
Controls	responsibleEntities	String	[Required] Include written description of Responsible Entities that are responsible for the Security Control. Character Limit = 2,000.	F
Controls	implementationStatus	String	[Optional] Implementation Status of the Security Control for the information system. Values include the following options: • Planned • Implemented • Inherited • Not Applicable • Manually Inherited	F
Controls	commonControlProvider	String	[Conditional] Indicate the type of Common Control Provider for an "Inherited" Security Control. Values include the following options:	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			• DoD • Component • Enclave	
Controls	naJustification	String	[Conditional] Provide justification for Security Controls deemed Not Applicable to the system.	F
Controls	controlDesignation	String	[Required] Values include the following options: • Common • System-Specific • Hybrid	F
Controls	estimatedCompletionDate	Date	[Required] Field is required for Implementation Plan.	F
Controls	implementationNarrative	String	[Required] Includes security control comments. Character Limit = 2,000.	F
Controls	slcmCriticality	String	[Conditional] Criticality of Security Control regarding SLCM. Character Limit = 2,000.	F
Controls	slcmFrequency	String	[Conditional] Values include the following options: • Constantly • Daily • Weekly • Monthly • Quarterly • Semi-Annually • Annually • Every Two Years • Every Three Years • Undetermined	F
Controls	slcmMethod	String	[Conditional] Values include the following options: • Automated • Semi-Automated • Manual • Undetermined	F
Controls	slcmReporting	String	[Conditional] Method for reporting Security Controls for SLCM. Character Limit = 2,000.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Controls	slcmTracking	String	[Conditional] How Non-Compliant Security Controls will be tracked for SLCM. Character Limit = 2,000.	F
Controls	slcmComments	String	[Conditional] Additional comments for Security Control regarding SLCM. Character Limit = 4,000.	F
Controls	severity	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	F
Controls	vulnerabiltySummary	String	[Optional] Include vulnerability summary. Character Limit = 2,000.	F
Controls	recommendations	String	[Optional] Include recommendations. Character Limit = 2,000.	F
Controls	relevanceOfThreat	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	F
Controls	likelihood	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	F
Controls	impact	String	[Optional] Values include the following options: • Very Low • Low • Moderate	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			- High - Very High	
Controls	impactDescription	String	[Optional] Include description of Security Control's impact.	F
Controls	residualRiskLevel	String	[Optional] Values include the following options: - Very Low - Low - Moderate - High - Very High	F
Controls	testMethod	String	[Optional] Identifies the assessment method / combination that will determine if the security requirements are implemented correctly. Values include the following options: - Test - Interview - Examine - Test, Interview - Test, Examine - Interview, Examine - Test, Interview, Examine	F
Test Results	controlAcronyms	String	"AC-3,PM-6"	P
Test Results	ccis	String	"000123,000069"	P
Test Results	latestOnly	Boolean	true, false	P
Test Results	systemId	Integer	[Required] Unique eMASS identifier. Will need to provide correct number.	F
Test Results	control	String	[Read-Only] Control acronym associated with the test result. NIST SP 800-53 Revision 4 defined.	F
Test Results	cci	String	[Required] CCI associated with test result.	F
Test Results	isInherited	Boolean	[Read-Only] Indicates whether a test result is inherited.	F
Test Results	testedBy	String	[Required] Last Name, First Name.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			Character Limit = 100.	
