GeoPlatform

Contingency and Disaster Response Plan

UNITED STATES DEPARTMENT OF THE INTERIOR

Version 1.0

November 2018

Table of Contents

Document Revision History

Date	Pages and/or Section #s	Description	Author
09/2018	Added service bands	Reviewed and updated accordingly	ISSO
09/2018	Added ZIVARO specific responsibilities to the entire plan	Reviewed and updated accordingly	SO
11/2018	Entire Plan	Reviewed and updated by Image Matters and Zivaro personnel	Image Matters & Zivaro
11/2018	Entire Plan	Reviewed and finalized	SO

1. Introduction

An information security contingency is an event with the potential to disrupt system operations and therefore, disrupting critical mission and business functions. Examples of such an event are a power outage, hardware failure, equipment destruction, storm, or fire. Particularly destructive events are often referred to as disasters; which can affect normal operations for an extended period. To quickly and effectively recover the GeoPlatform's services following a disruption or an emergency, a tested and cost-effective contingency plan must be in place.

1.1. Purpose

This Contingency and Disaster Recovery Plan establishes procedures to circumvent potential contingencies and disasters or to minimize the damage they case. The GeoPlatform's Contingency Plan outlines the procedures to recover the systems operations following a disruption. These disruptions do not necessarily require relocation to an alternate site. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    - **Notification and Activation** – To detect and assess damage and to activate the Contingency Plan
    - **Recovery** – To restore temporary IT operations and recover damage done to the original system
    - **Reconstitution –** To restore IT system processing capabilities to normal operations
- Identify activities, resources, and procedures needed to carry out processing requirements during prolonged interruptions to normal operations
- Ensure coordination with other GeoPlatform staff who will participate in the contingency planning strategies

1.2. Applicability

This Contingency Plan applies to the functions, operations and resources necessary to restore and resume the DOI and other GIS Task Order tenants' operations as installed in Amazon Web Service FedRAMP approved regions in the eastern and western United States. The Contingency Plan also supports the GeoPlatform's Disaster Recovery Plan (DRP).

Throughout this document:

- GIS Cloud Hosting Services - Brokered Services refers to AWS via Zivaro (formerly GTRI)
- Software Development Team refers to Image Matters LLC

1.2.1. Disaster Recovery

The Disaster Recovery Plan is designed to restore operations of the system at an alternate site following a major event or emergency.

a. Definition of a Disaster

A disaster is any event resulting in damage, loss, or destruction of property, processing resources, or processing services that significantly limits the ability of an application system or IT assets to carry on their usual business. In this document, disaster classifications are described in terms of the effect that an event would have on this system's operations.

b. Implementing a Disaster Recovery Capability

Successful implementation of a Disaster Recovery Capability requires a phased approach. There are three phases:

- Phase 1: Notification and Activation
- Phase 2: Recovery
- Phase 3: Reconstitution

Table I: Disaster Recovery Classifications

Disaster Classification	Scope of Impact
Catastrophic	Events would be a disaster that would disrupt all electrical grid operations in Virginia. Loss of electrical services in the AWS US East region
Critical	Some data centers experience service outages
Limited	Data or application breach resulting in loss of data

Catastrophic disasters necessitate the recovery of a defined minimal set of services at an alternate location followed by an eventual restoration of all services. Critical Disasters necessitate the recovery of a potentially smaller set of services at the primary site, followed by an eventual restoration of all services at that site. Limited disasters necessitate the restoration of all services at the primary site.

1.2.2. Preliminary Planning

This section covers the preliminary planning activities required to successfully respond to and recover from disasters

a. Impact Analysis / Recovery Priorities

The purpose of an Impact Analysis is to correlate specific system resources with the critical services that they provide, and based on that information, characterize the consequences of a disruption to each resource.

Table II: Outage Impact

Resources	Outage Impact	Allowable Outage Time
EC2 Instances	Web Application	48 hours
Relational Database	MySQL backend	48 hours
S3 Buckets	Automated code deployment, file hosting, backups	(Global Replication)

Recover priorities for system resources may be derived based on the data in Table II above. High priorities are based on the need to restore critical resources within their allowable outage times; moderate and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period.

Table III: Recovery Priorities

Resources	Recovery Priority (High, Medium, Low)
EC2 Instances	High
Relational Database	High
S3 Buckets	Medium

b. Response Time per Priority Level – Real Time Objectives (RTO)

Table IV: Recovery Time by Priority (By Service Band)

	Response Time by Priority Rating							
Service Band	**Urgent Min**	**Urgent Max**	**High Min**	**High Max**	**Normal Min**	**Normal Max**	**Low Min**	**Low Max**
Band 3	2 hr	8 hr	4 hr	16 hr	6 hr	24 hr	8 hr	36 hr
Band 4	8 hr	24 hr	16 hr	48 hr	24 hr	72 hr	36 hr	96 hr

c. Recovery Point Objectives (RPO)

Table V: Recovery Point Objectives by Service Band

Service Band	From	To
Band 3	4 hours	24 hours
Band 4	24 hours	48 hours

d. Maximum Tolerable Downtime (MTD)

Table VI: Maximum Tolerable Downtime by Service Bands

Service Band	From	To
Band 3	6 hours	60 hours
Band 4	32 hours	144 hours

1.3. Scope

This Contingency Plan was developed based upon consideration of various scenarios multiple assumptions.

