Effective Date: March 2020
Expiration Date: March 2025

GSFC ESDIS CMO
March 27, 2020
Released

423-RQMT-018, Rev A
Earth Science Data and Information Systems (ESDIS) Project, Code 423

NASA-Compliant General Application Platform (NGAP) Requirements Specification

Goddard Space Flight Center
Greenbelt, Maryland

Nat ona Aeronaut cs and
Space Adm n strat on

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

NGAP Requirements Specification
Signature/Approval Page

Prepared by:

Signature obtained on file ***03/27/2020***
Stephen Berrick — Date
ESDIS Science Systems Development Manager
NASA GSFC Code 586

Approved by:

Signature obtained on file ***03/27/2020***
Mark McInerney — Date
ESDIS Deputy Project Manager Technical
NASA GSFC Code 423

Approved by:

Signature obtained on file ***03/27/2020***
Andrew Mitchell — Date
ESDIS Project Manager
NASA GSFC Code 423

[Electronic] Signatures available in B32 Room E148
online at: / https://ops1-cm.ems.eosdis.nasa.gov/cm2/

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Preface

This document is under ESDIS Project configuration control. Once this document is approved, ESDIS approved changes are handled in accordance with Class I and Class II change control requirements described in the ESDIS Configuration Management Procedures., Changes to this document shall be verified a Document Change Notice (DCN) and implemented by change bars or by complete revision.

Any questions should be addressed to: esdis-esmo-cmo@lists.nasa.gov

ESDIS Configuration Management Office (CMO)
NASA/GSFC
Code 423
Greenbelt, Md. 20771

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Abstract

This document provides the NASA-compliant General Application Platform (NGAP) system requirements presented as a set of user stories following the Agile development approach.

***Keywords**: NGAP 2.0, Cloud, Platform, CloudTamer, Terraform*

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Change History Log

Revision	Effective Date	Description of Changes (Reference the CCR & CCB Approval Date)
Original, Rev-	08/23/2019	CCR 423-ESDIS-239; CCB Approved 06/25/2019 Pages: Baseline cover through page 44 Acronyms
Rev A	03/27/2020	CCR 423-ESDIS-287; CCB Approved 03/26/2020 Pages: Revision A cover through page 34

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Table of Contents

1 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
1.3 Related Documentation 1
1.3.1 Applicable Documents 1
1.3.2 Reference Documents 1
1.4 Agile Programming and Requirements Analysis 2
1.5 User Roles 2
2 ARCHITECTURE 3
2.1 Account Management and Federated Login 3
2.1.1 Management Accounts 3
2.1.2 CloudTamer 3
2.1.3 Application/End User Auth 3
2.1.4 Account Provisioning 3
2.1.5 Access Requests 4
2.1.5.1 Roles 4
2.1.5.2 Prerequisites 6
2.1.5.3 Additional Requirements 6
2.1.6 End User Application Authentication/Authorization 6
2.1.7 NGAP-Managed Roles/Policies 7
2.1.7.1 Cloud Access Roles 7
2.1.7.2 Login Roles 7
2.1.7.3 IAM Policies 7
2.1.7.4 Application-Specific IAM Policies 7
2.1.7.5 Whitelist vs. Blacklist Policies 7
2.1.7.6 NGAP-Managed Resources 8
2.1.8 User-Managed Roles/Policies 8
2.1.9 AWS Access Keys 9
2.1.9.1 User-Provisioned Access Keys 9
2.1.9.2 Deployment Keys 9
2.1.9.3 Roles vs. Users 9
2.1.10 Account Types and Hierarchy 9
2.1.10.1 Organization Structure 10
2.1.11 Infrastructure Automation 10
2.1.11.1 Infrastructure Automation Account 10
2.2 VPC/Network Layout 11
2.2.1 Application Accounts 11
2.2.2 Classless Inter-domain Routing (CIDR) Ranges 11
2.2.3 Public-Facing Endpoints 11
2.2.3.1 Private VPCs 11
2.2.3.2 Internet Services Account 12
2.2.3.3 TLS Certificates 12
2.2.3.4 Non-VPC Endpoints 12
2.2.3.5 Public-Facing Endpoint Request 12

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2.2.3.6 Non-VPC Resources ... 14
2.2.3.7 Elastic Load Balancing ... 14
2.2.3.8 Intrusion Detection and Packet Capture ... 14
2.2.3.9 Routing ... 15
2.2.3.10 Future Enhancements ... 15
2.2.3.11 Web Application Firewall (WAF) ... 15
2.2.4 Outgoing Internet Access ... 15
2.3 Monitoring and Security Controls ... 16
2.3.1 Log Aggregation/Forwarding ... 16
2.3.1.1 CloudWatch Logs ... 16
2.3.1.2 Access Logs ... 16
2.3.2 Packet Capture ... 17
2.3.3 Monitoring ... 17
2.3.4 Scanning and Inventory ... 18
2.3.4.1 Scanning ... 18
2.3.4.2 EC2 Host & Software Inventory ... 18
3 REQUIREMENTS ... 23
3.1 Introduction ... 23
3.2 Account and Access Management ... 23
3.3 Authentication ... 24
3.4 Logging ... 24
3.5 Billing and Cost ... 25
3.6 Scanning and Software Inventory ... 25
3.7 Outgoing Internet Access ... 25
3.8 CI/CD ... 26
3.9 Security Requirements ... 27
3.9.1 System Integrity ... 27
3.9.2 System and Communications Protection ... 27
3.9.3 Risk Assessment ... 28
3.9.4 Contingency Planning ... 28
3.9.5 Supporting Documents ... 28
3.9.6 Incident Response ... 29
3.9.7 Configuration Management ... 29
3.9.8 Identification and Authentication ... 30
3.9.9 Access Control ... 30
3.9.10 Security Awareness and Training Policy and Procedures ... 31
3.9.11 Audit and Accountability Policies and Procedures ... 31
3.9.12 Security Assessment and Authorization Policies and Procedures ... 32
3.10 EC2 Instance Patching ... 32
Appendix A Abbreviations and Acronyms ... 33

List of Tables

Table 1. Users Roles ... 5
Table 2. EC2 Host and Software Inventory ... 21

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

1 INTRODUCTION

NGAP 2.0 is an evolution of the NASA-Compliant General Application Platform towards a multi-account, Infrastructure-as-a-Service (IaaS) model giving individual application owners their own Amazon Web Services (AWS) accounts, with security controls and National Aeronautics and Space Administration (NASA) policies implemented and managed on their behalf by the NGAP team.

1.1 Purpose

The purpose of this document is to baseline the requirements aligned with the goal to deliver the NGAP 2.0 design and architecture at the committed time, with the required functionality, per the scheduled dates embodied in the critical path and roadmap. NGAP developers employ development processes that demonstrate results within baselined time increments, without compromising quality or adherence to customer requirements.

NGAP provides traceability of requirements throughout the systems design lifecycle (SDLC). The trail from testing through to design and ultimately specification, enables future success for development. The JIRA tool further supports and facilitates maintaining traceability links when new baselines are created.

1.2 Scope

The scope of this document describes the NGAP requirements as a set of "user stories" following the Agile development approach. To provide requirements traceability, the user stories are also mapped to the epics specified under NGAP project in JIRA.

1.3 Related Documentation

The latest versions of all documents below should be used. The latest Earth Science Data and Information System (ESDIS) Project documents can be obtained from Uniform Resource Locator (URL): https://ops1-cm.ems.eosdis.nasa.gov. ESDIS documents have a document number starting with either 423 or 505. Other documents are available for reference in the ESDIS project library website at: https://doclib.eosdis.nasa.gov/ or the Earthdata Wiki at https://wiki.earthdata.nasa.gov unless indicated otherwise.

1.3.1 Applicable Documents

The following documents are not binding on the content but referenced herein and, amplify or clarify the information presented in this document.

Document Number	Document Title
N/A	NGAP 2.0 Design
N/A	Terraform CI/CD & Security Plan

1.3.2 Reference Documents

The following documents are not binding on the content but referenced herein and, amplify or clarify the information presented in this document.

Document Number	Document Title
NPR 2810.1A	Security of Information Technology document

Use or disclosure of data contained on this page is subject to the restriction(s) on the title page of this document.

1.4 Agile Programming and Requirements Analysis

The EOSDIS Evolution and Development 2 (EED2) teams are using Agile Programming methodologies throughout the software development lifecycle, including the requirements analysis phase. The process of developing requirements has not changed much from other software programming management methods such as waterfall or iterative methods. The two major differences between Agile and other methods are:

a. A greater emphasis on stakeholder participation; and
b. Requirements are allowed to evolve throughout the Agile development process to account for changing priorities, new requirements that were left out initially, or changes due to issues encountered during development and testing.

These two differences may not seem all that different from other methods; however, requirements managed by Agile processes provide for a much more flexible framework from which to develop software.

In this document, requirements may/or may not be captured as a set of User Stories written in the form:

"As a <role> I want to <action> so that I can <explanation>".

