



INTEGRATED DISSEMINATION PROGRAM – APPLICATION ONBOARDING GUIDELINES

Version 8.1.0

This document explains the process of onboarding an application to the IDP servers in College Park and Boulder. The Development Organization must apply with the Office of Dissemination, then work with the NCO/IDSB/Onboarding Team through the onboarding steps.

TABLE OF CONTENTS

Revision History	4
NOAA Integrated Dissemination Program – College Park and Boulder	5
IDP Infrastructure	6
The IDP Support Team at NCO	6
Role of the Development Organization	8
Application QA Testing	9
Responsibilities After Operational Implementation	13
Deliverables	13

Revision History

Version	Date	Author(s)	Description
1.0	10/23/2013	Scott Jacobs	Created
2.0	11/12/2013	Scott Jacobs	Added info to "Monitoring and Logging" and "Failover Capability" sections
2.1	11/19/2013	Scott Jacobs	Added link to the data set lists maintained by PMB
3.0	11/20/2013	Michelle Mainelli, et al.	Modified various sections during a discussion
3.1	11/22/2013	Scott Jacobs	Applied changes based on feedback
3.2	12/3/2013	Scott Jacobs	Updated based on meeting with first Dev Org
3.3	12/10/2013	Scott Jacobs	Replaced "IDP" with "NPDS"
3.4	01/03/2014	Michelle Mainelli	"Living Version" of the Process
3.5	02/13/2014	Michelle Mainelli	Software repository will be Subversion and NPDS changed back to IDP
3.6	03/14/2014	Michelle Mainelli	Added Test Use Case as a code handoff requirement for the Development Organizations
3.7	3/27/2014	Michelle Mainelli	Added section regarding restricted data on page 5
3.8	9/12/2014	Kevin Stevens CISSP	Added section at end of document regarding the process / protocol for identifying and removing security flaws in source code during the onboarding process.
3.8	10/6/2014	Ken Ward	Formatted security section (cosmetic changes only).
3.9	10/14/2014	Ken Ward	Added diagram for process flows, Added more documentation needs, updated Tbl of Contents
4.0	08/31/2015	Tim Kempisty / Rebecca Cosgrove	Reorganized. Added intro to NCO team members. Describe Dev/QA/Production VM tiers in more detail. Added "Stages of Onboarding Process" to mimic project plan. Added scheduling estimates. Explain when documents are required. Added Weekly Quad Chart and Demonstration.
5.0	12/6/2015	Scott Jacobs	Incorporated NCO management edits and comments
6.0	12/10/2016	Scott Jacobs	Reformatted and updated information. Added info about the MDC.
7.0	04/16/2019	Anwar Al-Mallah	New Revision of Standards
7.1	05/08/2019	Craig Donahue	Updates based on feedback during last review.
7.2	5/30/2019	Carissa Klemmer	Revised references to IWSB SAs. Removed the "deliverables" section as it was complete redundant. Added more background content for NCO Tiers and the data centers.
8.0	8/1/2019	C Klemmer & S Earle	Document Released
8.1	4/1/2020	C Klemmer	Updated to include NWS Engineering Directive, minor updates to code handoff and testing plans. Added information on decommissioning of previous systems.

NOAA Integrated Dissemination Program – College Park and Boulder

Introduction

Welcome to the NOAA Integrated Dissemination Program (IDP) Onboarding Process. The NOAA IDP is managed by NCEP Central Operations (NCO). The IDP goal is dedicated to bringing mission critical NOAA applications into full operational support.

This document describes the processes and procedures necessary to transition Development Organization (DevOrg) applications to run operationally onto IDP. This process assumes that the application has obtained all appropriate approvals and is working through the Office of Dissemination portfolio manager.

IDP is built on the concept of shared data and virtual machines within a clustered private virtual cloud. This allows applications with different software design paradigms and computing needs to co-exist and run at peak performance. Input datasets exist on shared storage, and can be accessed by many projects, simplifying the data ingest process, conserving bandwidth, and accelerating the onboarding process. Product distribution is similarly shared.