The two key principles for the plan are:

- Contingency plan activation when the primary facility or the application itself is inaccessible (under the conditions further described in this document) and is therefore unable to perform processing
- By leveraging AWS, the GeoPlatform can provide seamless server, network, and database capabilities in the event of one or multiple datacenter failures due to multiple Availability Zones within a single AWS Region.
    - The facilities at the alternate sites (in AWS context this is covered via different availability zones) and its IT resources will be used to recover functionality during an emergency situation that prevents access to the original facility
    - The designated computer system at the alternate sites has been configured to begin processing information
    - The alternate sites (in AWS context this is covered via different availability zones) will be used to continue recovery and processing throughout the period of disruption until operations return to normal

  - AWS US East/West and GovCloud (US-West) Regions, including all the facilities at the alternate sites, are compliant with FedRAMP requirements at the Moderate impact level. AWS datacenter facilities that are not FedRAMP compliant, such as the Ohio region, will not be utilized.

The following assumptions were made by:

- **GIS Cloud Hosting Services - Brokered Services**
  - The system is inoperable at its primary site and cannot be recovered within at least 24 hours (and hardware and software are unavailable or will not be available for the same minimum duration)
  - Identified key personnel have been trained in their emergency response and recovery roles and are available to activate the Contingency Plan
  - Preventive controls (e.g. generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster
  - Availability zones are all redundantly connected to multiple Tier-1 transit providers. Computer center equipment to include all components that support the system are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure
  - Current backups of the application software and data are intact and available at the offsite storage facility
  - The equipment, connections, and capabilities required to operate are available at the alternate site (in AWS context this is covered via different availability zones)
  - Service agreements are maintained with hardware, software, and communications providers to support the emergency system recovery

- **GeoPlatform Software Development (FGDC GeoPlatform.gov)**
  - Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is “cold”. In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites
  - AWS has designed it’s systems to tolerate system or hardware failures with minimal customer impact. Data center Business Continuity management at AWS is under the direction of the Amazon Infrastructure Group
  - AWS provides the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designated as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to discrete uninterruptible power supply (UPS) and onsite backup generator facilities, they are each fed via different grids from independent utilities to further reduce single points of failure

The Contingency Plan DOES NOT apply to the following situations:

- The overall recovery and continuity of business operations beyond a disaster recovery situation. This plan does not include a Business Resumption Plan (BRP) and a Continuity of Operations Plan (COOP). However, it is worth noting that in order to exceed the scope of the Disaster Recovery scenario for this plan, multiple and simultaneous catastrophes on all availability zones contained in AWS US East/West and GovCloud (US-West) Regions.

1.4. System Description

The GeoPlatform system provides a centralized solution for development, software, hardware, security and facilities in support of federal partners mission and business operations.

The GeoPlatform offers access to a suite of geospatial assets including data, services, applications, and infrastructure. The GeoPlatform supports an operational environment, www.GeoPlatform.gov, where customers can discover, access, and use shared data, services, applications, and when appropriate, infrastructure assets.

The GeoPlatform is underpinned by:

- A segment architecture, aligned with the Federal Enterprise Architecture (FEA) that emphasizes reuse of open and interoperable standards and technology, and supports increased access to geospatial assets. The GeoPlatform uses a service-oriented architecture based upon common, secure, and scalable open-standards based technologies based in cloud computing
- Collaborative investment and portfolio management processes that enable partners and customers to leverage resources and share the costs of shared geospatial services
- Policies and governance structures to ensure sound management practices and effective partnerships that address the requirements of Federal, State, regional, local, and Tribal organizations, Administration policy, and agency missions
- A Managing Partner that serves as a government focal point responsible and accountable for coordination and provision of data and services provided by the GeoPlatform

GeoPlatform assets are managed as a portfolio, driving toward a scenario where the following characteristics are present:

- High quality and timely geospatial data, services, and applications are easy to discover and obtain
- Customer needs are identified, planned, budgeted, and met in a geospatial context
- Long-term costs of geospatial asset development, delivery, and access are reduced, duplicative efforts are minimized, and new business markets are developed
- Partners leverage non-geospatial assets with the goal of integrated information sharing
- Collaborative management of geospatial assets occurs across all levels of government
- Adaptable, proactive, and inclusive interactions are promoted among all stakeholders

GeoPlatform performs managed services coin GIS Cloud Hosting Services through its integration with Amazon Web Services (AWS), East / West FedRAMP Authorization, service model - Infrastructure as a Service (IaaS). This initiative is in correlation with the federal government's Cloud First Policy, and Data Center Optimization Initiative (DCOI – OMB - M-16-19), E-Government Act of 2002, and Executive Order 12906.

These services offerings culminate standard services (e.g., Instance Management, Database Management, Backup Management, Continuous Monitoring & Support, etc.) and Security Services (e.g., User and Permission Management, Firewalls, Operating System Hardening at Deployment, STIG compliance, Operating System Patching, Log Retention & Archiving, etc.) through the AWS FedRAMP agreement and authorization for operation in accordance with FedRAMP requirements.

