



United States Department of the Interior
NATIONAL PARK SERVICE
Natural Resource Stewardship and Science
Inventory and Monitoring Division
1201 Oakridge Dr. Ste. 150
Fort Collins, CO 80525



26 February 2018

To: Inventory and Monitoring Network Program Managers

From: Chief, Inventory and Monitoring Division

Subject: Guidance for documenting protected data

Effective: 26 February 2018

Executive Summary

1. According to federal policy, data are to be made public by default, and there are limited cases where data may be withheld from release to protect resources.
2. We need to determine what data need to be protected to avoid accidental release by IMD or cooperator staff.
3. We're asking networks to do the following for each park in their network:
 - a. Work with park staff to fill out a spreadsheet that documents protected resources and rules for disseminating and withholding information about those resources. A spreadsheet template for doing so is attached.
 - b. Draft a memo for approval and signature by the park's Superintendent that documents decisions made using the template provided in Appendix A.
 - c. Memorialize the decision by filing the spreadsheet in Data Store and the approval memo according to park or network records management policies. It is also recommended (but not required) that park Superintendents record the decision in their Superintendents Compendium.
4. We are only asking networks to focus on resources and information pertaining to IMD operations, but parks may wish to also include other natural, cultural, or archaeological resources present at their park.
5. Background and guidance on accomplishing this task follow.

Background

The Inventory & Monitoring Division (IMD) collects, maintains, and disseminates information about natural resources. Generally, IMD makes information available to park employees, regional offices, state and federal agencies, the scientific community, and the public. Dissemination of certain information, however, could put particular resources at risk. Some cultural and natural resource information is protected from public disclosure by resource confidentiality laws. These laws prohibit agencies from releasing protected information except in limited, specified circumstances. These resource confidentiality

EXPERIENCE YOUR AMERICA

The National Park Service cares for special places saved by the American people so that all may experience our heritage.

laws are intended to protect park resources from harm, theft, or destruction (Draft RM 66B; NPS 2010). Historically, decisions about what data to protect from release have been made on a case-by-case basis when IMD information is requested or as a part of the review process when IMD products are published.

In 2013, Executive Order 13642, *Making Open and Machine Readable the New Default for Government Information* (GPO 2013), and associated policies issued by the Office of Management and Budget (OMB) mandated that all data be made public by default unless those data are protected from release by one or more authorities. Further guidance from OMB (2013) instructed agencies to develop review procedures to ensure that privacy, confidentiality, security, or other restrictions to release are identified as early in the data lifecycle as practicable.

NPS RM66B (Draft), *Handling Protected Information* (NPS 2010), recommends that parks do the following to proactively identify and manage protected information:

1. Have a clearly defined process for data acquisition, storage, and archiving in place including security waivers for all personnel with access to the information.
2. Coordinate closely with data managers from I&M, cultural resources, and planning programs to ensure that there are similar processes in place between programs and via linked server data.
3. Clearly identify the individuals at the park and programs who have clearance and line approval to make decisions about data and its release (such as the park FOIA officer), and route all requests for data release through those individuals.
4. Develop and maintain lists of park resources that may qualify as resources at risk.
5. Identify the specific types of information about these resources that constitute protected information.
6. Determine the reduced level of resolution at which location information for particular resources can be shared without a confidentiality agreement.

The process identified in this guidance meets the requirements for steps 4-6. Because data are intended to be open and public by default, networks must identify potential types of data that must be classified as protected as early as possible in the data management workflow so as to limit the risk of accidental dissemination. Networks must work with appropriate park staff (typically resource management chiefs or above) to define what data are protected, the degree of protection warranted, and if/how data will be disseminated.

This guidance outlines the means for park and IMD staff to develop lists of resources that may warrant protection from data release, the type of information about those resources that may be released (if any), and procedures for documenting these decisions so that they can be applied consistently across IMD efforts and other park, region, or national programs as appropriate.

The goal is to maximize the amount and accuracy/completeness of data that are released to the public, but final determination of what data are considered protected rests with each park's Superintendent. In general, IMD and park staff should seek to identify the basic rules for protection of data (those that apply in all

EXPERIENCE YOUR AMERICA

The National Park Service cares for special places saved by the American people so that all may experience our heritage.

cases for a given resource), recognizing that the Superintendent may authorize release of additional (protected) data if he/she determines that doing so will not result in harm, theft, or destruction of resources.

Process for Identifying Protected Information

Authority to determine what data should be protected rests with each park's Superintendent, with input from resource management staff and subject matter experts (e.g., IMD staff). This determination involves several steps:

1. Identifying which species or resources potentially warrant protection from data release,
2. Determining the appropriate level of protection warranted (legal or operational protection),
3. Determining what information about protected species or resources (if any) can be released without resulting in harm, theft, or destruction, and
4. Determining who should not have access to protected data.

We have developed a spreadsheet template to be used in consultations between IMD and park staff to document these determinations. The template is pre-populated with categories of resources that should be considered, and options for identifying the level of protection, from whom records should be protected, methods of protection, for how long records should be protected, and associated notes for each resource. Networks will need to work with park staff to identify any resources that need to be added to the list, delete any resources that aren't applicable to the park, and choose the appropriate means of protection for each.