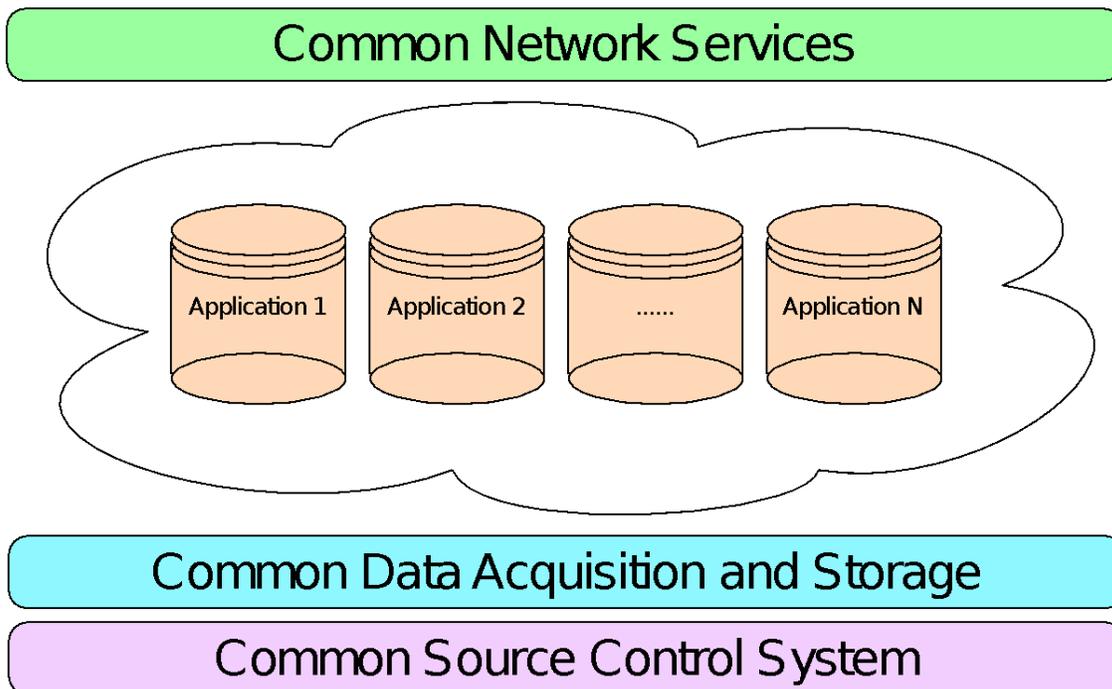


Figure 1: The private cloud represents the set of Virtual Machines available for hosting the various application containers. Each container may have unique VM configurations based on the needs of the application in that container. Shared services for Network, Dataflow and Source Control will be available to all containers.

IDP Infrastructure

This section provides a brief description of the configuration of IDP. IDP is comprised of two data centers, one in College Park, MD (CPRK) and one in Boulder, CO (BLDR). All operational applications on IDP will have independent, identical systems in each data center to provide backup redundancy and allow for regular system maintenance without any interruptions to operations.

The IDP setup will follow:

1. One Development environment for the DevOrg to build and work within.
2. At least one Quality Assurance (QA) environment for the Onboarding Team (OBT) to install and test new deliveries received from the DevOrg. . The decision of either one or two QA systems depends on how the application runs in operations, and will be at the discretion of the OBT. All changes from the DevOrg will flow first into the QA environment for thorough testing by the OBT. The DevOrg will have read only access to this environment.
3. Two operational environments, one in each IDP data center. Not until all testing has been completed, and all NCO change management approvals have been obtained, will the application will be installed on Ops. The DevOrg will have read only access to this environment.

Hardware and Virtual Machines (VMs)

The IDP System is comprised of a set of Dell PowerEdge blades for computing, and a NetApp network storage device. On top of the physical hardware, NCO uses VMWare to configure and manage the Virtual Machines (VMs) for each application. The VMs currently run RedHat Enterprise Linux. The number of CPUs and the amount of memory allocated to each VM are configured for the needs of each application.