Contract Operational Companies Supporting GeoPlatform services and solutions

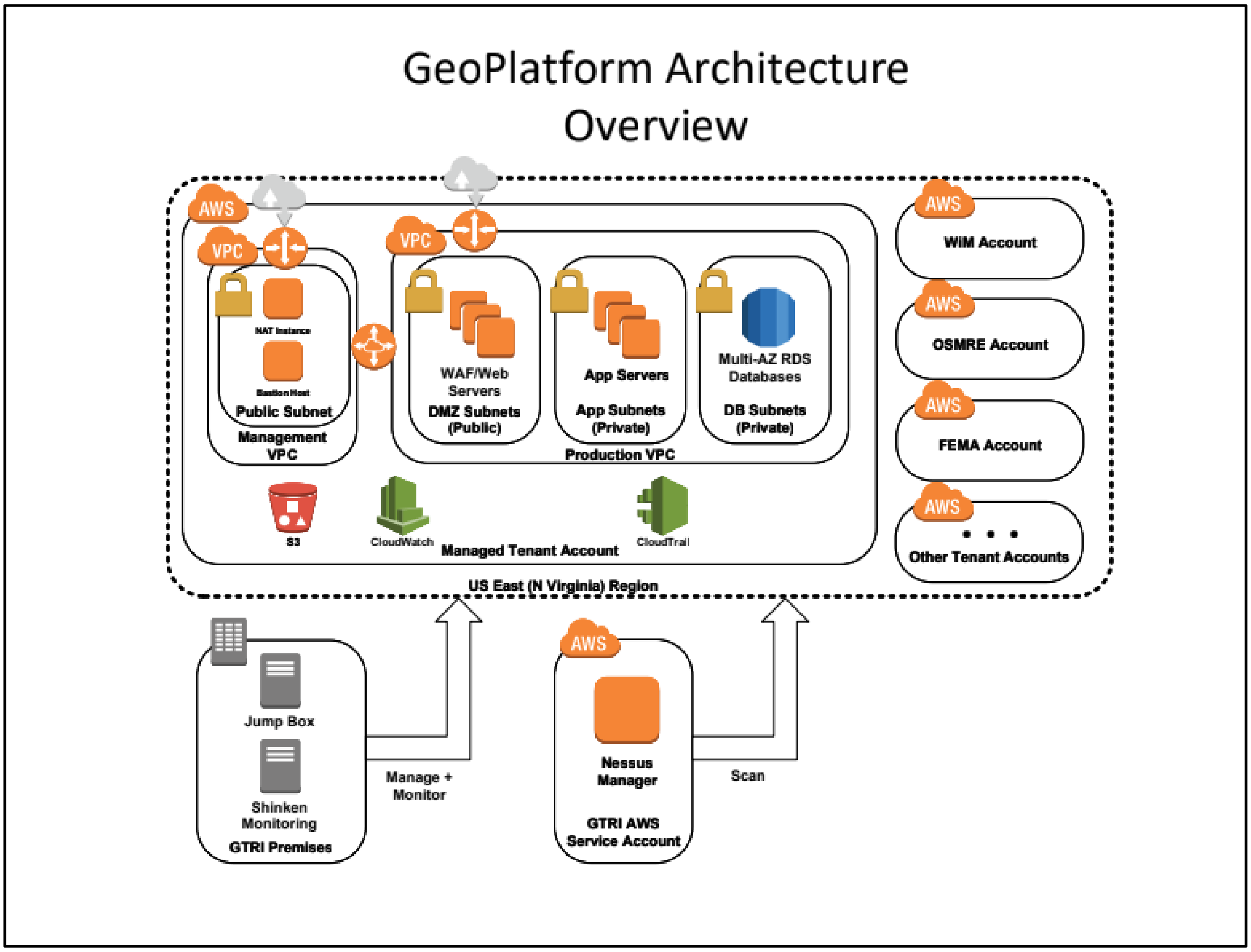
Image Matters LLC

GeoPlatform Software Development Operations are handled by a company called Image Matters. Image Matters conducts operations in a DevOps capacity, developing software that comprises the GeoPlatform.gov hosted by AWS FedRAMP operations. Their solutions are vetted through 3 instances providing the capacity to develop, test and install their solution into production. GeoPlatform code is stored in GitHub and the utilization of Semantic Versioning is implemented.

Zivaro, Inc

GIS Cloud Hosting Services – Brokered Services is handled by a company called Zivaro. Zivaro provides brokered services in accordance with NIST 500-292. Zivaro utilizes onboarding checklists to assist intra-agency operations with their PaaS, CaaS and SaaS needs. Through the onboarding procedures, Zivaro creates service level agreements (SLA) with the customers. Zivaro’s adherence to NIST 800-53 and the incorporation of AWS FedRAMP integration allows intra-agency operations to inherit security controls from the GeoPlatform investment.