Test Results	testDate	Date	[Required] Unix time format.	F
Test Results	description	String	[Required] Include description of test result. Character Limit = 4,000.	F
Test Results	type	String	[Read-Only] Indicates the location in the Control Approval Chain when the test result is submitted.	F
Test Results	complianceStatus	String	[Required] Values include the following options: • Compliant • Non-Compliant • Not Applicable	F
POA&Ms	scheduledCompletionDateStart	Date	1499644800	P
POA&Ms	scheduledCompletionDateEnd	Date	1499990400	P
POA&Ms	controlAcronyms	String	“AC-3,PM-6”	P
POA&Ms	ccis	String	“000123,000069”	P
POA&Ms	systemOnly	String	true, false	P
POA&Ms	systemId	Integer	[Required] Unique system identifier.	F
POA&Ms	poamId	Integer	[Required] Unique identifier representing the nth POA&M item entered into the site’s database.	F
POA&Ms	displayPoamId	Integer	[Required] Globally unique identifier for individual POA&M items, seen on the front-end as “ID”.	F
POA&Ms	isInherited	Boolean	[Read-only] Indicates whether a POA&M Item is inherited.	F
POA&Ms	externalUid	String	[Optional] Unique identifier external to the eMASS application for use with associating POA&Ms. Character Limit = 100.	F
POA&Ms	controlAcronym	String	[Optional] Control acronym associated with the POA&M item. NIST SP 800-53 Revision 4 defined.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
POA&Ms	cci	String	[Optional] CCI associated with POA&M item.	F
POA&Ms	status	String	[Required] Values include the following: • Ongoing • Risk Accepted • Completed • Not Applicable	F
POA&Ms	reviewStatus	String	[Read-only] Values include the following options: • Not Approved • Under Review • Approved	F
POA&Ms	vulnerabilityDescription	String	[Required] Provide a description of the POA&M item. Character Limit = 5,000.	F
POA&Ms	sourceIdentVuln	String	[Required] Include Source Identifying Vulnerability text. Character Limit = 2,000.	F
POA&Ms	securityChecks	String	[Optional] Security Checks that are associated with the POA&M.	F
POA&Ms	milestones	JSON	[Conditional] See Milestones endpoint for more details.	F
POA&Ms	pocOrganization	String	[Required] Organization/Office represented. Character Limit = 100.	F
POA&Ms	pocFirstName	String	[Conditional] First name of POC. Character Limit = 100.	F
POA&Ms	pocLastName	String	[Conditional] Last name of POC. Character Limit = 100.	F
POA&Ms	pocEmail	String	[Conditional] Email address of POC. Character Limit = 100.	F
POA&Ms	pocPhoneNumber	String	[Conditional] Phone number of POC. Character Limit = 100.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
POA&Ms	severity	String	[Conditional] Required for approved POA&M items. Values include the following options: • Very Low • Low • Moderate • High • Very High	F
POA&Ms	rawSeverity	String	[Optional] Values include the following options: • I • II • III	F
POA&Ms	relevanceOfThreat	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	F
POA&Ms	likelihood	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	F
POA&Ms	impact	String	[Optional] Values include the following options: • Very Low • Low • Moderate • High • Very High	F
POA&Ms	impactDescription	String	[Optional] Include description of Security Control’s impact.	F
POA&Ms	residualRiskLevel	String	[Optional] Values include the following options: • Very Low	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			• Low • Moderate • High • Very High	
POA&Ms	recommendations	String	[Optional] Include recommendations. Character Limit = 5,000.	F
POA&Ms	resources	String	[Required] List of resources used. Character Limit = 250.	F
POA&Ms	scheduledCompletionDate	Date	[Conditional] Required for ongoing and completed POA&M items. Unix time format.	F
POA&Ms	completionDate	Date	[Conditional] Field is required for completed POA&M items. Unix time format.	F
POA&Ms	extensionDate	Date	[Read-Only] Value returned for a POA&M item with review status “Approved” and has a milestone with a scheduled completion date that extends beyond the POA&M item’s scheduled completion date.	F
POA&Ms	comments	String	[Conditional] Field is required for completed and risk accepted POA&M items. Character Limit = 4,000.	F
POA&Ms	mitigation	String	[Optional] Include mitigation explanation. Character Limit = 2,000.	F
POA&Ms	isActive	Boolean	[Conditional] Optionally used in PUT to prevent uploading new duplicate/undesired milestones. Include an “isActive” field for the milestone and set it to false to prevent creating a new milestone.	F