System Administration

NCO will provide all routine system administration services - typically consisting of initial setup, patching the system and providing 24/7 support.

The IDP Support Team at NCO

The IDP onboarding process is a collaborative effort between several branches of NCO and the DevOrg.

Implementation and Data Services Branch (IDSB)

IDSB works with the DevOrg whose applications are on IDP or transitioning to IDP. These teams will be the application's "tier 2" support. They are responsible for the 24/7 operational support,

system optimization, maintenance, testing/implementing upgrades, and customer coordination/support.

The Lead of the OBT will be the focal point for contact with NCO. The DevOrg's first interaction with NCO will be with the OBT Lead and a few other key representatives. The OBT Lead will explain the process and work with the DevOrg to develop a project schedule. The OBT Lead will guide the DevOrg through the process and facilitate all interactions with the various groups in NCO.

The NCO OBT is a team of Program Analysts dedicated to IDP. They are responsible for installing and running all applications in production. The DevOrg will hand off code and a thorough set of documentation, via a combination of Google Docs and the shared Software Control System. The OBT will build the application independently, install it on the Test tier of VMs, execute the test plan, and repeat the process on the Production VMs. The goal is for the OBT to become familiar with the application, build it consistently, run it, and provide Tier 2 support (on-call, if needed), analysis, and troubleshooting. The team will also provide customer support for the application, including user management for applications that do direct dissemination.

Nested within the OBT are dedicated System Administrators (SA) who are responsible for building VMs, allocating disk space, and building the data dissemination architecture within the IDP environments.

The NCO Dataflow (DF) Team manages input and output datasets. The IDP system includes a centralized common data area for ingest and storage. IDP was designed to have all applications reading and writing data from the common storage repository. Publicly available datasets, which are also already available within IDP, are listed on the Products Catalog. For review of what is available in the catalog please email the DF Team Lead.

If an application requires a unique data set not included in the catalog, the requirement must be communicated to the DF Team through a process outlined later in this document. In addition to the input data requirements, the DevOrg will document the output of the application and requirements for disseminating those output data sets. In some cases, NCO will require a data agreement with the data provider. IDP provides common dissemination via ftp/ftps/https download, Local Data Manager (LDM), NOAAPORT/SBN, and direct delivery to a select set of organizations within NOAA.

Restricted Data: IDP does have a capability to handle restricted data. NCO operates under the impression that we are NOT working with restricted data unless we are formally notified and the restrictions are clearly described. If the application output is restricted, NCO will work with the DevOrg to set up the process by which the data is distributed. In this case, a formal sharing agreement will be required.

Operational Monitoring Branch (OMB)

The NCO Operations Monitoring Branch (OMB) provides “Tier 1” support and monitors the application and infrastructure health of the entire data center 24/7/365. The teams responsible for this are the Senior Duty Meteorologists (SDMs) and Tech Control (TC). If an issue is detected OMB follows clearly documented procedures for resolution.

Tier 1 and Tier 2 support responsibilities will be negotiated and defined in a Roles and Responsibilities document for each application that is signed across both NCO and the DevOrg.

Infrastructure and Web Services Branch (IWSB) and Network and Security Branch (NSB)

IWSB and NSB provide all system administration and network services on IDP: Defining architecture standards, creating user accounts; patching the system, managing firewall rules, etc. In some cases, such as with web applications and databases, IDSB may need onboarding assistance from IWSB.

Role of the Development Organization

The DevOrg will educate NCO about the application and requirements to run the application. Once the requirements have been gathered, OBT SAs will build a development environment to agreed upon specifications. The DevOrg will install the application on IDP in the development environment. Once the application has been thoroughly tested, they will deliver the application and all necessary documentation to the OBT for onboarding and implementation. To help with troubleshooting, the DevOrg must provide information about known problems and solutions to NCO. This information will be incorporated in the OBT maintenance documents and/or the Big Brother monitoring web pages.