1.4.1. System Architecture



1.5. Roles and Responsibilities

The following GeoPlatform teams have been trained to respond to a contingency event affecting this system:

- **Executive Management Team**
  - Provides overall guidance following an event/disaster and is responsible for activating the contingency plan and oversees the execution of contingency operations
  - Facilitates communication amongst the rest of the team and supervises contingency plan tests and exercises
  - The Authorizing Official or designated individual activates the plan and makes decisions regarding spending levels, acceptable risk, interagency coordination

- **GIS Cloud Hosting Services - Brokered Services**
  - GeoPlatform architecture leverages AWS backend services, which provides a high level of availability and redundancy. In addition, the Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24/7, 365 coverage to detect incidents and to manage the impact and resolution.

- Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A service health dashboard is available and maintained by the customer support team to alert customers to any issues that may be of broad impact. Additionally, direct communication with the AWS customer support team is available. The Zivaro Communication Plan will be enacted to notify customers of applicable events.

GIS Cloud Hosting Services - Brokered Services is responsible for AWS account management as well as the Information Assurance patching and vulnerability remediation for the Operating Systems. Account management includes responsibility for implementing, maintaining, and restoring all AWS infrastructure components including EC2 instances and RDS databases. The Software Development Team is responsible for performing the additional steps needed to restore the functionality of the n-tier, web-application architecture. Patching responsibilities include remediating all critical and high vulnerabilities in the operating system only. Patching application vulnerabilities is not the contractual responsibility of the Brokered Services, however such vulnerabilities are reported. A monthly vulnerability report is sent to the client's primary contact.

- **Software Development Team (Image Matters LLC)**
    - Responsible for development, and operation maintenance life cycle of the GeoPlatform.gov SaaS/PaaS suite of applications, services, data and content.
    - They deal with initial releases of the components that comprise the suite, in addition to the operation lifecycle. This includes release cycles, hotfix releases, service requests, automated backups, load balancing, and other maintenance operations.

Each team coordinates service requests for cloud resources to fit the development lifecycle.

AWS East, West, and GovCloud West are FedRAMP compliant and provide accessibility for data based on their handling of information, region automation, and associated policy to protect media handled by their operation. Please refer to the Service Level Agreements for more information.

1.5.1. Contact List

All contingency planning personnel are distributed the GeoPlatform Contingency Plan on an annual basis and whenever there is an update to the document. CP personnel are trained annually for their specific GeoPlatform CP roles and responsibilities through CP test preparation, test scenario selection, functional test and the CP Test Report which details the results of the testing and lessons learned to prevent any reoccurring issues in the future, if possible. Contingency Plan testing is coordinated by the Authorizing Official and other staff as necessary.

Table VII: Primary Disaster Recovery Roles and Responsibilities

Disaster Recovery Task	Accountable Personnel	Phone Number
AWS POC Operations Primary	Network Operations Center (Zivaro)	1-855-290-5488
AWS POC Operations Secondary	Chris Martin (Zivaro)	720-836-7412
Cloud Security Architect	Chris Martin (Zivaro)	720-836-7412
Data Backup	Lee Heazel (Image Matters)	812-339-9396
Data Recovery	Lee Heazel(Image Matters)	812-339-9396
C/DRP Testing	Lee Heazel (Image Matters)	812-339-9396
Disaster Reporting to CSIRC	Forest Gafford (Image Matters)	812-339-9396

Contacting Media	Thomas Dabolt	202-208-4109
Authorizing Official	Thomas Dabolt	202-208-4109
DNS Requests	David Boldt (Primary) Robbie Moreland (Alternate)	703-648-5679 573-308-3512
System Owner	Kayloni Ah Tong	202-513-0787
Information System Security Officer (ISSO)	Jacob Guzman	970-219-5394

1.6. References

- Federal Information Security Modernization Act (FISMA) of 2014
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix I-11
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- National Response Framework of 2013

2. Phase 1: Notification and Activation

The notification and activation phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to the system. Based on the assessment of the event, the plan may be activated by the Authorizing Official

In an emergency, the GeoPlatform's top priority is to preserve the health and safety of its staff before proceeding with the Notification and Activation procedures.

Contact information for key personnel is located in Table VII above. The notification sequence is listed below:

- Notify shareholders that an incident has occurred
- Contact Zivaro / AWS to gather impact analysis
- Provide shareholders with assessment details

2.1. Notification Procedures

The following procedures list notification actions to be taken upon a disaster or incident:

- Notify all teams of the nature of the impending or occurring emergency
- Notify all teams with details that pertaining to an impacted datacenter(s)
- Contact GIS Cloud Hosting Service - Brokered Services for impact analysis via the GIS Helpdesk ticketing system
  - Contact AWS directly if unavailable
- Contact government stakeholders and determine the course of action for contingency plan activation
- If Contingency Plan is to be activated, draft media release for stakeholders stating the impact and expected recovery time

2.2. Damage Assessment Procedures

Damage assessment to the system should be conducted as quickly as the given conditions permit, with personnel safety remaining the highest priority.