The requirement may be told from the perspective of an NGAP user, or developer role instead of the generic "The system shall...". Requirements written in this form help to refine the system requirement by identifying the user or consumer of the required functionality, the function that the user needs, and why this function is needed. The concept of providing value to the system user is reflected in the explanation of the user story form. This provides the rationale or the benefit of the requirement.
This also allows the developer to choose from "Best Practices" techniques on how to best implement a requirement. The first principle of the Agile Manifesto is:

Our highest priority is to satisfy the customer through early and continuous delivery of valuable software. (http://agilemanifesto.org/principles.html)

The NGAP requirements and user stories will be tracked and maintained using Atlassian's Jama Requirements Management tool. The user stories presented in this document are written to a Systems Requirements level and will be kept in sync with the user stories maintained in Jama.

1.5 User Roles

The following roles will be used to clarify NGAP User Stories by defining system boundaries and those that are responsible for completing the tasks associated with these requirements:

a. NGAP
b. NGAP Administrator
c. Budget Analyst
d. NGAP Security Administrator
e. Application Owner
f. NGAP User
g. NGAP Systems Architect

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2 ARCHITECTURE

2.1 Account Management and Federated Login

NGAP 2.0 adheres to a multi-account strategy, where each application and environment is given a separate AWS account–managed by NGAP–within which to work. This allows for:

- Isolation of the resources and development work in each account.
- Fine-grained control over user permissions within AWS (users can have different permissions in an application's System Integration Testing (SIT), User Accepting Testing (UAT) or Production accounts).
- Simplified tracking of billing and resource usage by various projects, without the overhead of maintaining error-prone and human driven tagging schemes.
- Account-specific, budget-based egress/throttling controls to mitigate unbounded data transfer costs per application.
- Improved ability to roll out security controls and monitoring in an automated fashion, without the risk of interfering with other projects and teams.
- Reduce the potential "blast zone" of a compromised account or resource to that specific application/account, without affecting other applications running in NGAP 2.0.

2.1.1 Management Accounts

In addition to the application/project-specific accounts (the Managed Accounts), there will be one or more Management Accounts, which only administrative users (NGAP, Networks and Security team members) will have access to. These accounts will host centralized logging, monitoring, and other shared services (see the sections on Log Aggregation and Monitoring for details) that are used by or from Managed Accounts.

2.1.2 CloudTamer

We will be making use of CloudTamer (https://stratussolutions.com/tamethecloud/), an integrated solution for AWS account management, budget enforcement, and compliance automation. NGAP users will login into the AWS console using CloudTamer's federated login; CloudTamer itself will delegate authentication to NASA IdMAX through Launchpad. Multi-factor authentication (MFA) using a Personal Identity Verification (PIV) card or Rivest, Shamir and Adelman (RSA) token will be required to access the CloudTamer console and federated login.

2.1.3 Application/End User Auth

Applications hosted on NGAP are responsible for integrating their own end-user authentication and authorization (if they require this functionality). This may be through Earthdata Login where login information is needed purely for metrics purposes, or Launchpad when NASA-compliant secure authentication is required.

2.1.4 Account Provisioning

AWS accounts will be created by Enterprise Managed Cloud Computing (EMCC) and then turned over to the NGAP team to be imported into CloudTamer and integrated with the Infrastructure Automation stack.

Use or disclosure of data contained on this page is subject to the restriction(s) on the title page of this document.

2.1.5 Access Requests

All NGAP users–application owners, NGAP admins/operators, billing/finance personnel–will request access to NGAP through the NASA Access Management System (NAMS) (https://nams.nasa.gov). CloudTamer will be integrated with NASA Launchpad via Security Assertion Markup Language (SAML) to enable the use of the roles provisioned via NAMS.

2.1.5.1 Roles

The profiles of anticipated users are listed in Table 1.

Table 1. Users Roles

Role Name	Use Case	Description	Proposed Level of Risk	Additional NAMS Approval Required
FINANCE-ADMIN	Users who need administrative access to finance for all accounts.	This profile is representative of role that the NASA official with project oversight would assume. This would allow the user to perform financial administrative tasks without granting access to any of the managed accounts.	40	
NGAP-SA	Users who need console access to all accounts with `root` permissions.	This is a profile representative of NGAP Tier 2 administrators. These users would have console access to all accounts and have the ability to alter accounts and account monitoring.	40	GSFC FPD Elevated Privileges
NGAP-ADMIN	Users who need console access to all accounts with the ability to manage groups and manage users.	This is a profile representative of NGAP Tier 1 administrators. These users would have console access to all accounts and the ability to alter user-access.	40	GSFC FPD Elevated Privileges

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Role Name	Use Case	Description	Proposed Level of Risk	Additional NAMS Approval Required
FINANCE-VIEWER	Users who need read-only access to finance information for all accounts.	This is a profile representative of NASA official subordinate to FINANCE-ADMIN and is tasked with monitoring the finances of accounts.	20	
APP-FINANCE-VIEWER	Users who need read-only access to finances of a specific account.	This is a role representative of stakeholders/managers on a projects housed in an account, who otherwise do not perform development or operations tasks on the project.	20	
NGAP-SEC	Users who need read-only access to all account for security audits	This is a role for NGAP security teams who will need to view(without edit) logs and IAM policy.	40	GSFC FPD Elevated Privileges
APP-ADMIN	Users with administrative control of a particular account	This is a role representative of an application owner.	30	
APP-DEVELOPER	Users who need console access to a particular account	This is a role representative of a developer on projects housed in an account.	30	
N/A	Users who need read-only access to finances AND access to the console.	This would be a combination of APP-FINANCE-VIEWER and APP-DEVELOPER.		

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2.1.5.2 Prerequisites

Users looking to occupy particular role(s) would request the roles by submitting a NAMS request governed by a NAMS workflow. Implicit in the NAMS process is a requirement that all users who need access must have:

- A NASA Agency User ID (AUID).
- Physical access to the NASA network/NASA Virtual Private Network (VPN), or a NAMS request issued on their behalf by a user with NAMS access.

2.1.5.3 Additional Requirements

All users should have a confidence level of at least 20 (Low Risk - OPM Tier 1). This would correspond to a value of 20 or more for the "Level of Risk" in an NGAP asset request.

All users should take SATERN training commensurate to the level of access they will be granted:

- All roles will require the completion of the Core Services on AWS (COURSE SS-CL_ACDA_A02_IT_ENUS) SATERN training
- Up-to-date IT Security Training--either annual or initial for new employees
- NGAP-SEC, NGAP-ADMIN, NGAP-SA requests will be dependent on approval for GSFC Flight Projects Directorate (FPD) Elevated Privileges which has the following SATERN training requirements:
    - ELEVATED PRIVILEGES ON NASA INFORMATION SYSTEMS
    - IT SECURITY FOR SYSTEMS ADMINISTRATORS - BEGINNING LEVEL
    - IT SECURITY FOR SYSTEMS ADMINISTRATORS - INTERMEDIATE LEVEL
    - DevOps Fundamentals: Tools, Technologies, and Infrastructures (COURSE SS-OS_DEVO_A01_IT_ENUS)

Detailed CloudTamer NAMS Workflow can be found at CloudTamer NAMS Workflow.

2.1.6 End User Application Authentication/Authorization

Individual applications hosted on NGAP may have their own authentication and authorization requirements. Users who log into an application hosted on NGAP (as opposed to logging into NGAP itself) will not access said application through CloudTamer. The application owner is responsible for implementing their own authentication and authorization mechanism, which MUST adhere to NASA/ESDIS requirements. NGAP recommends that application owners use Launchpad and NAMS for authentication and authorization; or Earthdata Login wherever user metrics, but no actual authorization, is required. Application owners may ONLY use another authentication/authorization mechanism if it meets NASA/ESDIS requirements, and they can provide the relevant policy documentation.

Note: Earthdata Login does not satisfy NASA requirements for authentication and authorization, and should only be used where login is needed only for user metrics, not for authentication or authorization.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2.1.7 NGAP-Managed Roles/Policies

The permissions that NGAP users will have in Managed Accounts are configured using AWS Identity Access Management (IAM) Policies, CloudTamer Permissions, and Cloud Access Roles in CloudTamer, for both NGAP team members and NGAP-hosted application team members.

2.1.7.1 Cloud Access Roles

CloudTamer uses Cloud Access Roles to allow users to log in to the AWS Console or use the AWS Application Programming Interface (API) / Command Line Interface (CLI). When logging in using a particular Cloud Access Role, you receive any IAM permissions granted to that Role through its attached AWS IAM Policies, as well as any Cloud Rules that are applied to the account or the Organizational Unit (OU) that it's a member of.

Cloud Access Roles are project-specific and can only be used to log into accounts under that project. AWS IAM Policies are defined globally, then assigned to specific Cloud Access Roles as needed.

2.1.7.2 Login Roles

Users will request access to NGAP through NAMS, as documented in CloudTamer NAMS Workflow. When a user's access is approved, they will be able to log into CloudTamer through Launchpad, with the roles that were requested and approved in NAMS. For "global" roles, such as FINANCE-ADMIN or NGAP-SA, roles will be directly associated with the relevant IAM Policies (what the user can do within the managed AWS accounts) and CloudTamer Permissions (what the user can do within CloudTamer).