The DevOrg will provide “Tier 3” support for the application. All applications must have 2 points of contact that can be reached out to on a 24x7 basis during emergency situations when the OBT Tier 2 support can not resolve the issue. This will be documented in the Roles and Responsibilities document which must be signed by director and program level personnel prior to go-live. If the issue can not be resolved quickly the DevOrg will join an NCO Tiger Team, which will be established to solve high impact and/or particularly hard problems encountered in production.

The DevOrg will provide no less than annual, and no more than quarterly scheduled updates to their operational application in IDP. Within these releases the DevOrg will respond to any requirements given by OBT. The DevOrg will also be able to quickly provide a code release to any identified security vulnerabilities with a turnaround of 30 days or less.

Redmine Ticketing System

Within the NCO Infrastructure there exists a Redmine Ticketing System that allows NCO support teams to create/monitor issues within NCO projects that include IDP Applications. With the exception of time critical bug fixes, the DevOrg is responsible for resolving all open tickets with each software update. All tickets that are resolved must add a complete explanation of the resolution, including relevant files modified to address the bug. The OBT will verify the fix during testing and close the bug following implementation into operations. If a ticket cannot be resolved, a comment must be added and approval received from OBT Lead prior to code delivery.

Application QA Testing

The program analysts on the OBT will build and install the application in the QA Environment, using the Installation and Execution Instructions provided by the DevOrg. The OBT will execute the test plans written by the DevOrg providing hands-on experience with the code and documentation before implementation into production. The end to end testing done by OBT will ensure that the application has the resources it needs to meet the performance requirements.

The instructions and test plans should be thought of as living documents. This process will almost certainly highlight parts of the documentation that need to be changed or improved. The goal is not only to test the application for acceptance and performance, but also to refine the procedures and documentation to provide any member of the OBT the ability to run the application and troubleshoot it.

After an application is operational, the QA environment is used to test software updates and new releases of the code. The DevOrg will have read-only access to the QA environment to help with troubleshooting.

The Onboarding Process

IDP Onboarding is a sequential process of gathering requirements, documenting the project, developing, testing, executing and monitoring. Each step is designed to ensure that the application has the resources it needs, and is supportable in the IDP environment. The priority of application upgrades is driven by DIS.

This timeline assumes that the Devorg has followed all upstream NWS processes and approvals. That includes any CARDS process approvals, and the OPPSD Engineering Review.

<https://www.nws.noaa.gov/directives/sym/pd01001003curr.pdf>
<https://www.nws.noaa.gov/directives/sym/pd01017023curr.pdf>.

Timeline Summary

Once DIS has prioritized your project:

- Project Kick-off Meeting
- Application Preparation Phase/ Requirements Gathering - typically 20 Business Days
- NCO Development Environment Phase Build - typically 30 Business Days
- DEV Build and Test - typically 90 business days
- Build QA/Prod Environment Phase - typically 40 business days, concurrent
- Hand-Off to NCO - Milestone (approximately 120 days after project started)
- Install Application in QA Environment and test - typically 20 days
- Install Application in Operational Environment - typically 10 days
- Begin 30-Day, frozen-code, stability testing - Milestone
- Complete 30-Day Operational Readiness Test - Milestone
- Brief NCO Director for approval to implement - Milestone
- Go Live - Milestone

Step 1: Project Kick-off Meeting

A milestone in the schedule to meet with NCO technical staff and management, after approval from the Mission Delivery Council (MDC). This meeting will provide NCO with the background necessary to support the application. The DevOrg will review the information provided to the MDC. A joint NCO-DevOrg project plan will be presented at an executive summary level to give everyone an overview of the entire schedule.

Step 2: Application Preparation Phase

To prepare the application for the Onboarding Process, an initial meeting will be held with the Onboarding Team, NSB, OMB, and DF team along with the DevOrg technical leads. At this meeting, the main topic of discussion will be an overview of the application and beginning to discuss resource requirements for the application.