- Contact GIS Cloud Hosting Services - Brokered Services for impact analysis via the GIS Helpdesk ticketing system
    - Contact AWS directly if Brokered Services is unavailable to gather impact analysis to data center operations
        - Cause of the emergency or disruption: AWS publishes a service health dashboard at https://status.aws.amazon.com/ that will, for all affected services and regions, describe the problem and estimated time to restore service
        - Whether the outage will cause permanent data loss: In general, AWS storage services are designed to be durable and to survive downtime without data loss, so even if the service becomes unavailable, data is not lost because it is replicated several times in disparate physical locations. The AWS service health dashboard, or AWS support, would be able to give guidance about whether an outage may have the potential to cause data loss
        - Estimated time to restore normal services: In the event of a limited outage (affecting a single physical site / AWS availability zone) it is possible to restore service in 2-4 hours from snapshots. In the event of a widespread region-wide outage, it is possible to restore service in 24-48 hours by redeploying applications and/or restoring cold archives
- Contact government stakeholders and determine course of action for contingency plan activation
- If Contingency Plan is to be activated, draft media release for stakeholders stating the impact and expected recovery time

2.3. Activation Procedures

The Contingency Plan is to be activated if one or more of the following criteria have been met:

- Disaster declaration by Executive Management
- System unavailability is over 24 hours
- Stakeholders provide directive to activate the contingency plan

Steps to activate the Contingency Plan:

1. Notify all Team Leaders and inform them of the details of the event, and if relocation is required.
2. Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and be prepared to respond and relocate if necessary.
3. The Contingency Planning Coordinator is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
4. The Contingency Planning Coordinator is to notify the alternate site that a contingency event has been declared and to prepare the facility for the organization’s arrival.

5. The Contingency Planning Coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

3. Phase 2: Recovery

By design, all EC2 instances within Geoplatform store any data that is meant to be persistent on Elastic Block Storage (EBS) volumes. It is possible, via the AWS APIs, to take consistent point-in-time snapshots of these volumes. It is Zivaro's policy, for instances that are Zivaro-managed, to create automated backup snapshots on a regular basis.

At a high level, recovery operations consist of restoring the last-known-good snapshots, provisioning new EC2 instances and mounting the restored volumes to them.

Zivaro's practice for its managed environments is to utilize CloudFormation to provision user accounts and the networking infrastructure, and Ansible playbooks to configure the instances and applications themselves.

3.1. General Recovery Process

There are separate recovery processes for the GIS Cloud Hosting Services - Brokered Services and the Software Development team. Those processes will be defined separately.

GIS Cloud Hosting Services - Brokered Services General Recovery Process

This section provides procedures for recovering the application while AWS repairs damage to the original system and capabilities. In general, the steps to recover are:

1. Update networking configuration
2. Recreate databases
3. Recreate virtual servers
4. Re-deploy applications
5. Acceptance testing
6. Advise clients of appropriate DNS record entries

Software Development Team General Recovery Process

In a catastrophic failure that eliminates all five Northern Virginia data centers, the Software Development Team will take the following actions to restore operations in a different zone that would be available in the United States (Northern California or Oregon). The following events would occur to restore operability to the GeoPlatform suite:

1. Impact Assessment to DOI Cloud
2. Notify GIS Cloud Hosting Services - Brokered Services, stakeholders and team members than an outage has occurred
3. Pull backup data from S3 locations
4. Provision a Virtual Private Cloud in a contingency zone
5. Provision subnet and gateway in the VPC

6. Provision Elastic Load Balancers in VPC
7. Provision a Relational Database (RDS) in the specified region
    - Restore backups from S3 to the RDS
8. Provision EC2 instances as defined in the Bill of Materials, or "GeoPlatform IPs and Endpoints.xlxs"
9. Deploy code to newly provisioned servers and build applications
10. Test newly deployed operations
11. Coordinate with government DNS personnel on name change requests
    - Validate new DNS entries
12. Notify team members and stakeholders that contingency environment is operational

3.2. Specific Recovery Process

There are separate recovery processes for the GIS Cloud Hosting Services - Brokered Services and the Software Development team. Those processes will be defined separately.

GIS Cloud Hosting Services - Brokered Services Specific Recovery Process

1. Recreate networking (Virtual Private Cloud) configuration
    - If the network is built via CloudFormation, update any references in the template to unavailable regions and availability zones and run the CloudFormation template to re-provision all networking resources in available regions and availability zones
    - If the network environment is a legacy environment without provisioning templates available, create a template, preferably based on the AWS NIST QuickStart templates - https://docs.aws.amazon.com/quickstart/latest/compliance-nist/templates.html
    - Success criteria: all routing rules to all application tiers have been recreated
2. Recreate databases (RDS Instances)
    - If any database resources need to be re-created, create new RDS instances and restore them from the last-known-good-backup
3. Recreate virtual servers (EC2 instances)
    - GeoPlatform: Utilize the AWS tools to deploy the applications onto the virtual server instances. Zivaro will restore virtual servers and establish appropriately secured network connectivity according to specific guidelines in the SLAs. The customer will be responsible to reconstitute the n-tier web application environment.
    - Non-GeoPlatform: If any EC2 instances need to be re-launched, update any references to unavailable regions or availability zones and re-launch the Ansible playbooks. Also, update any database references if necessary
4. Re-deploying applications
    - Ensure and verify physical and logical connectivity
5. Perform User Acceptance Testing to ensure that all systems are running as expected
6. Advise clients of appropriate DNS record entries

- The Brokered Services will provide necessary DNS targets that terminate on load balancers and proxy-WAF instances, as needed to restore functionality. The Software Development Team is responsible for implementing the appropriate DNS record entries.