Application-specific roles, which include APP-DEVELOPER and APP-FINANCE-VIEWER, will be granted permissions that are further scoped down to specific OUs (Organizational Units) or Projects. For example, an APP-DEVELOPER will be permitted to log into only the account(s) to which they have been explicitly added (through Cloud Access Roles).

2.1.7.3 IAM Policies

Each of the Cloud Access Roles used to implement project-specific access will consist of multiple AWS IAM Policies. Additionally, the policies attached to NGAP Operators in the Management Account are likely to differ from the policies that will be in place in Managed Accounts, to prevent any of NGAP's centralized logging, monitoring and other security controls from being modifiable.

2.1.7.4 Application-Specific IAM Policies

In some cases, an application team may need another more specific role; for example, a Database Administrator should have access to view and modify Relational Database Service (RDS) instances for an application, but not modify any other resources. In this case, NGAP will create an application-specific AWS IAM Policy in CloudTamer, e.g. "NGAP {Application Name} Application DBA (Database Administrator)", and assign it to the role in question.

2.1.7.5 Whitelist vs. Blacklist Policies

To simplify AWS IAM Policy management, we will separate the policies that we create into two classes: whitelist policies, which allow the use only of certain approved services and resources;

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

and blacklist policies, which explicitly deny actions that NGAP users should not be permitted. In general, a particular action (for example, creating a Simple Storage Service (S3) bucket and modifying data init) will be permitted using a whitelist policy; then exceptions (e.g. denying any actions on an NGAP-controlled monitoring/logging bucket) will be added using a blacklist policy.

This will allow us to keep a "library" of different whitelist policies defining the services and actions that different user types can perform, while consistently attaching our blacklist policies to all of the (project-specific) managed roles.

2.1.7.6 NGAP-Managed Resources

As previously mentioned, AWS IAM Policies in CloudTamer are defined globally and then used (through Cloud Access Roles) in specific projects and accounts. One resulting limitation is that the Policies we define cannot have account-specific Amazon Resource Names (ARNs) in them, or resource names that are generated e.g. by CloudFormation or another Infrastructure Automation tool. NGAP-managed resources in Managed Accounts will need to follow a naming convention that ensures a single "blacklist" policy defined in CloudTamer will apply to the relevant resource(s), regardless of AWS account. All of the NGAP-managed resources should be prefixed, where possible with "gsfc-ngap-managed-*", and may further differentiate between "hidden" resources, that app owners cannot even see from "restricted" resources, which may be visible to but not modifiable by application owners. They should additionally be tagged with "gsfc-ngap-managed = true"; additional tags of the format "gsfc-ngap-*" may be added if additional information about the resource would be useful.

We may encounter resources that cannot be restricted in IAM by name/prefix, and have account-specific identifiers (such as Virtual Private Cloud (VPC) or Subnet IDs). Policies that reference these resources will be created and managed by Terraform, and we will work with the CloudTamer development team to ensure these policies can be attached to the appropriate Cloud Access Roles as needed.

2.1.8 User-Managed Roles/Policies

In many cases, application developers need to be able to define their own IAM roles; for example, an execution role for a Lambda function. There is no mechanism built into AWS for permitting the ability to create IAM roles, while restricting the actions that can be permitted to a subset of the user's own permissions. To create a new role or policy, application owners/developers will need to submit the proposed role to the NGAP team so that it can be reviewed and provisioned by an NGAP Operator or Admin. The process for submitting a new IAM role/policy request, or an update to an existing IAM role or policy, is detailed here under App-Owner Defined Roles/Policies.

We may be able to automate approval of a subset of the permissions to be granted to application components, in order to streamline the request process; for example, application owners may be able to grant themselves s3:GetObject permissions on any bucket in their account that they have not otherwise been denied access to. The NGAP team will develop a process/tool for such requests under NGAP-2551.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2.1.9 AWS Access Keys

AWS Access Keys are commonly used for programmatic access to AWS APIs as a particular user or role. Access keys for application owners in NGAP 2.0 will be created and managed by NGAP Operators through CloudTamer, which ensures that access keys are tied to specific Cloud Access Roles, sharing the same policies and restrictions. NGAP users will be given access keys only to Cloud Access Roles for which they already have login ability.

2.1.9.1 User-Provisioned Access Keys

Allowing application owners to provision their own access keys–again, only for the roles that they have been given access to by NGAP–would help reduce the delays and operational burden incurred by having these requests go through NGAP. AWS Access Keys are commonly used for programmatic access to AWS APIs as a particular user or role. Application owners in NGAP 2.0 can provision access keys for any Cloud Access Role that they can use for normal login, and these access keys will share the same policies and restrictions as the user's normal login role.

2.1.9.2 Deployment Keys

In some cases, additional access keys will be provisioned for programmatic access by other NGAP/Earthdata tools, such as deployment automation using Bamboo.

These Access Keys will be provided to individual application owners through a secure, encrypted mechanism such as NASA Public Key Infrastructure (PKI), and will be similarly tied to specific Cloud Access Roles. The Cloud Access Role used for a deployment access key may be an existing application owner/developer role; or a new role created specifically for the deployment.

2.1.9.3 Roles vs. Users

CloudTamer implements federated login to AWS accounts, where users who log in are assigned the appropriate role, without an associated IAM user. Since access keys are tied to users, rather than roles, NGAP users will not be able to provision their own access keys through the AWS console.

Access keys provisioned through CloudTamer are tied to a non-login IAM user that CloudTamer generates, tied to the specific Cloud Access Role. The access key is the only way to access AWS as this user, as it has console login disabled.

2.1.10 Account Types and Hierarchy

Accounts are classified by type/purpose; the currently identified account types are documented below. Accounts will be organized under Projects and OUs in CloudTamer based on budget requirements; accounts of multiple types (e.g. Sandbox and Application/Production) may exist under the same OU, and accounts of the same type (different Sandbox accounts, for example) may be present at different levels of the organization hierarchy. When organized by end-user permissions, there are three classes of accounts in NGAP 2.0: Sandbox, Application, and Management.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2.1.10.1 Organization Structure

All accounts, regardless of type, are organized with a single organizational structure. This structure is used to track account costs and, in some cases, enforce project-specific security policies. Each account must have a dedicated budget within its organizational unit.

2.1.11 Infrastructure Automation

All NGAP-managed resources (VPCs, ingress/egress routes, scanning tools, etc.) will be controlled and provisioned through Terraform configuration in the ngap-infrastructure repository, following the Continuous Integration/Continuous Delivery (CI/CD) process outlined in the wiki Terraform CI/CD & Security Plan.

2.1.11.1 Infrastructure Automation Account

There will be a single AWS account provisioned to house infrastructure automation components, along with logging, monitoring and access control to ensure that the infrastructure automation tool and associated IAM entities are not misused. The AWS components involved in our Infrastructure Automation system are the following:

- An "InfrastructureAutomation" IAM user with ONLY programmatic access (no console login), to be used by Bamboo. This user will be able to AssumeRole into a parallel "InfrastructureAutomation" IAM role in each managed account, which has the permissions required to deploy the infrastructure definition.
- A secure configuration store (to be identified; NGAP-2507), used to store sensitive values (passwords, keys) that are not checked into the infrastructure management repository. Only the "InfrastructureAutomation" user will have access to these values.
- An S3 bucket and DynamoDB table used by Terraform to keep track of configuration state. Only the "InfrastructureAutomation" user will have access to these resources. The contents of the S3 bucket will be encrypted using an NGAP-provisioned Key Management Service (KMS) key, as Terraform's state files may contain sensitive values.

In addition, the following automated monitoring will be configured:

- CloudTrail logs, so that all AWS API events, including programmatic access, are recorded.
- Restrictions, possibly by source IP, on who/what is able to login as and use the InfrastructureAutomation user/role (only Bamboo should be able to do this).
- Automated notifications/alerting through CloudTrail and/or CloudWatch Events of infrastructure rollouts, including what user or service initiated the deployment.
- Lambda-based alerting for any unexpected API activity. Aside from setting up the Infrastructure Automation account itself, no one should be logging into this account to make any changes, apart from Bamboo via the defined mechanisms.
- Automated expiration/rotation of access keys.
- Any additional monitoring/security tools that are required to be put in place to meet policy.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2.2 VPC/Network Layout

2.2.1 Application Accounts

Application accounts will be provisioned with a single "private" Virtual Private Cloud (VPC) for application owner use, as well as one or more "Management VPCs" where NGAP-controlled resources will run. These may include application/container scanning tools that are automatically provisioned to scan resources as application owners create them, though the specific scanning tools that will be put in place are still being identified.

Resources in the application owner's VPC WILL NOT be publicly accessible. This will be controlled by NGAP through VPC route tables and Network Access Control Lists (ACLs), which application owners will not be able to modify. For more details, see Public-Facing Endpoints.