Milestones	scheduledCompletionDateStart	Date	1499644800	P
Milestones	scheduledCompletionDateEnd	Date	1499990400	P
Milestones	systemId	Integer	[Required] Unique system identifier.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Milestones	milestoneId	Integer	[Required] Unique milestone identifier.	F
Milestones	poamId	Integer	[Required] Unique POA&M item identifier.	F
Milestones	description	String	[Required] Provide a description of the milestone. Character Limit = 2,000.	F
Milestones	scheduledCompletionDate	Date	[Required] Unix date format.	F
Artifacts	filename	String	“sample.pdf”	P
Artifacts	controlAcronyms	String	“AC-3,PM-6”	P
Artifacts	ccis	String	“000123,000069”	P
Artifacts	systemOnly	Boolean	true, false	P
Artifacts	filename	String	[Required] Filename should match exactly one file within the provided zip file. Character Limit = 1,000.	F
Artifacts	filename	Binary	[Required] Application/zip file. Max 30MB per artifact.	F
Artifacts	systemId	Integer	[Required] Unique system identifier.	F
Artifacts	isInherited	Boolean	[Read-Only] Indicates whether an artifact is inherited.	F
Artifacts	isTemplate	Boolean	[Required] Indicates whether an artifact is a template.	F
Artifacts	type	String	[Required] Values include the following options: • Procedure • Diagram • Policy • Labor • Document • Image • Other • Scan Result May also accept custom artifact type values set by system administrators.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Artifacts	category	String	[Required] Values include the following options: - Implementation Guidance - Evidence May also accept custom artifact category values set by system administrators.	F
Artifacts	description	String	[Optional] Artifact description. Character Limit = 2,000.	F
Artifacts	refPageNumber	String	[Optional] Artifact reference page number. Character Limit = 50.	F
Artifacts	ccis	String	[Optional] CCI associated with the artifact.	F
Artifacts	controls	String	[Optional] Control acronym associated with the artifact. NIST SP 800-53 Revision 4 defined.	F
Artifacts	mimeContentType	String	[Read-Only] Standard MIME content type derived from file extension.	F
Artifacts	fileSize	String	[Read-Only] File size of attached artifact.	F
Artifacts	artifactExpirationDate	Date	[Optional] Date artifact expires and requires review. Unix date format.	F
Artifacts	lastReviewDate		[Optional] Date artifact was last reviewed. Unix date format.	F
Artifacts Export	filename	String	[Required] “sample.pdf” Returns a binary file associated with the given filename.	P
Artifacts Export	compress	Boolean	[Optional] true, false Determines if a zip archive of a binary file associated with the given filename is returned.	P
CAC	controlAcronyms	String	“AC-3,PM-6”	P
CAC	systemId	Integer	[Required] Unique system identifier	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
CAC	controlAcronym	String	[Required] Control acronym associated with the CAC. NIST SP 800-53 Revision 4 defined.	F
CAC	complianceStatus	String	[Read-Only] Compliance status of the control.	F
CAC	currentStageName	String	[Read-Only] Role in current stage.	F
CAC	currentStage	Integer	[Read-Only] Current stage in the Control Approval Chain.	F
CAC	totalStages	Integer	[Read-Only] Total number of steps in Control Approval Chain.	F
CAC	comments	String	[Conditional] 2,000 Characters.	F
PAC	systemId	Integer	[Required] Unique system identifier.	F
PAC	workflow	String	[Required] Values include the following: • Assess and Authorize • Assess Only • Security Plan Approval	F
PAC	name	String	[Required] Package name. Character Limit = 100.	F
PAC	currentStageName	String	[Read-Only] Name of the current stage in the active workflow.	F
PAC	currentStage	Integer	[Read-Only] Number of the current stage in the active workflow.	F
PAC	totalStages	Integer	[Read-Only] Total number of stages in the active workflow.	F
PAC	daysAtCurrentStage	Integer	[Read-Only] Indicates the number of days at current workflow stage.	F
PAC	comments	String	[Required] Comments related to package approval chain. Character Limit = 4,000.	F
CMMC Assessments	sinceDate	Date	Required parameter. Unix date format.	P
CMMC Assessments	operation	String	[Read-Only] Indicates the action that should be taken on the assessment record since the provided sinceDate.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			Values include the following options: • ADDED • UPDATED • DELETED	