Software Development Team Specific Recovery Process

1. Obtain backup from S3 bucket “**s3://doi-prod-backups/**”. Nightly backups for databases and applications live under the “**s3://doi-prod-backups/<application>**” for key applications as follows:

    - IDP/IDM – user database for MongoDB
    - CCB (Community Core Bundle) – Community site files and MySQL database backup
    - PORTAL– Portal site files and MySQL database backup
    - Dashboard – Site files and MySQL database backup
    - Foswiki – Site files backup
    - GIRA - Site files and MySQL database backup
    - Mongodb – Mongo database backups for IDM and Marketplace databases
    - REGP – Mongo database backups for REGP application
    - Survey - Site files and MySQL database backup

2. Provision the VPC in the available contingency zone. Preferred is Northern California regions as AMIs for each application are already shared between primary and this region.

    - Provision subnet and gateway for VPC
    - Elastic IP addresses for the following
        - IDP
        - PORTAL (Portal CMS instance)
        - GIRA
        - CCB (Community Core Bundle CMS instances)
        - WIKI
    - Elastic Load Balancers listening on Port 80 and Port 443 for:
        - WMV
        - SURVEY
        - REGP
        - APP
        - REGISTRY
        - PORTAL
        - MARKETPLACE
        - MAPS
        - DASHBOARD
    - Provision SSL certificate for geoplatform.gov (a wildcard certificate)
    - Provision Relational Database (RDS) in AWS US Zone East/West depending on availability after an incident. This can be achieved using the AWS console:
        - Database size/type: db.t2.medium

- Provision AWS EC2 Instances for each application. See “GeoPlatform - Buildsheet and Details R13.xlsx” or the Technical Considerations section for specifics for size and instance details. Assign the IAM role “ec2-codedeploy” to each instance during launch
- Verify that each server has the appropriate AWS key pair associated with the instance. This allows code, scripts and environment variables to be deployed to the instance
- Create code deploy services for each environment to deploy the application to the Production (PROD) environment
- Application servers are built from an automated script that pulls code repository from the GitHub repository “GeoPlatform/<AppName>”
- GeoPlatform Software Development tests each application and verify that the application is available per the application specific test plan
- Contact government personnel in charge of DNS requests for the new environments – David Boldt @ dboldt@usgs.gov or alternate Robbie Moreland @ pmoreland@usgs.gov.
    - Preferred method: To issue a service ticket for tracking purposes, contact the GS Help DNS group at gs_help_dns@usgs.gov
        - idp.geoplatform.gov
        - sp.geoplatform.gov
        - www.geoplatform.gov
        - cms.geoplatform.gov
        - survey.geoplatform.gov
        - viewer.geoplatform.gov
        - dashboard.geoplatform.gov
        - servicechecker.geoplatform.gov
        - registry.geoplatform.gov
        - maps.geoplatform.gov
        - ckan.geoplatform.gov
        - regp.geoplatform.gov
        - ccb.geoplatform.gov
        - app.geoplatform.gov
        - gira.geoplatform.gov
        - marketplace.geoplatform.gov
    - Validate that each endpoint is available and loads without error
    - Contact and notify shareholders that the GeoPlatform contingency site is available

3.3. Technical Considerations

The following section provides the types and sizes of each resource to be provisioned in the contingency environment.

- EC2 Instances
    - Instance sizes will mirror the existing production environment and can be expanded as needed

    - EC2 instances are living instances that have established baselines for each customer environment stated in the SLA, but have the capability to quickly scale capacity up or down as customer requirements can vary daily. These customer requirements are submitted through the Zivaro Help Desk ticketing system which will capture and track these changes of customer requirements to resolution. The customer assumes responsibility from Zivaro for the technical considerations for reconstitution of their environment after the specific baseline stated in the SLA has been established. Customers are responsible for reviewing their SLA Part 2 on an annual basis to ensure their baseline is setup and continually monitored.

- Relational Database
    - Database instance sizes will mirror the existing production environment and can be expanded as needed
- AMIs
    - Backup AMIs are located in both US East (Virginia) and the US West (Northern California) regions
- DNS
    - DNS entries for GeoPlatform.gov are handled externally by USGS. Point of contact is David Boldt at dboldt@usgs.gov or alternate listed in Table VII
- Program Code
    - Private Code repositories are hosted by GitHub at the following: https://github.com/GeoPlatform

4. Phase 3: Reconstitution

This section discusses activities necessary for restoring system operations at the original or new site. When the computer center at the original or new site has been restored, system operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

    - Contact Zivaro or AWS and ensure that the datacenter(s) in the US East, US West, and GovCloud (US West) regions are operational, as required, depending on where the asset resides.
        - AWS US East/West and GovCloud (US-West) Regions, including all the facilities at the alternate sites, are compliant with FedRAMP requirements at the Moderate impact level. AWS datacenter facilities that are not FedRAMP compliant, will not be utilized, such as the Ohio region, which is currently non-compliant.

