SF 115 Supplementary Cover Sheet

Summary:

This action establishes two new Office of the Secretary series entitled:

"1408 – Social Media Records," and "1409 – DOI Data Loss Prevention," along with their associated sub-items. Several sub-items of 1408 are included for reference and do not establish a new retention (1408.3, 1408.4, 1408.5).

Please consult with J. Peter Langsdorf for any correspondence, and with the office contacts for each item:

For Social Media (1408):
Larry Gillick, Acting Director of New Media
Larry_Gillick@ios.doi.gov
202-208-5141

For Data Loss Prevention (1409):
Darrel Garnett, CIPP
Information Assurance Engineer
Darrell_Garnett@ios.doi.gov
703-648-5564

Reason for submission:

(1) This action provides for the disposition of temporary electronic records common to several offices that have been previously unscheduled.

(2) This actions expands the General Electronic Systems Records section of the OS Records Manual, including useful guidance to employees for the handling of electronic records.

REQUEST FOR RECORDS DISPOSITION AUTHORITY		JOB NUMBER	
TO: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001		Date Received	
FROM: (Agency or establishment) Department of the Interior		NOTIFICATION TO AGENCY	
2. MAJOR SUBDIVISION Office of the Secretary		In accordance with the provisions of 44 U.S.C., 3303a, the disposition request, including amendments, is approved except for items that may be marked "disposition not approved or "withdrawn" in column 10.	
3. MINOR SUBDIVISION			
4. NAME OF PERSON WITH WHOM TO CONFER Keith Holden	4. TELEPHONE NUMBER 202-219-1563	DATE	ARCHIVIST OF THE UNITED STATES

5. 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 4 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	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
November 30, 2010	Keith A. Holden	Office of the Secretary Records Officer

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	1400 General System Records 1408 Social Media Records 1408.1 Web Publishing 1408.2 Social Networking and Voting 1408.3 File Sharing 1408.4 User Information/Accounts 1408.5 Traffic Monitoring 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)	N/A	

Additional General Electronic Records, Addendum to 1400

1408 – Social Media Records. Social Media is an umbrella term used to define the various activities integrating web technology, social interaction, and user-generated content. Through social media, individuals or collaboration of individuals, create, organize, edit, comment on, combine, and share content. These strategies can be used to connect people to the government and to share information (e.g., providing information, promoting discussion about the agency, soliciting responses from the public, recruiting personnel, and providing collaborative space). Information contained in social media platforms may still be considered federal records and are covered by the following items.

1408.1 Web Publishing. Data in these applications consists of information published by the government and does not include information from outside sources. This is most commonly limited to micro-blogging, and blogging where comments are not enabled or not considered federal records. Information that is published to social media platforms is typically duplicative of information stored elsewhere, often as a general public release.

Some examples of web publishing include Twitter, WordPress, Wikispaces, Blogger, Plurk, etc.

Disposition: Temporary. Cut off when data is published for the public. Destroy when no longer needed for agency business.

1408.2 Social Networking and Voting. Data in these applications is valued for the input and comments that are received from the public. Users are able to comment on information published by the agency, or in some cases publish material of their own for the express purpose of providing feedback or suggestions to the agency. In some cases, users may be able to vote on the information published or on associated comments from other users.

This item does not include user account information that the government has controlling access to.

Examples of social networking applications include Facebook, comment-capable blogs, LinkedIn, IdeaScale, Chaordix, etc.

Disposition: Temporary. Cut off when voting/comments are closed. Destroy when no longer needed for agency business. If action is taken based off of the comments/input, a copy of this information must be maintained as part of the development records for that project. Consult your records liaison or records officer for proper classification of these records.

1408.3 File Sharing. Data in these applications is stored for use by multiple individuals within the government for collaborative purposes. This is most often utilized during the developmental process of official agency publications or reports, receiving input from

several individuals as a draft evolves. This item also includes use of file-sharing applications to circulate photographs and videos.

In all cases, data on these platforms should be maintained outside of the application, as well. Final versions of documents should be held elsewhere, as should original copies of videos and photographs.

Examples of file sharing applications include Flickr, collaborative workspaces, YouTube, Picasa, SharePoint, etc.

Disposition: These records are considered duplicative copies of official agency records. They are non-records and may be destroyed when no longer needed for reference.

1408.4 User Information/Accounts. This data applies to information collected by the social media application for account registration/management in an application that is operated or managed by the agency. It may include user name, email address, passwords, and other information about an individual, varying by the social media platform. There is a strong potential for PII in these applications.

This information must be accessible and controllable by the agency for it to be applicable with this records schedule. Social media applications in which the agency participates as a user (e.g. Facebook, Twitter) do not apply, as the agency has no role in managing account registration.

Disposition: These records are considered the same as **1404.3 User Identification Files (Routine Systems)** and should be treated accordingly.

1408.5 Traffic Monitoring. Data in these applications is used to track browsing activity and sequence of traffic. IP addresses or "cookies" can be analyzed to show browsing history and where individuals arrive at and browse from DOI sites.

Google analytics is an example of an application supplying this data.

Disposition: This data is considered part of what is maintained with **1403 Management and Maintenance Files** for electronic systems and should be handled accordingly.

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.