CMMC Assessments	hqOrganizationName	String	[Read-Only] The name of the DIB Company.	F
CMMC Assessments	uei	String	[Read-Only] The Unique Entity Identifier assigned to the DIB Company.	F
CMMC Assessments	cageCodesInScope	String	[Read-Only] The five position code(s) associated with the Organization Seeking Certification (OSC).	F
CMMC Assessments	oscName	String	[Read-Only] The name of the Organization Seeking Certification.	F
CMMC Assessments	scope	String	[Read-Only] The scope of the OSC assessment. Values include the following options: • Enterprise • Non-Enterprise	F
CMMC Assessments	scopeDescription	String	[Read-Only] Brief description of the scope of the OSC assessment.	F
CMMC Assessments	awardedCMMCLevel	String	[Read-Only] Values include the following options: • Not Certified • Level 1 • Level 2 • Level 3 • Level 4 • Level 5	F
CMMC Assessments	expirationDate	Date	[Read-Only] Expiration date of the awarded CMMC certification. Unix date format.	F
CMMC Assessments	assessmentId	String	[Read-Only] Unique identifier for the assessment/certificate. “41b89528-a7a8-470a-90f4-c3fd1267d6f7”	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
CMMC Assessments	modelVersion	String	[Read-Only] Version of the CMMC Model used as part of the assessment.	F
CMMC Assessments	highestLevelOrderCageCode	String	[Read-Only] Identifies the highest-level CAGE Code associated with a given organization.	F
CMMC Assessments	certificationUniqueId	String	[Read-Only] Identifies the unique ID that is associated with a given CMMC certification for an organization.	F
CMMC Assessments	poam	Boolean	[Read-Only] Identifies whether any security requirements received a POA&M during the assessment.	F
CMMC Assessments	overallScore	Integer	[Read-Only] Identifies the overall calculated score for the assessment based on the assigned values to each applicable security requirement.	F
CMMC Assessments	oscAssessmentOfficialLastName	String	[Read-Only] Last name of the company official contracting with the C3PAO for the assessment.	F
CMMC Assessments	oscAssessmentOfficialFirstName	String	[Read-Only] First name of the company official contracting with the C3PAO for the assessment.	F
CMMC Assessments	oscAssessmentOfficialEmail	String	[Read-Only] Email of the company official contracting with the C3PAO for the assessment.	F
CMMC Assessments	oscAssessmentOfficialTitle	String	[Read-Only] Title of the company official contracting with the C3PAO for the assessment.	F
CMMC Assessments	sspName	String	[Read-Only] Name of the System Security Plan.	F
CMMC Assessments	sspVersion	String	[Read-Only] Version of the System Security Plan.	F
CMMC Assessments	sspDate	Date	[Read-Only] Date of the System Security Plan. Unix date format.	F
Static Code Scans	applicationName	String	[Required] Name of the software application that was assessed.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Static Code Scans	cweId	String	[Required] The Common Weakness Enumerator (CWE) identifier.	F
Static Code Scans	clearFindings	Boolean	[Optional] When used by itself, can clear out all application findings for a single application/version pairing.	F
Static Code Scans	codeCheckName	String	[Required] Name of the software vulnerability or weakness.	F
Static Code Scans	count	Integer	[Required] Number of instances observed for a specified finding.	F
Static Code Scans	rawSeverity	String	[Optional] Values include the following options: • Low • Medium • Moderate • High • Critical Note: In eMASS, values of “Critical” will appear as “Very High”, and values of “Medium” will appear as “Moderate” Note: Any values not listed as options in the list above will map to “Unknown” and appear as blank values.	F
Static Code Scans	scanDate	Date	[Required] Unix date format.	F
Static Code Scans	version	String	[Required] The version of the application.	F
Workflow Definitions	includeInactive	Boolean	[Optional] true, false If no value is specified, the default returns false to not include outdated workflow definitions.	P
Workflow Definitions	registrationType	String	[Optional] Accepts multiple comma-separated values including the following options: • assessAndAuthorize • assessOnly • guest • regular • functional	P

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			• cloudServiceProvider • commonControlProvider For example: If the guest value is used, only workflows available to systems with a guest registration type will be returned.	