- Notify shareholders and team via email that the site operations will be transferred back to the original operations facility/region
- Backup the data from the contingency sites to the appropriate S3 buckets every morning. The S3 buckets retain daily backups for a week, 16 weekly backups, and one monthly backup indefinitely. All data will be encrypted at rest.
- Determine what legacy components are available after operations at primary site have been approved (where applicable). These may include:
    - Elastic Load Balancer

  - Subnet
  - Security Groups
  - Elastic IPs
  - RDS
  - EC2 Instances
  - VPCs

- Migration of contingency system takes place by copying Amazon Machine Image (AMI) from contingency site location to original operations facility during non-peak hours
- If RDS instance is not already present, then allocate the appropriate RDS instance at the original facility and restore data
- Test system and application functionality on newly restored site
- Create DNS requests for the newly restored systems
- Once the restored system functionality is restored and DNS requests resolve to the new site, shut down (turn off) the contingency servers after 48 hours of operation
- After 480 hours of continuous operation without incident, it is acceptable to terminate the EC2 instances, RDS, and all other objects at the contingency site

4.1. Original or New Site Restoration

The following subset of procedures (per team) can be followed to restore or replace the original site so that normal operations may be transferred.

GIS Cloud Hosting Services - Brokered Services & Software Development Team Procedures

- Verify that the original datacenter is operational and ready to resume operations for GeoPlatform

Software Development Team Procedures

- Notify stakeholders that migration from contingency site back to the original site will commence
- Verify that current backup data is in the “s3://doi-prod-backups/<app>” bucket. If not, run backup script to backup pertinent data for each instance and/or database
- Create an AMI image of each contingency server. Copy the newly created AMI from the contingency region to the original regional (US AWS West to US AWS East)
- Launch each application AMI as defined in the “GeoPlatform IPs and Endpoints.xlsx”
- Provision Subnets per Bill of Materials and/or CA Boundary Components.xlsx
- Provision Elastic IPs per Bill of Materials and/or CA Boundary Components.xlsx
- Provision Elastic Load Balancer per Bill of Materials and/or CA Boundary Components.xlsx
- If the RDS service has been restored, then restore MySQL data to the “mysql-doi-production-rds” instance. If it has not, then provision a new RDS instance as defined in the “GeoPlatform - Buildsheet and Details R13.xlsx”
- Verify that the applications are operational at the original facility according to test plan

- Send out the DNS request to GS Help DNS at gs_help_dns@usgs.gov so they may enter the new HOST records for the original site
- Verify that DNS requests are resolving to the new site and then turn off the servers operating at the contingency site
- After 480 hours of continuous operation without incident, it is acceptable to terminate the EC2 instances, RDS, and all other objects at the contingency site

4.2. Concurrent Processing

The following procedures are used to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

GeoPlatform Software Development Team Procedures

- Verify that the original site's DNS resolves and no instance or infrastructure outages occur in a 48 hour period at the original site. Once stability is achieved, servers may be shut down at the contingency site

4.3. Plan Deactivation

The following procedures to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

GeoPlatform Software Development Team Procedures

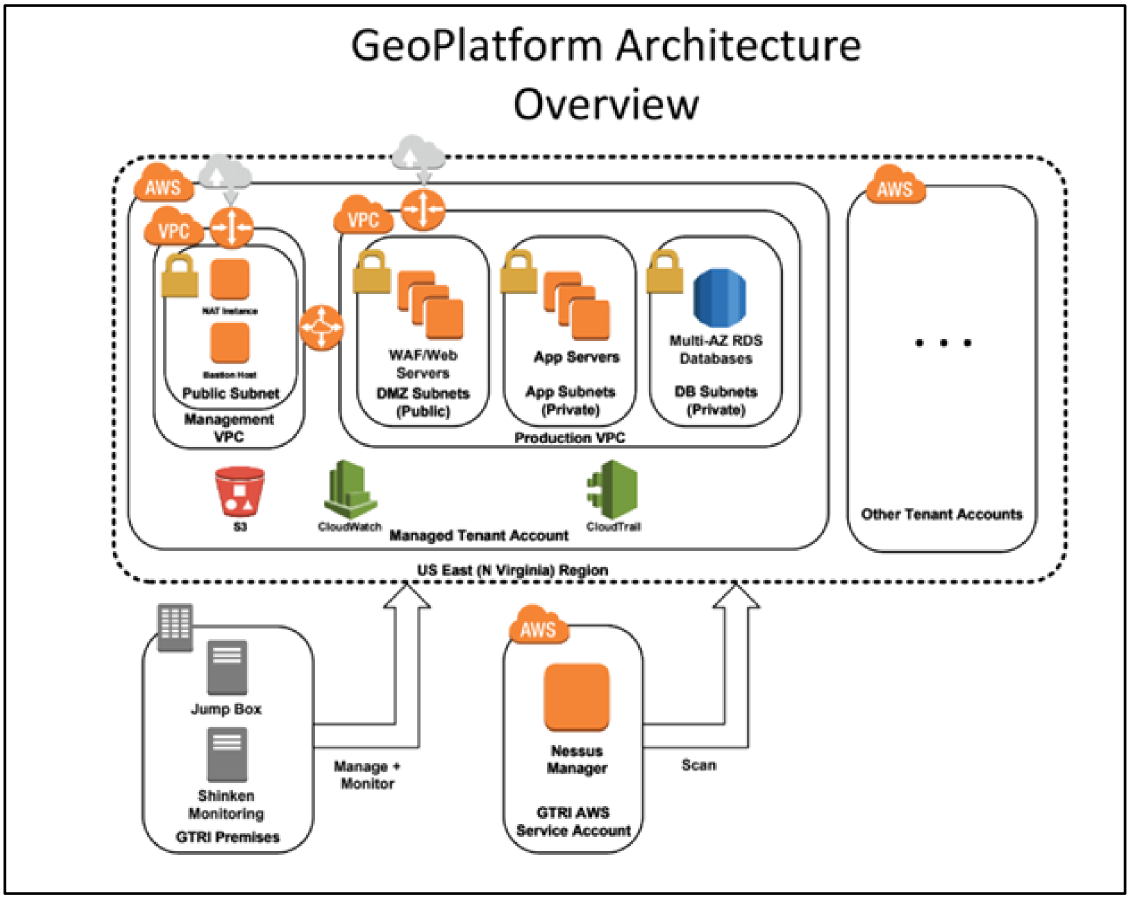
- Using the performance monitoring tools, verify that there are no instance outages for 480 hours and that hardware utilization does not cross performance thresholds for automated alerts
- Once operational stability is achieved at the original site, and after receiving customer/stakeholder approval, terminate operations at contingency site
- Terminate
    - EC2 Instances
    - RDS Instances