Note that parks do *not* have to determine dissemination rules on a species-by-species basis. Resources can be "lumped" as appropriate. For example, a park may wish to use the same rules for all federally-listed T&E species. To aid the decision-making process, prior to working with park staff it is recommended that networks:

- Determine/request whether parks maintain a list of park resources that may qualify as resources at risk as recommended by RM66B.
- Use NPSpecies to generate a full species list for all taxa with the "full list with details" option selected. This list will indicate any species in the system that have a state or federal T&E status as of the last refresh of the state and federal lists.
- Use any established data protection standards included in the data quality standards documents associated with your network's protocols or quality assurance plans

Documenting Decisions

After completion of a park's spreadsheet, networks should use the information to draft a memo for Superintendent approval using the template in Appendix A. Once approved, networks should file a digital copy of the memo and the spreadsheet on Data Store with other protocol documents, and the hardcopy should be filed in the park and network records management systems as appropriate.

Additionally, it is recommended that a record of the decision be entered into each park's Superintendents Compendium. This will ensure that the decision is both persistent over time as park leadership changes, as

EXPERIENCE YOUR AMERICA

The National Park Service cares for special places saved by the American people so that all may experience our heritage.

well as provide a cue to park staff to review and update the decision as appropriate. Recommended language is as follows:

“The park superintendent has identified resources that are rare, threatened, endangered, or commercially valuable. The locations of these resources and information that could be used to locate them are protected from public release when there is a risk of harm, theft, or destruction. The list of resources that are protected are maintained by [park resource manager or I&M network]. Data about these resources are only reported as described in [MEMO reference]”. The most recent approved list of resources is available at [provide URL to link of record in Data Store].”

Definitions and Considerations

Types of Data that Might Warrant Protection from Release

NPS does not define “sensitive” data per se, but does allow data to be protected from release under the Freedom of Information Act (FOIA). Generally, data may be protected from release when doing so will result in harm, theft, or destruction of the resource (Draft RM 66B; NPS 2010). Justification for withholding information—including the **specific location, abundance, presence, or absence** of a resource—may be based on any of the four resource confidentiality laws or the Executive Order applicable to NPS” (Draft RM 66B; NPS 2010):

- National Parks Omnibus Management Act, Section 207, [16 U.S.C. § 5937](#), allows NPS to withhold information regarding the nature and specific location of certain cultural and natural resources in the national park system from release under FOIA. The law also identifies conditions under which the Secretary may release this information. Information concerning the nature and specific location of a National Park System resource which is endangered, threatened, rare, or commercially valuable, of mineral or paleontological objects within units of the National Park System, or of objects of cultural patrimony within units of the National Park System, may be withheld from the public ([16 U.S.C. § 5937](#)).
- National Historic Preservation Act, [16 U.S.C. § 470w-3](#), allows an agency to withhold information about the location, character, or ownership of certain historic resources under certain circumstances. This law also identifies conditions under which the Secretary may release this information.
- Archaeological Resource Protection Act, [16 U.S.C. § 470hh](#) (and the NPS implementing regulation, [43 C.F.R. § 7.18](#)) prohibits the release, under FOIA or any other law, of information concerning the nature and location of certain archeological resources. This law also identifies conditions under which the Secretary may release this information.
- Federal Cave Resources Protection Act, [16 U.S.C. § 4304](#), prohibits making information concerning the specific location of any significant cave available under FOIA except under certain circumstances. “Significant caves” are identified by the DOI Secretary; this list is updated periodically ([16 U.S.C. § 4303](#)).

EXPERIENCE YOUR AMERICA

The National Park Service cares for special places saved by the American people so that all may experience our heritage.

- [Executive Order No. 13007](#), Indian Sacred Sites, instructs agencies to accommodate access to and ceremonial use of Indian sacred sites on federal land by Indian religious practitioners, avoid adversely affecting the physical integrity of such sacred sites, and maintain the confidentiality of those sacred sites, where appropriate.

Most relevant to IMD activities is identification of resources that are endangered, threatened, rare, or commercially valuable, but information pertaining to other resources at parks may warrant protection as well. For example, networks with monitoring at “significant caves” or at culturally sensitive locations will need to protect that information in a way that is consistent with park practices. Likewise, networks that monitor harvested species of fish and wildlife may need to protect information to ensure that legislatively approved activities such as hunting, trapping, and fishing conform to applicable Federal and State laws (36 Code of Federal Regulations (CFR) 2.2, and 43 CFR 24.4.).

Identification of resources that potentially warrant protection is, in many cases, straightforward. For example, data pertaining to state- or federally-listed or candidate species are potentially protected based on their threatened/ endangered status. Data about species like ginseng and *Galax* are also potentially protected because of their high commercial value. Species that are legally hunted, trapped, and fished are potentially protected. However, identifying all potentially-protected resources at a park and deciding which data could result in harm, theft, or destruction of the resource if data were made public can only be made in consultation with park staff.

