



# *NWCG Application Architecture*

## **Principles, Guidelines, and Standards for Data Exchange Between Applications**

**Program  
Management  
Office**

Version 1.0

**National Wildfire  
Coordinating Group**

**Information Resource  
Management**

January 2003

This document is a publication of the NWCG IRM Program Management Office. Questions or comments regarding this document should be directed to:

**IRM Program Management Office**

National Wildfire Coordinating Group

3833 S. Development Avenue

Boise, ID 83705

**Barry Mathias, Program Manager**

(208) 947-3740

barry\_mathias@blm.gov

**Allen Deitz, Repository Manager**

(208) 947-3742

allen\_deitz@blm.gov

**Judy Crosby, Data Architect**

(208) 947-3741

judy\_crosby@blm.gov

**Al Borup, Applications Architect**

(208) 947-3743

al\_borup@blm.gov

Introduction.....3  
Background.....3  
General Principles.....4  
General Guidelines .....5  
Long-Term Focus.....5  
Conclusion .....6

## Introduction

This document is written for the project managers and developers of all NWCG automated systems. It conveys certain principles and guidelines to be considered in the development of data exchange mechanisms between NWCG applications. This document is not all-inclusive and should be used in conjunction with current advice from the IRMWT and IRM-PMO. Each project is unique and will have special requirements and considerations that may not exactly fit the guidelines identified within this document.

This document attempts to stay fairly high-level and avoid implementation suggestions or detail. NWCG currently has no standards for data exchange mechanisms. It is hoped that the principles and guidelines outlined in this document, along with well-conceived technical solutions for current NWCG systems to serve data to each other will become the foundation for NWCG Application Architecture Data Exchange standards.

The IRM-PMO harvests “lessons learned” from all of our project development efforts. As we gain deeper understanding of what it takes to achieve successful, enterprise-level data exchange mechanisms, this document will change. When using this document, consider the version date, and check with the IRM-PMO for newer revisions. Generally, the date of an IRM-PMO document determines the precedence of information as it may apply to other IRM-PMO documents.

Key words may be helpful in distinguishing principles, guidelines, and standards. Within this document a principle is identified by an action verb, guidelines contain the verbs “will” or “should”, and standards contain the verb “shall”.

## Background

In the past, application interfaces have been built to meet specific data exchange requirements between two applications. Much like “stovepipe” or “monolithic” applications, individual made-to-order interfaces between two distinct applications typically:

- ❑ Are costly and time consuming to modify – changing a piece of code that provides the interface has the potential of impacting other code on both the data serving application and the data requesting application.
- ❑ Are not shareable with other applications that have similar data exchange requirements – the interface implementation is totally unique for two specific applications and will not work for any other purpose.
- ❑ Can cause redundant code to be created and maintained if similar interfaces with other applications are required.
- ❑ Can tend to mix business rules across applications complicating change management on both applications – for example, an application on one side of the interface might rely on the other to do all formatting of the data it requests and the format requirement changes.

## General Principles

It is important that system-to-system interface requirements transcend individual needs of any two distinct applications and be viewed from an NWCG enterprise perspective. Where practical and feasible, NWCG systems shall design and implement interfaces which allow applications to provide services to any number of systems in the entire wildland fire organization.

These enterprise-level service oriented interfaces typically:

- ❑ Offer access to particular data sets (such as official system-of-record lists), and are unaffected by other business areas of the application requesting or providing the data.
- ❑ Will not be concerned with, or affected by, business rule changes of any applications that request the data.
- ❑ Will be easily modifiable to support changes in its own business rules – changing a service-oriented interface that focuses only on its own business has little risk of affecting other parts of an application.
- ❑ Will not be concerned with or affected by whatever operating system, database package, hardware platform, or other software component in use by the requesting client application.
- ❑ Require the requesting client application to perform any custom manipulations of the data it receives.
- ❑ Provide a single interface that is accessible by multiple applications – after authentication, each requesting client application is served the data they have asked for in a predictable and consistent format.
- ❑ Will have the potential to be optionally built to be configurable for each requesting client application – parameterization of the request commands can allow for selectable data sets or formats, without the need for interface recoding.
- ❑ Have potential to use parameterized request commands to allow applications to ask for data in a variety of formats, without the need for interface recoding.
- ❑ Offer high potential for code-reuse and sharing – since these types of interfaces are very general in nature, once built, they have potential to be used as a template for serving another type of data with simple modifications.
- ❑ Will be required when general access to authoritative source (system of record) data is necessary – applications should be designed to ensure consistency of data with the named system of record.
- ❑ Will serve only data that conforms to NWCG data standards, if they exist.

## General Guidelines

- ❑ These interfaces can enable request parameters such as time stamps or other commands that could tailor the conditions for the selection, ordering, or formatting of data to be delivered to a requesting application.
- ❑ Unless the interface responds to request parameters, all requesting applications should receive data in same format. It should not be the responsibility of the providing application to format data specifically for each and every client that requests it.
- ❑ These data services should be available on an as-needed basis, and, where practical, should not attempt to dictate the periodicity by which other client applications access that service.
- ❑ Avoid trying to tightly integrate any NWCG applications – strive to keep them “loosely coupled” by employing generalized data services.
- ❑ Avoid building single “do-everything” system-to-system interfaces that try to fulfill all data sharing needs specific to any two NWCG applications.
- ❑ Divide the data needs into business area components and provide individual services to access that specific data. This may require that applications provide multiple services.
- ❑ Document any data exchange agreement between two distinct applications with an Interconnection Security Agreement (ISA) and a Memorandum of Understanding/Agreement (MOU/A). The MOU/A should delineate all expectations, limitations, permissions and boundaries associated with the data exchange. See **NIST Special Publication 800-47** *Security Guide for Interconnecting Information Technology Systems* at [www.nist.gov](http://www.nist.gov) for guidance on developing and documenting these agreements.
- ❑ Interface specifications, services provided, and contact information should be made available via the NWCG PMO website.

## Long-Term Focus

Eventually, the idea of generalized access to data should be expanded to allow generalized access and/or sharing of processes or services as well. Any NWCG application that houses data or can provide a service that is valuable to any another NWCG application or that contains “System of Record” data will make it available to any authorized application through a single, generalized interface for that data or service.

As an example of process sharing, there could be a single service that authenticates all users accessing any NWCG application. This would provide a single point-of-entry for admission to any of NWCG’s applications. It would also eliminate the need for each individual application to implement and maintain redundant authentication code. When a change to the business of authenticating a user occurs, the implementation code would only have to be changed in one place. No other NWCG business area components would be affected.

## Conclusion

From an enterprise-wide perspective, the generalized approach to service-oriented interfaces provides more robust benefits than myriad single custom interfaces between applications. Of course, there may be cases where a general approach simply cannot satisfy complex data exchange requirements between applications. The principles presented in this paper are not meant to imply that a custom interface is not allowed. However, interfaces of that nature should be the exception and not the rule.