5. Appendices

Appendix A: Personnel Contact List

Disaster Recovery Task	Accountable Personnel	Phone Number
AWS POC Operations Primary	Network Operations Center (Zivaro)	1-855-290-5488
AWS POC Operations Secondary	Chris Martin (Zivaro)	720-836-7412
Cloud Security Architect	Chris Martin (Zivaro)	720-836-7412
Data Backup	Lee Heazel (Image Matters)	812-339-9396
Data Recovery	Lee Heazel (Image Matters)	812-339-9396
C/DRP Testing	Lee Heazel (Image Matters)	812-339-9396
Disaster Reporting to CSIRC	Forest Gafford (Image Matters)	812-339-9396
Contacting Media	Thomas Dabolt	202-208-4109
Authorizing Official	Thomas Dabolt	202-208-4109
DNS Requests	David Boldt (Primary) Robbie Moreland (Alternate)	703-648-5679 573-308-3512
System Owner	Kayloni Ah Tong	202-513-0787
Information System Security Officer (ISSO)	Jacob Guzman	970-219-5394

Appendix B: Architecture and Security Environment



The security environment shall contain the following items, which must be protected and replicated to ensure that the contingency plan is able to operate and function.

- Amazon Web Services account number 824888058401
    - This account encapsulates all necessary infrastructure to operate the GeoPlatform to include server instances, firewall, elastic load balancers, backups and database systems
- GitHub account for GeoPlatform – https://github.com/GeoPlatform
    - Contains public and private code repositories necessary to build each application. Private repositories are only accessible by authenticated and authorized members of the GeoPlatform Software Development (SaaS/PaaS) Team. Public repositories provide read-only access to non-authenticated visitors for purposes of fostering a community of engaged software developers building customized, external client applications that are separate and not part of the GeoPlatform SaaS/PaaS baseline.
- Private Enterprise cloud hosted GitHub account for Cloud Services Broker – https://github.com/GTRIglobal
    - Contains private code repositories necessary to build each application

Appendix C: Equipment and Specifications

EC2 Instances

- Instance sizes will mirror the existing production environment and can be expanded as needed
    - EC2 instances are living instances that have established baselines for each customer environment stated in the SLA, but have the capability to quickly scale capacity both up and down as customer requirements can vary daily. These customer requirements are submitted through the Zivaro Help Desk ticketing system which will capture and track these changes of customer requirements to resolution. The customer assumes responsibility from Zivaro for the technical considerations for reconstitution of their environment after the specific baseline stated in the SLA has been established. Customers are responsible for reviewing their SLA Part 2 on an annual basis to ensure their baseline is setup and continually monitored.
    - A list of all EC2 instances used in GeoPlatform can be found in the BuildSheet (GeoPlatform - Buildsheet and Details R13.xlsx)

RDS Instances

- Database instance sizes will mirror the existing production environment and can be expanded as needed
- A list of all RDS instances used in GeoPlatform can be found in the BuildSheet (GeoPlatform - Buildsheet and Details R13.xlsx)

Contingency Plan Approvals

Authorizing Official Signature

Signature: Thomas Dabolt	
Name: Thomas Dabolt	**Date:** 11/18/2018

System Owner Signature

Signature: KAYLONI AH TONG Digitally signed by KAYLONI AH TONG Date: 2018.11.18 18:29:34 -05'00'	
Name: Kayloni Ah Tong	**Date:**

ISSO Signature

Signature:	
Name: Jacob Guzman	**Date:**