2.2.2 Classless Inter-domain Routing (CIDR) Ranges

The application owner's VPC will be provisioned a unique 10.x.x.x/20 CIDR range, to give us flexibility in routing between VPCs and the ability to identify a resource based on its Internet Protocol (IP) address, until and unless we are able to evidence that globally unique (within NGAP 2.0) IPv4 addresses are no longer required.

2.2.3 Public-Facing Endpoints

NGAP shares responsibility for ensuring the security and stability of the services we host with application owners, by providing and enforcing a set of controls that application owners must adhere to. Many of these are automated controls, that NGAP is able to maintain independent of application owners; however, some controls (for example, updating running instances to the latest approved Amazon Machine Images (AMI)–see Automated Distribution Of Approved AMIs) will often require the participation of application owners. While monitoring will be put in place to ensure these controls are being adhered to (as in Automated Distribution Of Approved AMIs, by checking for the use of old/unapproved AMIs), NGAP must ensure that application owners are aware of, and have prepared appropriate tools/processes/automation for, carrying out their responsibilities regarding these controls.

In order to accomplish this, NGAP restricts the ability of application owners to create public-facing resources in their AWS account, or to modify an existing resource to make it public-facing. Application owners have a significant amount of freedom to stand up services, instances and other resources within the "Private" section of their account, which is only accessible from within that account and certain NGAP-controlled "Internal" networks; but will not be able to provision resources within the "Public" section of their account without submitting a request through the NGAP Service Desk.

2.2.3.1 Private VPCs

Each project or team within NGAP 2.0 will be provided their own AWS Account to use as a billing and access boundary. Within that account, the NGAP team will provision one or more "Private" VPCs for the application owner's use. These VPCs will have Route Tables and Network ACLs configured by NGAP to allow only internal traffic (traffic from within the same VPC); application owners will not be able to host public-facing services in these VPCs. Application owners will be able to configure their own Security Groups and related

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

ingress/egress rules, but these will be overridden by any conflicting Network ACL rules, which application owners will not be able to modify.

For traffic to be able to make it to an instance or other resource, both the Network ACL associated with the resource's Subnet and the/a Security Group associated with the resource itself must allow this traffic. If a Security Group allows ingress on port 80 from 0.0.0.0/0 but the Network ACL does not, that traffic will still be denied.

A separate Internet Services account, containing only NGAP-managed resources, will provide public-facing endpoints for resources in an application owner's private VPC. Application owners WILL NOT be able to provision resources within the Internet Services account themselves.

2.2.3.2 Internet Services Account

Resources provisioned with an application owner's VPC will be exposed through the Internet Services account, where NGAP will manage public-facing load balancers, Transport Layer Security (TLS) termination, and additional security & monitoring tools. PrivateLink will be used to connect the public-facing endpoints and Web Application Firewall (WAF) stack to services running in application owners' accounts. The PrivateLink VPC Endpoint Service (the "producer" end of a PrivateLink connection) will be provisioned and controlled by NGAP; and may connect to the application owner's Network Load Balancer directly, or to an NGAP-controlled one (in the Management VPC) if the application in question does not have a Network Load Balancer.

2.2.3.3 TLS Certificates

TLS certificates will be provisioned for an app by NGAP, using Let's Encrypt, to enable automated certificate creation. App owners will have to provide their desired domain name when they request the public-facing endpoint; see Requesting and provisioning a public endpoint in NGAP 2.0.

At the application owner's request, the application owner may provide their own TLS certificate (or a NASA Operational Security Authority (NOCA) cert) instead of using an NGAP-provisioned certificate from Let's Encrypt, though NGAP will need to validate the provided certificate to ensure it complies with NASA TLS requirements and is compatible with NGAP's front-end load balancing stack. Some application owners may prefer to do this in order to have an Extended Validation (EV) or Organization Validated certificate, rather than the Domain Validated certificate provided by Let's Encrypt.

2.2.3.4 Non-VPC Endpoints

Currently, the only non-VPC service approved for use as a public endpoint is S3. Application owners will have the ability to create their own S3 buckets, but will not be able to make them public.

2.2.3.5 Public-Facing Endpoint Request

To request a new public-facing endpoint (or a configuration change to make an existing resource public-facing), an application owner will fill out the "Request Public-Facing Service" request in the NGAP Service Desk (see workflow documentation at Requesting and provisioning a public

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

endpoint in NGAP 2.0). This request will be routed to the NGAP Operations team, who will verify that the service to be made public adheres to the following controls:

- The application to be made public has been registered in NASA's System for Tracking and Registering Applications and Websites (STRAW), with the domain name/URL that will be assigned to the public-facing endpoint, and has the correct Contact Information for the application owner.
- Automated vulnerability scanning has been hooked up, and vulnerabilities are being tracked both by NGAP Operations and by the application owner.
- The application owner has an established process for mitigating any vulnerabilities that are discovered, either before or after the application is made public.
- Only approved and up-to-date AMIs are in use, and the application owner has demonstrated their ability to update all running instances within the time frame defined in Automated Distribution Of Approved AMIs.
- If the application owner wants to provide their own SSL certificates (instead of having NGAP provision certificates for them), the certificates have been provided to NGAP and verified to be compliant with NASA/ESDIS policy.

Exceptions to the above requirements:

- Services like Amazon S3 may be used without a custom domain name & certificate, if the service is not being used as an application's primary user-facing endpoint (for example, a website could provide S3 URLs to download granules or other data, as long as the website itself has its own domain & certs).
- Application owners are not responsible for patching/update of instances underlying AWS-managed services like Lambda, SQS (Simple Queue Service), ElasticSearch etc. where the underlying infrastructure is not exposed to AWS consumers.

The types of vulnerability scans to be applied to a service will depend on the architecture of the service in question.

Once the NGAP team has made the determination that an application can be made public, we will take the following steps:

- If necessary, create a back-end Network Load Balancer in a Management VPC in the application account.
- Create a VPC Endpoint Service connected to the Network Load Balancer that was provisioned by NGAP or the application owner, and configure it to allow use only by the Internet Services account.
- Provision a VPC Endpoint and public-facing Elastic Load Balancer (ELB) in the Internet Services account, and configure any required routing for the app's requests to go to the correct VPC Endpoint.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

2.2.3.6 Non-VPC Resources

Several AWS services, including API Gateway and S3, involve resources that are not provisioned within a VPC, and thus cannot be restricted based on the routing and Network ACL rules defined above. The mechanism that will be used to restrict an application owner's ability to provision these resources depend on the specific service, but each will be one of three types:

- Restrict application owners' ability to modify the security/visibility configuration of a resource. For example, S3 buckets will be created with their default (private) access control, which can then be modified only by the NGAP team.
- Detect that an unapproved public-facing resource has been created or made public, and automatically reverse that action (destroying or resetting the configuration of the resource in question), as well as notify NGAP Operations and application owners that unapproved resources are being created. Repeated breaches of this policy may result in administrative action, and termination (or hibernation/archiving) of the application owner's account and any of the resources in it.
- Deny application owners the ability to provision the resource at all; they will need to submit a request through the NGAP Service Desk in order to have it provisioned for them by the NGAP team, or to have a deployment user created and hooked up via Bamboo.

If a new service is introduced or requested by an application owner, the NGAP team will develop, test and roll out at least one of the above control mechanisms for the service before adding it to the set of services that application owners can make use of.

2.2.3.7 Elastic Load Balancing

Each application will be provisioned a "Classic" Elastic Load Balancer. This ELB will handle TLS termination and packet filtering through AWS Security Groups. The ELBs will load balance between the remaining security and monitoring tools in the Internet Services account, to ensure availability. It WILL NOT load balance between back-end application components; this will be handled by the Network Load Balancer provisioned within the individual Application account (see Public-Facing Endpoints). Application owners are responsible for ensuring the availability and resiliency of their own apps (e.g. by provisioning resources in multiple Availability Zones). NGAP will provide VPCs and Subnets that allow this, but will not ensure the uptime, availability, or redundancy of non-NGAP-managed components.

Once incoming traffic leaves the front-end ELBs, it will no longer be encrypted, allowing the WAF, Intrusion Detection and Protection System (IDPS) and any other security tools in the Internet Services account to monitor and inspect the unencrypted packet data.

Application Load Balancers (ALBs) support hostname- and path-based routing, allowing a single load balancer to be used for multiple applications, each with their own TLS certificate.

2.2.3.8 Intrusion Detection and Packet Capture

Suricata (https://suricata-ids.org/) will be used for Intrusion Detection and Packet Capture of incoming traffic. Suricata is a free and open source, mature, fast and robust network threat detection engine that performs real time intrusion detection and prevention, network security monitoring and offline packet capture (pcap) processing. Logged alerts from the IDPS system

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

will be sent to CloudWatch Logs, and through there to the Logging account, through our normal Log Forwarding stack. PCAP data will be uploaded to an S3 bucket in the Logging account; see Packet Capture for details.

2.2.3.9 Routing

NGAP will maintain a custom routing component, which will perform hostname-based routing to the relevant application's VPC Endpoint (and could potentially also include path-based routing). The routing component can also be configured to respond with a landing page or redirect, in the case that a specific application or set of applications needs to be taken down for maintenance or other reasons.

