# Job Number

N1-048-11-3

## Request for Records Disposition Authority

### To

NATIONAL ARCHIVES & RECORDS ADMINISTRATION  
8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001

### From

(Agency or establishment)  
Department of the Interior  
2 MAJOR SUBDIVISION  
Office of the Secretary  
3 MINOR SUBDIVISION

### Date Received

12/9/10

### Notification to Agency

In accordance with the provisions of 44 US C. 3303a, the disposition request, including amendments, is approved except for items that may be marked “disposition not approved or withdrawn” in column 10.

## Name of Person with Whom to Confer

Keith Holden

### Telephone Number

202-219-1563

### Date

3/9/10

### Archivist of the United States

[Signature]

### AGENCY INFORMATION

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached page(s) are not needed now for the business of this agency or will not be needed after the retention periods specified, and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies

- [ ] is not required  
- [ ] is attached, or  
- [ ] has been requested

### Date

November 30, 2010

### Signature of Agency Representative

[Signature]

### Title

Office of the Secretary Records Officer

### Item No

7

### Description of Item and Proposed Disposition

1408 General System Records  
1408 Social Media Records  
1408 1 Web Publishing  
1408 2 Social Networking and Voting  
1409 DOI Data Loss Prevention (DLP) System Data Files  
1409 1 Minor Incidents  
1409 2 Major Incidents  
1409 3 Critical Incidents

(See Attachment for Description and Disposition)

### GRS or Superseated Job Citation

N/A

### Action Taken

(See Attachment for Description and Disposition)
Additional General Electronic Records, Addendum to 1400

1409 - DOI Data Loss Prevention (DLP) System Data Files.
DOI Data Loss Prevention Systems monitor email and web traffic within DOI to ensure that personally identifiable information (PII) and other sensitive personal data is not released to unauthorized parties, and to record communications and activity that violate the department’s Acceptable Use policy (as outlined in the DOI Information Technology Security Policy Handbook). Systems may also be designed to detect and/or respond to other specific incidents, such as known malware/viruses and other computer threats.

Data files contain a record of incidents that match the above criteria, classed into three categories for PII/Accept Use each: Minor, Major, and Critical. They are tracked for statistical reporting and, in the case of Major and Critical incidents, maintained for possible use in Human Resources or Law Enforcement investigations.

Information in an incident file includes: server where the message/traffic originated; date and time of the incident, sender’s email and/or IP address, recipient’s email and/or IP address, and the message/data that was sent (subject line, attachments, body of message).

1409.1 – Minor Incidents. These incidents constitute violations that are unintentional and/or represent minimal consequences to the bureau or agency. They are tracked primarily for statistical reporting purposes only, or as an indication that employees lack proper training in the appropriate use of government equipment.

Minor PII incidents include, but are not limited to: Incidents which involve an individual sending his/her own PII information out of the DOI network. This can include family members such as spouses as well as children. Examples include, SSN’s, CCN’s, Username/Password, W2’s, New hire paperwork, etc.

Minor Acceptable Use incidents include, but are not limited to: Incidents which involve an individual using inappropriate language in a personal, non-professional conversation or environment. Incidents which show poor taste or judgment.

Disposition: Temporary: Cut off when the incident is classified/recorded. Destroy 6 months after cut-off, or when no longer needed for agency business, whichever is later. Do not preserve records longer than 1 year.

1409.2 – Major Incidents. These incidents constitute severe violations of policy and represent a danger to the security of an individual (in the case of PII) or to the bureau or office (for Acceptable Use).

Major PII incidents include, but are not limited to: Incidents which involve an individual sending several other individual's information, or an individual sending his/her government assigned credit card, username/password, etc. out of the DOI network. Examples include, Payroll worksheets, Government related username/password, Government related credit card, etc.
Major Acceptable Use incidents include, but are not limited to: Incidents which involve an individual using inappropriate language for solicitation of sexual acts, sexually/racially derogatory comments, describing activities which are deemed to be inappropriate or offensive to fellow employees, partners, contractors or the public; or adult rated/pornographic authoring.

Disposition  Temporary  Cut off when all necessary follow-up actions have been completed  Destroy 3 years after cut-off.

[Note: Though this disposition resembles that provided for in GRS 24-7, that chapter indicates that a system’s data files should be separately scheduled. As the incident files comprise this system’s data, a separate records schedule is believed necessary.]

1409.3 – Critical Incidents. These incidents constitute a severe, widespread, and/or time-sensitive compromise of information and security, constituting an immediate and dangerous risk to individuals or to the bureau/agency. Incidents may include the compromise of a computer system with employee data being maliciously sent to an outside party or parties, the description or discussion of illegal activities.

Critical incidents are escalated to the proper authorities.

Disposition  Temporary  Cut off when incident data is transferred to the investigating organization. Destroy data immediately upon successful transfer.