June 3, 2013
Incident GIS Data Flow Plan

In the summer of 2012, the Rocky Mountain Area had several incidents that did not disseminate GIS data outside of the incident, as has been standard since 2006 when the GIS Standard Operating Procedures on Incidents was published by the NWCG. This led to difficulties in gaining access to GIS data for cooperators who needed timely information. This caused delays in distributing information to the public and creating products for high-level decision makers within the County, State, and Federal Governments.

Below are suggestions on how to resolve this issue within the Rocky Mountain Area. We recommend that Incident Command Teams who are dispatched to the Rocky Mountain Area follow these steps for disseminating incident data:

1. Fire perimeters and other geospatial data (*e.g. fire origin, fire line, drop points, water sources*) will be posted as soon as possible by the incident following the GIS Standard Operating Procedures (GSTOP). GSTOP is currently posted at http://gis.nwcg.gov/gstop_sop.html.
2. All maps and geospatial data should be approved by the Incident Commander(IC) or designee prior to being distributed.
3. The GIS Specialist (GISS)/Situation Unit Leader (SITL) will be provided the login and password for posting data to ftp.nifc.gov by the Rocky Mountain Area for all teams. Incidents will post data at ftp://ftp.nifc.gov/Incident_Specific_Data/ROCKY_MTN/*year*/*firename*/*GIS*/*date* .
4. The incident team will create a plan on how data and products will be distributed to cooperators who need this information in a timely manner. The scale of this plan would be determined by incident complexity and interest in the fire. Generally, the Planning Section, Public Information Officer (PIOF), and the Liaison Officer will jointly create the data flow plan. However, other interested parties may be invited to participate. At a minimum the plan should include a list of cooperators that receive data and products. A lead will be designated to update and maintain this plan.
5. When there are multiple public information specialists (PIOF) on the incident, one PIOF will be designated as the liaison between the Planning Section and the public information group to coordinate data and hardcopy map distribution.
6. These data flow procedures should be added to each Rocky Mountain Incident Management Team's Standard Operating Guide to ensure that teams have access to ftp.nifc.gov and are aware of these procedures.
7. These data flow procedures should be added to incoming team In-briefing Package to ensure that incoming IC, PIOF, Liaison Officer, and Planning Section (SITL and GISS) are aware of the Rocky Mountain Area process for data distribution.

Sensitive Data Issues -

1. Infrared (IR) data displayed on a map may become sensitive. The IR products that may become sensitive include Heat Perimeter (polygon), Intense Heat (polygon), Scattered Heat (polygon), and Isolated Heat Sources (point).
    a. When there are no sensitivity issues with the IR data, follow the normal GSTOP procedure as mentioned above by posting data to ftp.nifc.gov/Incident_Specific_Data/ROCKY_MTN/*year*/*firename* /IR/*date*.

b. When sensitivity issues arise with IR and perimeter data, as identified by the IC, host agency, or agency administrator(s) the following will occur:

    i. IR data will be posted to a password-protected area of ftp.nifc.gov, ftp://ftp.nifc.gov/Incident_Specific_Data/Rocky_Mtn/<*blind_folder*>. The username and password must be given to the Planning Section including Infrared Interpreter (IRIN), SITL, and GISS. The Planning Section will contact the Rocky Mountain Area Coordination Center (RMACC) Intelligence Officer, Marco Perea (mperea@blm.gov) to obtain the access information. Access will also be provided to cooperators who need access to this information for "For Official Use Only (FOUO)" purposes, as identified in the incident's data flow plan. The Planning Section will share their data flow plan with RMACC's intelligence officer.
    ii. The SITL will verify and approve IR data as soon as possible after it has been processed by the IRIN. If data is verified to be accurate, then data will remain on the password-protected ftp.nifc.gov site. Either some or all of the data can be moved to the non-password protected portion of the ftp site if it is determined to not be sensitive at that point, or a read-me file should be placed in the IR data folder stating the reasons for limiting the distribution to FOUO.
    iii. If it is approved, the GISS updates the incident perimeter as directed by SITL. The updated perimeter is posted as soon as possible to ftp.nifc.gov/Incident_Specific_Data/Rocky_Mtn/*year*/*firename* /GIS/*date*. A read-me file should be placed on the ftp site stating reasons for limiting the distribution of the IR data to FOUO.

2. Other sensitive data (Examples: Powerlines, dams, transmission sites, etc.)
    a. When other data is determined to be sensitive by the IC, host agency, or agency administrator:
        i. The process of developing the data flow plan stated in #4 above should include what data is sensitive and the limits to its use and distribution.
        ii. Sensitive data will not be placed on the public portion of any ftp site.
        iii. The process to follow will be the same as the IR data above. Simply:
            1. Store on password protected site for ftp.nifc.gov
            2. SITL will evaluate the sensitivity of the data and determine how it should be distributed.
            3. GISS creates derivative products from sensitive data
            4. Derivative products may/may not be posted to public FTP.
        iv. If sensitive data comes to the incident from another entity, follow all the guidelines for its use, copying, and/or distribution.