For the initial rollout, the routing component will be an adaptation of the existing NGAP 1.0/1.1 routers, which are based on a cluster of nginx instances running in a reverse proxy configuration. Commercial and other products are being evaluated to potentially replace this and other portions of the Internet Services TIC-in-the-Cloud in the future.

2.2.3.10 Future Enhancements

All of the specific security and monitoring tools listed here are proposed for the initial architecture buildout only; any or all may be swapped out or added to as more robust, commercial or otherwise tools are evaluated as replacements.

2.2.3.11 Web Application Firewall (WAF)

ModSecurity will be used as a layer 7 web application firewall. ModSecurity is an open source, cross-platform web application firewall that provides a powerful rules language and API to implement advanced protections. The Open Web Application Security Project (OWASP) provides a "Core Rule Set" (https://www.modsecurity.org/crs/) which covers a wide range of attacks, including the OWASP Top Ten, while minimizing false alerts.

As above, any alerts will be sent through CloudWatch Logs to the Logging account.

2.2.4 Outgoing Internet Access

The approach to providing, monitoring and securing outgoing internet access detailed here is planned to eventually be replaced with a Transit VPC and routing solution to be identified. When this solution is implemented, several of the tools that will initially be implemented within individual application accounts will move to or be replaced by components within the Internet Services account (or another account/VPC).

Because we are reliant on AWS' built-in, VPC-internal Domain Name Server (DNS) for VPC Endpoints and Private Zones, we do not currently have a way to remove/replace the NGAP-managed DNS server within each account with a shared, centrally-managed DNS system.

The initial Outgoing Internet Access approach does not provide for EBNet or other direct on-prem connectivity, though specific data (such as logging/monitoring information) can be sent to on-prem systems by first going to/through the Logging account. Applications running under this initial Outgoing Internet Access solution will not have direct access to on-prem systems; and on-prem systems will not be able to access private resources running within individual application

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

accounts/VPCs, unless/until those resources are exposed through the Internet Services account (see Public-Facing Endpoints).

2.3 Monitoring and Security Controls

2.3.1 Log Aggregation/Forwarding

Individual accounts will write all required logs to CloudWatch Logs or to S3; these logs will then be forwarded to a Kinesis Stream and S3 Bucket(s) in the NGAP-managed Logging account.

From the Logging account, logs may then be ingested into a cloud-based log aggregator (Splunk, ElasticSearch/Kibana, or other tool), forwarded to EISOC's or Earthdata's on-prem Splunk instance, or sent to another endpoint not yet identified.

Only the logs for NGAP-managed components will be forwarded "by default". Application owners may request that their application logs be forwarded, but we will need to ensure that there is sufficient budget/licensing for the log aggregation tools (e.g. on-prem Splunk) that will receive the logs.

Where logs will be forwarded to from the Logging account, and whether different subsets of logs (e.g. tenant application logs vs. NGAP monitoring/access logs) will need to be forwarded to different locations is still in flux. Changes to the "final resting place" of the logs should not dramatically impact the log forwarding architecture, since Kinesis supports multiple consumers, each of which can send all or a subset of the logs to the required endpoint.

Initially, NGAP system/platform logs will be sent to the Earthdata Splunk, as they are currently in NGAP 1.x.

2.3.1.1 CloudWatch Logs

Most AWS services are designed to integrate with CloudWatch Logs for monitoring (the notable exception being certain access logs; see the "Access Logs" section, below). Managed Accounts in NGAP 2.0 will be configured to forward all CloudWatch platform and system logs to the Management Account, which will then forward these logs to the Earthdata Splunk instance.

2.3.1.2 Access Logs

Access/error logs for public-facing endpoints are of critical importance, in order to detect unauthorized access or attempted attacks against hosted services. Application owners in NGAP 2.0 will not be able to provision public-facing endpoints themselves (see Public-Facing Endpoints); only NGAP admins/operators will be able to do this.

NGAP will be responsible for ensuring that all of the public-facing endpoints that we provision have access logs enabled and properly forwarded, as a prerequisite to making those endpoints public. If the AWS service in question uses CloudWatch Logs for its access logs, the forwarding architecture outlined above will be used; however, some services use other mechanisms for their access logs. Each of these is detailed here, along with the mechanism that NGAP will put in place to ensure its logs are picked up and forwarded to the Logging account.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Additional services may be evaluated and rolled out to NGAP 2.0 as available for use for public-facing endpoints in the future. Part of the evaluation of these services will include determining whether they support the required access logging, and implementing whatever forwarding mechanisms are needed. A service that does not directly implement the required access logs may need to be kept internal-only, with a public-facing router/reverse proxy stack providing the required logs.

Most of the services that do not use CloudWatch Logs make use of S3 buckets instead. Each Managed Account will have corresponding S3 buckets (one for each region in use, since some AWS services require the logging bucket be in the same region as the resource writing to it) provisioned in the Management Account, with cross-account permissions set up to allow the Managed Account to write log files to them. Versioning will be enabled to ensure log data cannot be completely overwritten, and deletion will be prohibited. A Lambda function will subscribe to logging events on this S3 bucket, and forward the logs to the Kinesis Stream associated with that Managed Account.

2.3.2 Packet Capture

PCAP data will be produced by components documented under Public-Facing Endpoints and Outgoing Internet Access. PCAP data will be sent to an S3 bucket in the Logging account via an S3 Gateway VPC Endpoint, to avoid incurring charges for data transfer across accounts/VPCs. The PCAP bucket will be configured through lifecycle policies and/or custom Lambda functions to expire data after at least 24 hours, and up to 7 days, depending on cost.

We will initially store 24 hours of data; the time frame will be increased as we collect volume/cost data from real application use.

A second "Incident Response" bucket will also be provisioned, but will generally be left empty to avoid incurring additional cost. NGAP will set up automation to, when needed, copy a subset of PCAP data (i.e. for a specific account or application) to the Incident Response bucket, where it will not be automatically expired/deleted, and will remain available for the Security team to access, until incident response is complete. Once the data is no longer needed and further PCAP data is not being forwarded to the Incident Response bucket, the data can be manually deleted by the Security team or by NGAP admins.

2.3.3 Monitoring

All accounts will have CloudTrail, VPC Flow Logs, and GuardDuty enabled. Application owners will not be able to alter these settings, though they will have access to the outputs of these tools for their own account. CloudTrail logs and VPC Flow Logs will be forwarded to the Logging account through the normal Log Forwarding stack, detailed above. GuardDuty will be configured to "roll up" all it's findings to the Security Tools account, which will be used as the GuardDuty "master" account.

AWS Config, CloudTrail, and CloudWatch Events will be used to implement additional Lambda-based monitoring, in some cases with automated remediation. This will provide an additional layer of security over the IAM policies we define; for example, an IAM policy will prevent application owners from provisioning resources in the Management VPC; but an

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

additional alert will be set to detect such resources, in case an edge case or error in the IAM policy allows such an action

2.3.4 Scanning and Inventory

This document defines the scanning tools to be used in the NGAP 2.0 environment. Scans will be applied to all NGAP 2.0 management and managed (app owner) accounts unless noted here.

2.3.4.1 Scanning

Scans will be applied to all NGAP 2.0 management and managed (app owner) accounts unless noted here.

By default, all scan data (findings, etc.) will be forwarded to CloudWatch in the NGAP 2.0 Logging account. Any rollups of reports to be forwarded to tools, for example, such as Department of Homeland Security (DHS) Einstein or tools in EISOC, will be handled by a separate document.

2.3.4.2 EC2 Host & Software Inventory

Table 2. EC2 Host and Software Inventory

Control Name	Capability	Details	Scanning Frequency	Alert Priority	Remediation
SSM	EC2 Instance Scanning	EC2 Systems Manager (SSM) will capture: • Name • IP address • Date of creation • Boot time • Kernel version • Installed software SSM will be configured to report into the Security Tools account, giving one place to view inventory data. SSM will also be used to run Automation policies for CIS-CAT scores and anti-virus scans	Adhoc	Configuration	Manual

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Control Name	Capability	Details	Scanning Frequency	Alert Priority	Remediation
AWS Inspector	Inspector	AWS Inspector will be used to scan all running EC2 instances and EC2 AMIs stored in all accounts and scanned against custom security rules. At this time, we will scan for Common Vulnerabilities and Exposures (CVEs) and security best practices based on the default set of Inspector rules.	Weekly	Configuration	Automatic for Management Accounts
SSM	Automatic CVE Remediation	High and Critical findings identified by Amazon Inspector for NGAP-managed components in all accounts will be automatically patched. This may be accomplished by delivering newly built NGAP AMIs or via SSM	30 days	Incident	Automatic