The schedule will also be discussed. NCO will provide a rough estimate for delivery of the required resources for the Development, QA and Production environments. Before any systems are built the IWSB Branch Chief will sign off to ensure that IDP has the capacity derived from the requirements. The DevOrg will provide an initial estimate for the code development and documentation handoff to the OBT. The OBT lead will begin updating a weekly quad with the status of milestones.

Finally, the discussion will include a definition of the roles and responsibilities for NCO and the DevOrg. NCO will be responsible for Tier 1, which includes 24x7 monitoring, and Tier 2, which covers the onboarding tasks and 24x7 on-call troubleshooting support. The details of the DevOrg's ability to provide Tier 3 support will be discussed. This information will be collected by the DevOrg and provided in the Roles & Responsibilities document.

Step 3: Development Environment Phase

During this phase the OBT SA will provision the system resources as outlined from the requirements gathering. The DF team will begin acquiring any input data specified. The DevOrg has the responsibility to create a VLAB project to track tasks and provide a code repository. When the VLAB project is ready, the DevOrg will inform the OBT Lead so the OBT can create a connected VLAB project to track onboarding tasks and to share the code repository.

If during the installation, testing and development work, the resources are found to be insufficient, the DevOrg will communicate with OBT SA to augment the resources.

If the application includes a web site, the URL must be provided to the Networking and Security Branch (NSB) to scan the site. The results of the scan will be reviewed with the DevOrg. Fixes must be made for Critical, High and Medium problems found by the scan. The application may not be handed to the OBT until it passes the scan.

Throughout the development process, the DevOrg Lead must provide the OBT Lead with weekly updates regarding progress and any changes to the code handoff date by Thursday of each week. The two Leads will work together to update the project plan and brief their respective managers.

The DevOrg must also begin compiling the required documentation for the OBT to install and manage the application in production. The following is a list of the documents, which are described in more detail in the Deliverables section:

- Release Notes (two sets, one for Onboarding team with great detail, one for public following our template)
- Installation guide
- Test plan and test cases and test harness
- Troubleshooting guide
- Site failover plan
- Patching failover plan
- Emergency shutdown steps
- Monitoring requirements

NCO OMB team will begin drafting the Roles and Responsibility documents and begin circulating them for comments. These documents need to be signed off on by both organizations prior to the go-live brief.

Once an adequate period of testing has passed with the DevOrg successfully running their code the OBT SA will begin building out the QA and Ops server environments.

Step 4: Hand-off to NCO Onboarding Team

A milestone in the project plan that signals the end of Development and the beginning of the NCO activities to bring the application to operations. The DevOrg will provide the repository tag and all required documents to the OBT.

Step 5: QA Environment Phase

The OBT will use the documentation provided by the DevOrg to install and test the application on the QA servers. All tests in the test plan must pass before the application can be moved to the next step. If the application fails installation or any of the tests, if the OBT cannot simply resolve, it will be handed back to the DevOrg to fix any problems, returning the entire process to Step 3. The OBT will add and configure the application monitoring.

If applicable, the OBT together with the DevOrg, will draft a Service Change Notice following the NWS Directive National Public Information Statements and Service Change Notices 10-1805. This is to notify all users of changes coming to the application to be implemented on IDP.

Step 6: Operational Readiness Test

All new applications, or major releases must run in a frozen QA environment for a 30 calendar day stability test. The test must run uninterrupted for the entire period. If the application fails, and the root cause is found to be internal to the application, the 30-day test will be restarted after a fix is provided by the DevOrg. Every failure is unique, and NCO management will make the decision about restarting after all the facts are gathered. During the 30-day test, NCO will monitor and support the application as if it were in production. During this period users must be evaluating the data and providing feedback.

Upgrades that are determined to be minor or bug releases may be subject to a 2 week frozen stability test. Based on the release notes provided, the OBT Lead will make the decision if a 2 week test is required.