Levels of Protection

Legally Protected. Applies only to data protected from release based on one or more of the authorities listed above.

Operationally Protected. Applies to data for which there is no statutory authority to withhold data, but NPS practice is to not release data. Operationally-protected data must be released if requested, but is withheld from release by default to protect site fidelity, visitor safety, and resource conditions (in instances where data have already been made public). Examples include:

- Locations of long-term monitoring sites where there is a reasonable expectation that disclosure of specific locations would increase human activity near the site(s) and affect the representativeness of ongoing monitoring efforts.
- Locations of mine entrances, which are typically already publically-available through USGS publications.

In no case should data be classified as “operationally protected” to allow NPS or partner staff time to publish findings.

Not Protected. By default, data are not protected from release unless there is a statutory authority to withhold data. Data that don’t fall into one of the categories above are considered not protected by default (we are not asking networks and parks to explicitly identify data that should not be protected). Some types of IMD data are likely never protected, including water quality and quantity data, and invasive species data; but there may be exceptions based on sampling designs (such as the location of water quality data collection in cases where measurements are co-located with T&E species monitoring).

EXPERIENCE YOUR AMERICA

The National Park Service cares for special places saved by the American people so that all may experience our heritage.

Protection from Release to What Audiences

Prevent Public Release. In general, data are protected from release to the public, but are available for use by internal NPS audiences. Data sets, reports, maps, or other products that contain information that is protected from release to the public must be clearly identified so as to avoid accidental release.

Prevent Release to NPS Staff. In some cases information about protected resources is further restricted to specific individuals or job positions. In such cases it is important to document the individuals to whom access may be granted or restricted.

Methods of Protecting Data

Redaction. Protected data are removed from the data set or information product. Note that parks may wish to redact only a subset of information pertaining to a resource. For example,

- Specific location and abundance data may be withheld for T&E species, but documenting presence or abundance at a park might be deemed appropriate if doing so is unlikely to harm the resource.

Fuzzing. Location data are reported based on a buffered area within which the true location occurs. If fuzzing is to be used, data should be reported at locations on a pre-determined park-wide grid. The true observation location should not be the center of the fuzzed locations, and the grid size should be based, in part, on the ecology, behavior, and type of resource.

Park / Management Unit Centroid. All location data are transformed and reported at the location of the centroid of the park or management unit in which the observation occurred.

Delayed Release. Data are protected from release using one of the methods above for a period of time, after which the means of protecting data changes. After the “hold” expires, data may either become public, or may continue to be protected using other means. Examples include:

- Specific locations of migratory bird observations may change from being fuzzed to public after one year.
- Presence of commercially valuable species in a park may change from redacted to reported at the park centroid after a ten-year hold.

References

- National Park Service (NPS). 2010. Draft Reference Manual RM 66B: Handling Protected Information. National Park Service, Washington, DC.
- Office of Management and Budget (OMB). 2013. Open Data Policy-Managing Information as an Asset. Office of Management and Budget.
- U.S. Government Printing Office (GPO). 1996. Indian Sacred Sites. Executive Order 13007.
- U.S. Government Printing Office (GPO). 2013. Making Open and Machine Readable the New Default for Government Information. Executive Order 13642.

EXPERIENCE YOUR AMERICA

The National Park Service cares for special places saved by the American people so that all may experience our heritage.

Appendix A. Template to Document Park Decisions

The following is to be issued on park or network letterhead and signed by the park Superintendent. The table should be filled out based on information gathered in the [spreadsheet template](#).

To: [Network Program manager, park staff, file, or others as appropriate]

From: [Park Superintendent]

Subject: Handling of protected natural resource data

The Superintendent of [PARK NAME] has identified resources that are rare, threatened, endangered, or commercially valuable. Information about these resources (the specific location, abundance, presence, or absence), if released to the public or other unapproved audiences, has been determined to potentially result in harm, theft, or destruction. To ensure data are appropriately protected in accordance with park management priorities, the following rules must be followed when disseminating natural resource information collected through inventory, monitoring, or other related scientific activities.

Type of Data		Level of Protection	Rules for Dissemination
	This row included for instructions only. Delete prior to approval. Information below are provided as examples only and should be updated based on information in the spreadsheet template	<u>Legally Protected</u> . Only applicable if covered under existing statute as exempt from dissemination Or <u>Operationally Protected</u> . Data withheld from release to protect resources or site fidelity but may be subject to release upon request.	Specify any park-specific reporting & dissemination rules. This should include <i>who</i> data are restricted to/from, methods of protection to be used, and any time restrictions identified in the worksheet.
Resource Data and Information			
	Specific T&E Species locations	Legally Protected	
	Other T&E Species Locations	Legally Protected	
Location Data and Information			
	Permanent sampling locations	Operationally protected	
	Mine locations	Operationally protected	
	Cave entrances	Legally protected	
	Spring locations	Legally protected	

EXPERIENCE YOUR AMERICA

The National Park Service cares for special places saved by the American people so that all may experience our heritage.