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Control Name	Capability	Details	Scanning Frequency	Alert Priority	Remediation
AWS Config	AWS Account Configuration	AWS Config is a configuration scanning tool that will be used to validate NGAP-chosen configurations of AWS components, such as VPC, IAM users and roles, etc. For example: • a user or NGAP administrator is able to add Internet access to a VPC • an IAM role for EC2 systems manager is not applied to an ec2 instance • AWS Config will set off an alert and trigger a Lambda function for automatic remediation	Constant	Configuration	Automatic
AWS Shield	Distributed Denial of Service (DDOS) Protection	AWS Shield protection is the default protection for all AWS accounts. We will be relying on this for our default DDOS protection.	Constant	Configuration	

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Control Name	Capability	Details	Scanning Frequency	Alert Priority	Remediation
ClamAV	File Integrity Management (FIM) • EC2 Host Virus Scanning	ClamAV will be installed and used to scan all files on EC2 instances. Virus definitions will be updated daily. Virus scanning logs will be saved to the NGAP Logging account. Virus scanning will be initiated by an Automation policy in SSM.	Daily	Configuration	
AWS Snowball	Media Protection (MP)	AWS Snowball may be used in NGAP 2.0 in app-owner (managed) accounts to transfer large amounts of data to and from S3. This is media that must be physically plugged into NASA and partner networks, and therefore fall under Media Protection controls.	N/A	Configuration	

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Control Name	Capability	Details	Scanning Frequency	Alert Priority	Remediation
Clair	Docker Imager Inventory	Clair will be configured to scan existing Docker images in ECR registries in managed (app owner) accounts. If the app owner is using something other than an ECR to store Docker images, Clair will not automatically scan it. NGAP may use the Klar tool to assist with this automation of discovering the ECR in any given account and listing all registered images to scan.	Adhoc	Configuration	Manual
SSM Run Command	Emergency Patching	We will use EC2 Systems Manager Run Command to do emergency or critical patching across all running instances.	N/A	Incident	Manual

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

3 REQUIREMENTS

3.1 Introduction

The NGAP requirements and user stories will be tracked and maintained using Atlassian's Jama Requirements Management tool. The user stories presented in this document are written to a Systems Requirements level and will be kept in sync with the user stories maintained in Jama. Of note is that the stories in this document have all been approved, but not all have been prioritized for implementation as of the date of this document.

3.2 Account and Access Management

Account and Access Management includes three account types: Management, Sandbox, and Application accounts. CloudTamer (https://stratussolutions.com/tamethecloud/) is used as an integrated solution for AWS account management, budget enforcement, and compliance automation. This section will also include the requirements related to CloudTamer.

Story ID	User Story	Status
NGAP-STORY-325	As NGAP, I want a writeup of the standard account structure	Completed
NGAP-STORY-392	Application accounts shall be supplied with an active SSM activation code	Completed
NGAP-STORY-414	As an application owner, I want to be able to request an s3 bucket to be made readable to users in any or no region.	Completed
NGAP-STORY-415	As an NGAP administrator, I want to be able to designate an existing s3 bucket as readable to users in any or no region.	Completed
NGAP-STORY-416	As NGAP, I want to manage all cloud access via a portal at a NASA-delegated domain.	Completed
NGAP-STORY-417	As NGAP SA, I want to define IAM policies for the all NAMS approved roles	Completed
NGAP-STORY-418	As an NGAP administrator, I want to prohibit application owners from making their own s3 buckets readable to users in any or no region.	Completed
NGAP-STORY-419	As an application owner, I want to be able to programatically generate Security Token Service (STS) credentials with read-only access to my s3 bucket for users in any or no region	Completed
NGAP-STORY-421	As an NGAP administrator, I want S3 bucket visibility to be managed within NGAP source control	Completed
NGAP-STORY-422	As an application owner, I want a demonstration of how to use Earthdata Login to get STS credentials to an s3 bucket for access from any or no region	Completed
NGAP-STORY-423	As an application owner, I want to be able to request an s3 bucket to be made readable to users within the same region.	Completed
NGAP-STORY-424	As an NGAP administrator, I want to be able to designate an existing s3 bucket as readable to users within the same region.	Completed
NGAP-STORY-425	As an NGAP administrator, I want to prohibit application owners from making their own s3 buckets readable to users within the same region	Completed
NGAP-STORY-426	As an application owner, I want to be able to programatically generate STS credentials with read-only access to my s3 bucket for users within the same region	Completed

Use or disclosure of data contained on this page is subject to the restriction(s) on the title page of this document.

3.3 Authentication

The Authentication into the NGAP 2.0 platform will be through NASA approved authentication mechanism – launchpad. NGAP users will login into the AWS console using CloudTamer's federated login; CloudTamer itself will delegate authentication to NASA IdMAX through Launchpad. Multi-factor authentication (MFA) using a PIV card or RSA token will be required to access the CloudTamer console and federated login.

Story ID	User Story	Status
NGAP-STORY-378	As NGAP, I want to map NAMS roles to CloudTamer Roles	Approved
NGAP-STORY-379	As NGAP, I want to oversee and assist CloudTamer tool installation & configuration (Sprint 5)	Completed
NGAP-STORY-380	As NGAP, I want to request certificates and updated DNS for CloudTamer	Completed
NGAP-STORY-381	As NGAP, I need to support CloudTamer creating a SAML passthrough for Launchpad	Completed

3.4 Logging

All accounts will have CloudTrail, VPC Flow Logs and GuardDuty enabled to monitor activity in application accounts. The requirements in this section track the actions taken by users-both application owners and NGAP admins/operators- and automate compliance and security controls in a scalable and manageable fashion.

Story ID	User Story	Status
NGAP-STORY-400	As an NGAP administrator, I want all CIS benchmarks sent to kinesis logs stream	Completed
NGAP-STORY-403	As an NGAP Security Administrator, I want all VPC flow logs sent to an S3 bucket in the Logging management account	Completed
NGAP-STORY-405	As an NGAP Account Manager, I want all VPC flow logs in the Logging Account S3 bucket to be cleaned up according to the documented lifecycle policies.	Completed
NGAP-STORY-409	As an NGAP administrator, I want all CloudTrail logs from managed NGAP 2.0 accounts to be forwarded to splunk	Completed
NGAP-STORY-410	As an NGAP administrator, I want all EC2 system logs from managed NGAP 2.0 accounts to be forwarded to splunk	Completed
NGAP-STORY-411	As an NGAP administrator, I want all GuardDuty findings from managed NGAP 2.0 accounts to be forwarded to splunk	Verified internal
NGAP-STORY-420	As an NGAP administrator, I want all access logs and CloudTrail logs for public and externally accessible s3 buckets the managed NGAP 2.0 accounts to be sent to the logging account	Completed
NGAP-STORY-429	As an NGAP administrator, I want VPC flow logs from all managed accounts to be forwarded to S3 in the logging account	Completed

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

3.5 Billing and Cost

This section describes requirements for Budget enforcements and cost monitoring and reporting mechanisms.

Story ID	User Story	Status
NGAP-STORY-386	As a Budget Analyst, I want to enable EC2 memory usage metrics in NGAP 2.0 AMI	Approved
NGAP-STORY-447	As the NGAP systems architect, I want a design for implementation of the ASF egress solution in NGAP 2.0	Completed
NGAP-STORY-448	As the NGAP systems architect, I want a design for implementation of a circuit breaker to prevent cost overruns	Completed
NGAP-STORY-449	As a NGAP administrator, I want to set multiple account thresholds by project in CloudTamer.	Completed
NGAP-STORY-450	As a Budget Analyst, I want to develop a Workflow Process for Requesting new Budgets for Onboarding New Projects	Completed
NGAP-STORY-451	As a Budget Analyst, I want to develop a Cost Model Spreadsheet Submission Process to tracking and monitoring	Completed
NGAP-STORY-452	As a Budget Analyst, I want to develop a Multi Year Cost Model Spreadsheet to Forecast Required Budgets	Completed

3.6 Scanning and Software Inventory

This section defines the scanning tools to be used in the NGAP 2.0 environment. Scans will be applied to all NGAP 2.0 management and managed (app owner) accounts unless otherwise specified.