Step 7: NCO Director Brief

For all new applications, a milestone in the project plan to get approval to move the application to Production. An application overview, resource usage, testing standards and the Roles & Responsibilities document are presented to the NCO Director for approval. The document will be prepared by OBT and presented by OMB. OBT, OMB, IDSB Chief, NCO Director and the DevOrg are required to attend.

Step 8: Production Environment Phase

The OBT will use the documentation and the results of the QA activities to install and verify the Production environment for both CPRK and BLDR. For an initial installation, the Production servers will be fully configured and the Go-Live will be a single day event. For an upgrade to the application, an implementation plan will be developed by the OBT to allow the current version to continue to run while the new version is installed and verified.

Step 9: Go-Live!

The final milestone for declaring the application operational. The OBT Lead will announce the operational status for the application to the NWS executives and the DevOrg managers. After the go-live NCO will apply any changes made to the production tier, and flush them back through the QA and Dev tiers. This will ensure that all environments remain consistent.

Step 10: Tear down of previous systems

Regardless of where the application was previously hosted, the old hosts of the application must be shut off upon successful go live and be fully decommissioned after 30 days (if managed by NCO), or following the guidelines put forth by the owner of the previous system.

Responsibilities After Operational Implementation

Once the application is implemented into Operations on IDP, NCO will provide 24x7 support and any agreed-upon customer support functions. The DevOrg will provide Tier 3 support and supply two phone numbers that Tier 2 can call as needed.

NCO will expect updates to the application to come through the same onboarding process. The priority of upgrades NCO accepts will be led by the Office of Dissemination. Some updates will be minor and require limited testing. Some updates will be major enough to require new agreements, additional hardware, and the full onboarding process. The IDP OBT Lead will work with the DevOrg to determine the scope of the upgrade.

The OBT team lead will hold regular status meetings with all organizations with operational applications on IDP to gauge performance and discuss the status of any pending upgrades. These are in addition to the DIS bi-weekly status meetings.

Deliverables

Required Documentation from the Development Organization

The DevOrg must create a set of artifacts and make them available to NCO. The documents are required to provide a context for the application and to provide information about the installation and execution of the application.

Each document listed plays a significant role in sharing information with NCO for the successful installation and execution of the application in the IDP environment.

Executive Summary / Charter

This document will explain the need for the application in NWS operations. It will identify data inputs and products created, as well as the users of those products. This document is required for the initial meeting with NCO.

System Resource Requirements

The DevOrg will bring the known system resource requirements to the initial meeting with NCO. After the meeting, this DevOrg and NCO will collaborate together to fill out our system spec template with the requirements. The requirements should include CPU, Memory, Storage, data, users, and website hits/volume (if applicable). Those then need to be approved by the IWSB Branch Chief.

Input and Output Data Requirements

This document will provide details about the input to, and output from, the application.

For the input data, the DevOrg must provide:

- Data provider or source
- Method of acquisition (e.g., http, ftp, pull from provider, provider pushes to IDP, etc)
- File format

In some cases, NCO may already be ingesting required data. For those data sets, NCO will provide a location on disk for the application to read the data files

For the output data, the DevOrg must provide:

- The users of the products
- Method of distribution (e.g., ftp, web site, etc)
- Full WMO headers of products to be sent on the SBN
 - If these are existing products, a cutover plan must be included in the data requirements document
 - If these are new products, or the header is changing, the DevOrg and NCO will work together to get approval for the products from the Data Review Group and announce the products via a Service Change Notice
- Any channels of communications to the applications users community for OBT to advertise to
- The level of effort needed to field helpdesk questions by the user community
 - If this is determined to be extensive there will need to be additional support roles determined so that NCO can staff accordingly.

Project Management Plan and Schedule

The DevOrg Lead and the OBT Lead will work together to create the Project Plan and Schedule. After the initial meeting with NCO, the DevOrg will set an initial estimate for the code and documentation handoff. The Project Plan will reflect the development work to meet that goal. The OBT Lead will add the onboarding tasks to the Project Plan using the code handoff date as

the start of the activities. Both Leads will jointly brief managers of both organizations regularly on the project progress at the DIS bi-weekly and through NCO Quads.