Workflow Definitions	description	String	[Read-Only] Description of the workflow or the stage transition. For stage transitions, this matches the action dropdown that appears for PAC users.	F
Workflow Definitions	endStage	String	[Read-Only] The landing stage that is active after performing a transition.	F
Workflow Definitions	isActive	String	[Read-Only] Returns true if the workflow is available to the site. Note: Unless using the includeInactive parameter, workflow definitions set to false for isActive will be excluded. Note: If an admin disables the workflow in the Administration module, it will be set to false for isActive. Note: If a workflow definition is updated, all prior versions will automatically be set to false for isActive.	F
Workflow Definitions	name	String	[Read-Only] Name of the workflow stage. Note: For older workflows, this will match the user assigned to the stage.	F
Workflow Definitions	version	Integer	[Read-Only] Version of the workflow definition.	F
Workflow Definitions	workflow	String	[Read-Only] The workflow type.	F
Workflow Instances	includeComments	Boolean	true, false If no value is specified, the default returns true to include transition comments.	P

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			Note: Corresponds to the Comments textbox that is required at most workflow transitions. Does not include other text input fields such as Terms / Conditions for Authorization.	
Workflow Instances	pageIndex	Integer	If no value is specified, the default returns results from the first page with an index of 0.	P
Workflow Instances	sinceDate	Date	Unix Date format. Note: Filters off the lastEditedDate field. Note: The authorization/assessment decisions on completed workflows can be edited for up to 30 days after the initial decision is made.	P
Workflow Instances	status	String	Values include the following options: • active • inactive • all If no value is specified, the default returns all to include both active and inactive workflows. Note: Any workflows at a current stage of Complete or Canceled are inactive. Legacy workflows with a current stage of Authorized, Approved, or Denied are also inactive. Ongoing workflows currently at other stages are active.	P
Workflow Instances	comments	String	[Read-Only] Comments entered by the user when performing the transition.	F
Workflow Instances	createdBy	String	[Read-Only] User that performed the workflow transition.	F
Workflow Instances	createdDate	Date	[Read-Only] Date the workflow instance or the workflow transition was created.	F
Workflow Instances	currentStage	String	[Read-Only] Name of the current stage.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Workflow Instances	description	String	[Read-Only] Description of the stage transition. This matches the action dropdown that appears for PAC users.	F
Workflow Instances	endStage	String	[Read-Only] The landing stage that is active after performing a transition.	F
Workflow Instances	lastEditedBy	String	[Read-Only] User that last acted on the workflow.	F
Workflow Instances	lastEditedDate	Date	[Read-Only] Date the workflow was last acted on.	F
Workflow Instances	packageName	String	[Read-Only] The package name.	F
Workflow Instances	startStage	String	[Read-Only] The beginning stage that is active before performing a transition.	F
Workflow Instances	systemName	String	[Read-Only] The system name.	F
Workflow Instances	version	Integer	[Read-Only] Version of the workflow definition.	F
Workflow Instances	workflow	String	[Read-Only] The workflow type.	F
Workflow Instances	workflowInstanceId	Integer	[Read-Only] Unique workflow instance identifier.	F
Cloud Resources	assessmentProcedure	String	[Optional] Comma separated correlation to Assessment Procedure (i.e. CCI number for DoD Control Set). Character Limit = 100.	F
Cloud Resources	complianceCheckTimestamp	Date	[Optional] Unix date format.	F
Cloud Resources	complianceReason	String	[Optional] Reason/comments for compliance result. Character Limit = 1,000.	F
Cloud Resources	control	String	[Optional] Comma separated correlation to Security Control (e.g. exact NIST Control acronym). Character Limit = 100.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Cloud Resources	cspAccountId	String	[Optional] System/owner's CSP account ID/number. Character Limit = 100.	F