Story ID	User Story	Status
NGAP-STORY-388	As an NGAP Administrator, I want Systems Manager in the Security Management Account to manage servers in Application Accounts (and run CIS CAT)	Completed
NGAP-STORY-389	As a Security Analyst, I want all Software inventory on EC2 instances to be sent from individual managed accounts to the Security Tools/Monitoring account (secmonprod) for centralized reporting	Completed
NGAP-STORY-439	As an NGAP administrator, I want system inventory from all instances in managed accounts to be converted to a format which EDW can accept	Completed
NGAP-STORY-456	As an NGAP administrator, I need to allow KSC security read only access to SSM.	Completed
NGAP-STORY-457	As an NGAP administrator, I want to tag every managed instance in SSM.	Completed

3.7 Outgoing Internet Access

This section details the approach to providing, monitoring and securing outgoing internet access. Requirements under this will include requirements related to logging, DNS, packet filtering, VPC endpoints, other outgoing traffic (SSH, FTP) and admin requirements to manage Managed accounts.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Story ID	User Story	Status
NGAP-STORY-396	As NGAP, I want an automated NAT Instance definition and deployment	Completed
NGAP-STORY-397	As NGAP, I want an automated deployment of S3 VPC Endpoints	Completed
NGAP-STORY-402	As NGAP, I want an automated SSH bastion solution in the 2.0 alpha account	Completed
NGAP-STORY-427	As an NGAP administrator, I want updates to the AWS IP address ranges assigned for a region to automatically be applied to s3 bucket policies.	Completed
NGAP-STORY-430	As an NGAP administrator, I want outgoing internet access from managed accounts to be filtered by port, protocol, source, and target	Completed
NGAP-STORY-431	As an application owner, I want to be able to access HTTP(S) recources on the internet from my account	Completed
NGAP-STORY-432	As an NGAP administrator, I want to be able to permit outgoing traffic on non HTTP(S) protocols on a per account basis	Verified internal
NGAP-STORY-433	As an NGAP administrator, I want to manage a DNS to be used by managed accounts	Completed
NGAP-STORY-434	As an NGAP administrator, I want to be able to provide VPC endpoints to managed accounts	Completed
NGAP-STORY-435	As an NGAP administrator, I want to log all DNS queries	Completed
NGAP-STORY-436	As an NGAP administrator, I want to capture all outgoing network packets	Completed
NGAP-STORY-437	As an NGAP administrator, I want to ensure that all lambdas in managed accounts are running in a managed VPC	Completed
NGAP-STORY-438	As an NGAP administrator, I want to provide each managed account with an account-specific NAT address/range.	Completed
NGAP-STORY-458	As an NGAP Administrator, I need an S3 bucket in the monitoring account to hold the DNS blacklist file.	Completed

3.8 CI/CD

This section describes the requirements to roll out infrastructure changes in a staged automated manner to different sets of accounts. The CI/CD process manages the life cycle of Infrastructure changes in a controlled and centralized environment. This section will also include Terraform-related requirements.

Story ID	User Story	Status
NGAP-STORY-393	As NGAP, I want an automated VPC and NACL deployment solution	Completed
NGAP-STORY-404	As an NGAP administrator, I want to add the mgmt ngap-infrastructure stage to bamboo deploy scripts	Completed
NGAP-STORY-407	As an NGAP Administrator, I want to develop NGAP versioning and release roll out plan	Completed
NGAP-STORY-441	As an NGAP administrator, I want to be able to automatically roll out patches to all EC2 instances running in managed accounts	Deferred
NGAP-STORY-442	As an NGAP administrator, I want to be able to set a schedule for automatic patch roll outs	Deferred

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Story ID	User Story	Status
NGAP-STORY-443	As an NGAP administrator, I want to be able to automatically generate and make available in all managed accounts an up to date base AMI	Completed
NGAP-STORY-444	As an NGAP administrator, I want to be able to set a schedule for automatic AMI releases	Deferred
NGAP-STORY-445	As an application owner, I want to be able to opt out of automatic patching (provided I have an OSA)	Deferred

3.9 Security Requirements

3.9.1 System Integrity

NGAP Platform has to provide integrity as per NASA and NIST (National Institute of Standards and Technology) standards. The platform has to be able to detect malicious code, un-patched systems, suspicious event and attack indicators.

Story ID	User Story	Status
NGAP-STORY-472	As NGAP Security team, I want to monitor for unauthorized usage, attacks, and indicators of compromise.	Approved
NGAP-STORY-473	As NGAP Security team, I want automated responses to suspicious events.	Approved
NGAP-STORY-474	As NGAP Security team, I want to detect and erradicate malicious code.	Approved
NGAP-STORY-475	As NGAP Security team, I want security relevant updates (patches) installed within 30 days.	Approved
NGAP-STORY-476	As NGAP Security team, I want a way to identify, report, and correct missing patches or flaws within the application.	Approved

3.9.2 System and Communications Protection

When it comes to protection of systems and communication, NGAP platform will adhere to or put in place some security standards or measures. The platform should be capable of detecting and deterring DDoS attacks, encrypt all web traffic in accordance to federal standards. The platform should be able to monitor and report on privileged user usage at the console, provide access in accordance to the principle of least privilege.

Story ID	User Story	Status
NGAP-STORY-467	As NGAP Security team, I want automated protections against denial of service attacks and include the ability to detect, deter, limit, and respond to such attacks.	Approved
NGAP-STORY-468	As NGAP Security team, I want the platform and applications to encrypt web based traffic between users and the system in accordance with federal standards.	Approved
NGAP-STORY-469	As NGAP Security team, I want the platform, system, and application to terminate network communications after a pre-defined time period to avoid network hijacking and piggybacking.	Approved
NGAP-STORY-470	As NGAP Security team, I want to monitor and control the flow of information using the principle of least privledge within the boundary of the entire system.	Approved

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Story ID	User Story	Status
NGAP-STORY-471	As NGAP Security team, I want the platform to utilize a secure, fault-tolerant, and authoritative DNS system.	Approved
NGAP-STORY-487	As NGAP Security team, I would like to log access to management console sign-in.	Approved
NGAP-STORY-488	As NGAP Security team, I would like to log access or usage of root ID on management console	Approved

3.9.3 Risk Assessment

NGAP Platform will adhere to the principle of continuous monitoring, which entails periodic risk assessments run on systems, vulnerabilities identified on system and have a minimum Internet Security Configuration Assessment Tool (CIS-CAT) score of 85.

Story ID	User Story	Status
NGAP-STORY-465	As NGAP Security team, I want periodic Information Security Risk Assessments conducted on the system.	Approved
NGAP-STORY-466	As NGAP Security team, I want an automated vulnerability identification tool employed to identify system and application vulnerabilities at all levels of the shared responsibility model.	Approved
NGAP-STORY-477	As NGAP Security team, I want to run CIS CAT on EC2 instances and collect scores at least twice a month	Approved

3.9.4 Contingency Planning

In case of natural disaster or network outage, NGAP should have a comprehensive contingency plan (CP) for each of its major components. CP has to be designed, documented and at least once a year be tested.

Story ID	User Story	Status
NGAP-STORY-464	As NGAP Security team, I want contingency operations and management baked into the platform.	Approved
NGAP-STORY-481	As NGAP Security team, I want all team members trained for contingency operations according to their role/function.	Approved
NGAP-STORY-482	As NGAP Security team, I want a (functional) contingency plan test, annually, to determine the effectiveness and operational readiness of the plan.	Approved
NGAP-STORY-483	As NGAP Security team, I want recovery and reconstitution procedures for major components of the system.	Approved
NGAP-STORY-484	As NGAP Security team, I want backups of critical system and infrasatructure conducted.	Approved

3.9.5 Supporting Documents

Other than the deliverable security documents, the NGAP platform shall have some of its supporting documents created and maintained.

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Story ID	User Story	Status
NGAP-STORY-478	As NGAP Security team, I want all the system architecture documentation in a centralized location	Approved
NGAP-STORY-479	As NGAP Security team, I want an Operations Manual for NGAP Platform	Approved
NGAP-STORY-480	As NGAP Security team, I would like to keep track of privileged users for a monthly audit.	Approved
NGAP-STORY-489	As NGAP Security team, I would like to document configuration changes to AWS resources.	Approved
NGAP-STORY-490	As NGAP Security team, I would like to review ticket requests which open one-off ports or access on a public facing AWS resource.	Approved

3.9.6 Incident Response

As part of continuous monitoring, NGAP platform shall create, write, test and adhere to an Incident response (IR) plan - which draws its basic structure from NASA IR plan.

Story ID	User Story	Status
NGAP-STORY-485	As NGAP Security team, I want all confirmed incidents reported within 60 minutes to the NASA SOC.	Approved
NGAP-STORY-486	As NGAP Security team, I want to develop and maintain an Incident Response Plan for the NGAP Platform	Approved

3.9.7 Configuration Management

NGAP platform shall keep an up to date inventory of all the running resources within its boundary. NGAP platform shall also create and document its baseline configuration and monitor for any deviations and document that as well.

Story ID	User Story	Status
NGAP-STORY-493	As a security team member, I would like to capture baseline configuration of systems	Approved
NGAP-STORY-501	As a security team, we would like a real-time updated list of all accounts within the authorization boundary, under the SSP. [CM-8a]	Completed
NGAP-STORY-502	As a security team member, I would like a central, searchable inventory that includes all utilized components of AWS: compute (ec2, lambdas), storage (s3, EFS), and databases (RDS, redshift). [CM-8a.1]	Completed
NGAP-STORY-503	As a security team member, I would like an inventory method that captures a component, even if the component is misconfigured. [CM-8a.2]	Completed
NGAP-STORY-504	As a security team member, I would like a central, searchable software and hardware inventory archived for at least 90 days. [CM-8a.3]	Completed
NGAP-STORY-505	As a security team member, I would like to easily query all compute, database, and storage components for their associated: SSP, POC, operational state, and deployment state. [CM-8a.4]	Verified internal
NGAP-STORY-506	As a security team member, I would like a comprehensive inventory to be archived and available for at least a yearly external audit review [CM-8b]	Approved

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Story ID	User Story	Status
NGAP-STORY-507	As a security team member, I would like a central, searchable log of updates or removals to infrastructure that includes the change method (console, cli, or terraform) and change agent (user, role, api key). [CM-8(1)]	Verified internal
NGAP-STORY-508	As a security team member, I would like a record of deviation between terraform state and deployed configurations. [CM-8(6)]	Approved
NGAP-STORY-509	As a security team, we would like single centralized "gold standard" storage archive.	In Progress
NGAP-STORY-515	As NGAP Security team, I require that every EC2 instance installs, runs, and registers the AWS/SSM agent	Approved
NGAP-STORY-516	As NGAP Security team, I need AWS config rules configured in every account to identify which EC2 instances are not running SSM and to report on them.	Approved

3.9.8 Identification and Authentication

NGAP platform shall incorporate MFA for all user access to console or systems running on the platform. NGAP platform shall require users who have privileged access to use PIV card for authentication.