Code and Documentation Handoff

The documents must comply with the following requirements:

- Formats allowed: *.doc, *.pdf, Google Doc, Sheets, or Slides
- The document should be placed in a single file or web page (for Google formats) in order to be easily printed by OBT when needed

The following documents should be delivered to NCO with the source code:

Software Build and Installation Instructions

The DevOrg must provide a detailed guide for building and installing the application. The NCO OBT will use this document to ensure the application is complete and installed properly. The format should follow a step-by-step outline of the *actual commands* necessary. It also must include roll back instructions that have been tested by the DevOrg.

Execution Instructions

The DevOrg will include a document explaining the *start* and *stop* procedures for the application. This would include any *cron* entries that ensure the application is running. If the application must run on system reboot, those details must also be included.

Test Plan and Test Cases

Once the application is installed and running, it must pass a set of tests provided by the DevOrg. The DevOrg must run each test successfully prior to code delivery. The DevOrg should build automated tests that can be run as part of the build steps. If that is not possible, the Test Plan and individual Test Cases should exercise all parts of the application. They must include the expected results output. This document is best delivered as a spreadsheet with each test on a new line and a column for the OBT to enter “pass” or “fail”.

Monitoring Plan

NCO currently uses the Big Brother monitoring tool. Big Brother allows thresholds to be set for resource usage and other unique data. The DevOrg and the OBT will work together to identify the logs and processes to monitor for the application. Background information and call-out steps will be added to the Big Brother notes web pages. The joint plan will define all the monitored data and usage thresholds. The DevOrg is responsible for the requirements, the OBT is responsible for the written tests.

Release Notes

The first draft Release Notes will be created by the DevOrg for the code and document handoff. NCO will provide the document format. The Release Notes will be sent to users and managers prior to the 30-day Operational Readiness Test. The final version of the document will be sent with the formal announcement of the operational status of the application. For a template of the release notes form please contact the OBT Lead.

Troubleshooting Guide

Over time, all software will exhibit problems. For known problems, the DevOrg will provide a guide defining the problems and the steps to resolve them. The OBT provides on-call support for all IDP applications, therefore, the document should present the steps that can be executed off-hours without the need to contact the DevOrg. This document must be updated as new problems are encountered.

System Requirements Changes (Optional)

Every quarter the OBT does an analysis of the resource utilization of each application. This is done to ensure that during a maximum load (critical weather) event that the resources don't exceed 80% utilization. The OBT may make utilization changes to ensure that all IDP resources are being utilized in the most efficient way possible, with a target standard of 80% utilized.

Inventory of Existing Production Systems

As a part of going live on IDP, all previous systems used to run the application must be identified by the Development Organization so that a proper decommissioning of those devices and/or configuration can occur.

Failover Plans

NCO maintains two data centers, one in College Park and the other in Boulder. The DevOrg must work with the OBT to develop a plan for failovers between sites. The failover must be fully automated with a single action required by a human to initiate it. There are certain situations where executing the failover will only be done in production environments. If the failover is so complicated that it requires testing outside of production we will build 2 QA environments. The DevOrg will provide the concept and requirements for failovers, the OBT will be responsible for execution.

Emergency Shutdown Procedure

The document should describe the steps of how the application will be moved to the other site as quickly as possible in the event of an emergency in the entire data center. In addition, it will describe how to quickly shutdown the application at the emergent site.

Roles & Responsibilities

The document includes the roles and responsibilities for NCO and DevOrg. Usually, NCO is responsible for Tier 1, which includes 24x7 monitoring, and Tier 2, which covers the onboarding tasks and 24x7 on-call troubleshooting support. The DevOrg will provide Tier 3 support and any agreed-upon Operations & Maintenance funding. In addition, The DevOrg will provide periodic updates to the application, and respond to any infrastructure or security changes on IDP that require modification to existing applications.