Cloud Resources	cspPolicyDefinitionId	String	[Required] Unique identifier/compliance namespace for CSP/Resource's policy definition/compliance check. Character Limit = 500.	F
Cloud Resources	cspRegion	String	[Optional] CSP region of system. Character Limit = 100.	F
Cloud Resources	initiatedBy	String	[Optional] Email of POC. Character Limit = 100.	F
Cloud Resources	isBaseline	Boolean	[Optional] True/false flag for providing results as baseline. If true, all existing compliance results for the resourceId will be replaced by results in the current call.	F
Cloud Resources	isCompliant	Boolean	[Required] Compliance status of the policy for the identified cloud resource.	F
Cloud Resources	policyDefinitionTitle	String	[Required] Friendly policy/compliance check title. Recommend short title. Character Limit = 2,000.	F
Cloud Resources	policyDeploymentName	String	[Optional] Name of policy deployment. Character Limit = 500.	F
Cloud Resources	policyDeploymentVersion	String	[Optional] Version of policy deployment. Character Limit = 50.	F
Cloud Resources	provider	String	[Required] Cloud service provider name. Character Limit = 100.	F
Cloud Resources	resourceId	String	[Required] Unique identifier/resource namespace for policy compliance result. Character Limit = 500.	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
Cloud Resources	resourceName	String	[Required] Friendly name of Cloud resource. Character Limit = 500.	F
Cloud Resources	resourceType	String	[Required] Type of Cloud resource. Character Limit = 100.	F
Cloud Resources	severity	String	[Optional] Values include the following options: • Low • Medium • High • Critical	F
Cloud Resources	tags	String	[Optional] Informational tags associated to results for other metadata.	F
Containers	benchmark	String	[Required] Identifier of the benchmark/grouping of compliance results. (e.g. for STIG results, provide the benchmark id for the STIG technology). Character Limit = 100.	F
Containers	containerId	String	[Required] Unique identifier of the container. Character Limit = 500.	F
Containers	containerName	String	[Required] Friendly name of the container. Character Limit = 500.	F
Containers	isBaseline	Boolean	[Optional] True/false flag for providing results as baseline. If true, all existing compliance results for the provided *benchmark* within the *container* will be replaced by results in the current call.	F
Containers	lastSeen	Date	[Required] Unix date format.	F
Containers	message	String	[Optional] Comments for the result. Character Limit = 1,000.	F
Containers	namespace	String	[Optional] Namespace of container in container orchestration (e.g. Kubernetes namespace).	F

Endpoint	Name	Type	Detail/Example	Parameter (P) / Field (F)
			Character Limit = 100.	
Containers	podIp	String	[Optional] IP address of pod (e.g. Kubernetes assigned IP) Character Limit = 100.	F
Containers	podName	String	[Optional] Name of pod (e.g. Kubernetes pod). Character Limit = 100.	F
Containers	ruleId	String	[Required] Identifier for the compliance result, vulnerability, etc. the result is for. (e.g. for STIGs, use the SV-XXXrXX identifier; for CVEs, the CVE-XXXX-XXX identifier, etc.).	F
Containers	status	String	[Required] Values include the following options: • Pass • Fail • Other • Not Reviewed • Not Checked • Not Applicable	F
Containers	tags	String	[Optional] Informational tags associated to results for other metadata.	F
Containers	time	Date	[Required] Datetime of scan/result. Unix date format.	F

APPENDIX C – ACRONYMS

Acronym	Definition
AP	Assessment Procedure
API	Application Programming Interface
ATC	Authority to Connect
CAC	Control Approval Chain
CCI	Control Correlation Identifier
CCSD	Command Communications Service Designator
CMMC	Cybersecurity Maturity Model Certification
CSP	Cloud Service Provider
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DoD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service
HTTP	Hypertext Transfer Protocol
NIPR	Non-secure Internet Protocol Router
PAC	Package Approval Chain
PKI	Public Key Infrastructure
POA&M	Plan of Action & Milestones
RMF	Risk Management Framework
SAR	Security Assessment Report
SIPR	Secure Internet Protocol Router
SLCM	System Level Continuous Monitoring
SP	Security Plan