Story ID	User Story	Status
NGAP-STORY-494	As NGAP Security team, I want PIV access to all "highly" privileged AWS accounts and functions.	Approved
NGAP-STORY-495	As NGAP Security team, I want to uniquely identify devices accessing NGAP for administrative or development purposes.	Approved
NGAP-STORY-496	As NGAP Security team, I want NAMS to be used for assigning access levels (including Elevated Privilege roles), granting authorizations, and tracking authorization to the NGAP platform.	Approved
NGAP-STORY-497	As NGAP Security Team, I want cryptographic access keys to expire after a designated time period, and a method to immediately revoke access keys.	Approved
NGAP-STORY-498	As NGAP Security Team, I want cryptographic access keys to utilize the principle of least privledge when creating access keys such that the key can only be used for the intended purpose.	Approved
NGAP-STORY-499	As NGAP Security Team, I want an automated method to detect access key exposure and immediately revoke that access key if exposed.	Approved
NGAP-STORY-500	As NGAP Security Team, I want 2-Factor authentication to all accounts and services, privileged or non-privileged.	Approved

3.9.9 Access Control

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Story ID	User Story	Status
NGAP-STORY-510	As NGAP Security team, I want AWS console access keys limited by source IP address and/or multi-factor access	Approved
NGAP-STORY-511	As NGAP security team, I require all SSH access to pass through a NASA TIC (Trusted Internet Connections)	Approved
NGAP-STORY-512	As NGAP Security, I want to know about user access from outside the United States.	Approved
NGAP-STORY-513	As NGAP Security team, I require separation between development, production, and management accounts.	Approved
NGAP-STORY-514	As NGAP Security, I require that administrative level access is separated from development access.	Approved
NGAP-STORY-517	As NGAP Security, I require all accounts to be processed through NAMS.	Approved
NGAP-STORY-518	As NGAP Security, I require information flow controls to be defined, authorized, and monitored internally and externally.	Approved
NGAP-STORY-519	AS NGAP Security, I require that personnel administering access control functions do not also administer audit functions.	Approved
NGAP-STORY-520	As NGAP Security, I require the NGAP AMI and CloudTamer to enforce: System Use Notification, Session Timeout, Unsuccessful Login attempts, and Session Lock features within the OS.	Approved
NGAP-STORY-521	As NGAP Security, I require accounts using external/commercial SaaS applications to have a risk assessment performed and written authorization for use by the NASA OCIO (Office of the Chief Information Officer).	Approved
NGAP-STORY-511	As NGAP security team, I require all SSH access to pass through a NASA TIC	Approved

3.9.10 Security Awareness and Training Policy and Procedures

Story ID	User Story	Status
NGAP-STORY-522	As NGAP Security, I require that NAMS workflows incorporate NASA training requirements as a pre-requisite for access to the system.	Approved

3.9.11 Audit and Accountability Policies and Procedures

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Story ID	User Story	Status
NGAP-STORY-523	As NGAP Security, I require events to be logged to a central respository.	Approved
NGAP-STORY-524	As NGAP Security, I require all system use and access to be logged in the central repository.	Approved
NGAP-STORY-525	As NGAP Security, I require all logs to maintain a consistent timestamp format based on a network time server.	Approved
NGAP-STORY-526	As NGAP Security, I require log streaming and processing or generation failures to create an action for remediation.	Approved
NGAP-STORY-527	As NGAP Security, I require the centralized log repository to be protected from accidental deletion, and have controlled and very limited write permissions.	Approved
NGAP-STORY-528	As NGAP Security, I require the centralized log archive to contain logs online and accessible via read-only for a minimum of 365 days.	Approved

3.9.12 Security Assessment and Authorization Policies and Procedures

Story ID	User Story	Status
NGAP-STORY-529	As NGAP Security, I require self-assessments annually or after a significant change.	Approved
NGAP-STORY-530	As NGAP Security, I require documentation on all system interconnections outside the platform.	Approved
NGAP-STORY-531	As NGAP Security, I require penetration testing to be performed on the platform components and hosted application bi-annually.	Approved
NGAP-STORY-532	As NGAP Security, I require the platform to help maintain the system security plan, support annual authorization and continuous monitoring efforts, and resolve POA&M's levied on the system.	Approved

3.10 EC2 Instance Patching

The key control that relates to software patches on EC2 instances is SI-2: System Information and Integrity - Flaw Remediation under NIST 800-53. Every software that is installed on any EC2 instance in NGAP 2.0 will have to be tagged, and ensured that systems are patched regularly to avoid running old, insecure versions of software with known vulnerabilities.

Story ID	User Story	Status
NGAP-STORY-454	As an application owner, I want all new AMIs to be tagged with a version ID so I can always find the latest AMI release	Completed
NGAP-STORY-455	As an NGAP 2.0 administrator I want AMIs to be automatically shared with managed accounts upon creation	Completed
NGAP-STORY-459	As an NGAP application owner, I need a mechanism to be alerted to new AMI updates	Completed
NGAP-STORY-463	As an NGAP administrator, I want to share the NGAP 2.0 AMI with all management accounts	Completed

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.

Appendix A Abbreviations and Acronyms

ACL	Access Control List
ALB	Application Load Balancer
AMI	Amazon Machine Images
API	Application Programming Interface
ARN	Amazon Resource Name
ASF	Alaska Satellite Facility
AUID	Agency User ID
AWS	Amazon Web Services
CI/CD	Continuous Integration/Continuous Delivery (Deployment)
CIDR	Classless Inter-domain Routing
CIS	Center for Internet Security
CIS-CAT	Center for Internet Security Configuration Assessment Tool
CLI	Command Line Interface
CP	Contingency Planning
CVE	Common Vulnerabilities and Exposures
DBA	Database Administrator
DCN	Document Change Notice
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DNS EBnet	Domain Name System EOSDIS Backbone network
EC2	Elastic Compute Cloud
ECR	Elastic Container Registry
EDW	Enterprise Data Warehouse
EED2	EOSDIS Evolution and Development 2
EFS	Elastic File System
EISOC	Code 423 EOS Information Security and Compliance Office
ELB	Elastic Load Balancer
EMCC	Enterprise Managed Cloud Computing
EOSDIS	Earth Observing System Data and Information System
ESDIS	Earth Science Data and Information System
EV	Extended Validation
FIM	File Integrity Management
FPD	Flights Project Directorate
FTP	File Transfer Protocol
GSFC	Goddard Space Flight Center
HTTPS	Hyper-Text Transfer Protocol
IaaS	Infrastructure-as-a-Service
IAM	Identity Access Management
ID	Identifier
IDPS	Intrusion Detection and Protection System
IP	Internet Protocol

Use or disclosure of data contained on this page is subject to the restriction(s) on the title page of this document.

IR	Infrared
KMS	Key Management Service
KSC	Kennedy Space Center
MFA	Multi Factor Authentication
MP	Media Protection
NACL	Networking and Cryptography Library
NAMS	NASA Access Management System
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NGAP	NASA-Compliant General Application Platform
NIST	National Institute of Standards and Technology
NOCA	National Organization for Competency Assurance
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OSA	Operational Security Agreement
OU	Organizational Unit
OWASP	Open Web Application Security Project
PCAP	Packet Capture
PIV	Personal Identity Verification
PKI POA&Ms	Public Key Infrastructure Plan of Action/Milestones
POC	Point Of Contact
RDS	Relational Database Service
RSA	Rivest, Shamir and Adelman
S3	Simple Storage Service
SAML	Security Assertion Markup Language
SDLC	Systems Design Lifecycle
SIT	System Integration Testing
SOC	Security Operations Center
SQS	Simple Queue Service
SSH SSL	Secure Shell Secure Sockets Layer
SSM	Systems Manager
SSP	Systems Security Plan
STRAW	System for Tracking and Registering Applications and Websites
STS	Security Token Service
TIC	Trusted Internet Connections
TLS UAT	Transport Layer Security User Acceptance Testing
URL	Uniform Resource Locator
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall

Check ESDIS CM library, https://ops1-cm.ems.eosdis.nasa.gov/cm2/, to verify that this is the correct version prior to use.