



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the [DOI PIA Guide](#) for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: OS DiscoverText

Bureau/Office: Office of the Chief Information Officer

Date: May 25, 2017

Point of Contact:

Name: Teri Barnett

Title: Departmental Privacy Officer

Email: Teri_Barnett@ios.doi.gov

Phone: (202) 208-1605

Address: 1849 C Street NW, Mail Stop 7112 MIB, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

- Yes, information is collected from or maintained on
 - Members of the general public
 - Federal personnel and/or Federal contractors
 - Volunteers
 - All

No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

DiscoverText is a text analytic tool developed by Texifter to provide text and public comment analysis capabilities for Federal agencies including the Department of the Interior (DOI). DiscoverText provides the ability to filter and organize comments received from members of the public in response to notices published by DOI in the *Federal Register*. Public comments are submitted electronically through the Regulations.gov website on documents with an open comment period such as Proposed Rules or



Federal Register notices, and are extracted for analysis using the DiscoverText tool. The DOI Office of the Secretary uses DiscoverText to gain valuable insight into data received from the public, and conduct better and more accurate analysis of public comments submitted on Regulations.gov.

Public comments analyzed through DiscoverText are obtained from the Federal Docket Management System (FDMS) managed by the Environmental Protection Agency (EPA), which is a government-wide online public docket and comment system that is used by Federal agencies to support the rulemaking process. Only the public comments published on Regulations.gov will be analyzed through DiscoverText. Regulations.gov is a centralized Federal government website that facilitates public access and participation in the Federal regulatory process. Members of the public may search for and submit comments on regulations such as a proposed rule, final rule, or *Federal Register* notice through Regulations.gov.

Federal agencies are responsible for managing their own records in FDMS, and DOI has access to all the comments submitted in response to DOI notices, including any personally identifiable information (PII) that may be included in a comment or attachment submitted by the public. PII is generally limited to name and contact information voluntarily provided by members of the public and organizations submitting comments on rulemaking or notices published by DOI for the purpose of clarifying comments or facilitating the processing of a comment.

Reliance on the use of this PIA to analyze the public comments, received through Regulations.gov, using DiscoverText is constrained to only that information which is already made publicly available through Regulations.gov.

C. What is the legal authority?

5 U.S.C. 301; Section 206(d) of the E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch 36); 5 U.S.C. 553, Administrative Procedures Act; Clinger-Cohen Act of 1986

D. Why is this PIA being completed or modified?

- New Information System
- New Electronic Collection
- Existing Information System under Periodic Review
- Merging of Systems
- Significantly Modified Information System
- Conversion from Paper to Electronic Records
- Retiring or Decommissioning a System
- Other: *Describe*

E. Is this information system registered in CSAM?

- Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
- No



F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII (Yes/No)	Describe If Yes, provide a description.
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

Yes: *List Privacy Act SORN Identifier(s)*

Records are obtained from the Federal Docket Management System and are covered by the EPA/GOVT-2, Federal Docket Management System (FDMS) system of records notice, 78 FR 60868, October 2, 2013, which may be viewed at <https://www.gpo.gov/fdsys/pkg/FR-2013-10-02/html/2013-24120.htm>.

No

H. Does this information system or electronic collection require an OMB Control Number?

Yes: *Describe*

No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

Name

Personal Email Address

Mailing/Home Address

Other: *Specify the PII collected.*

Records in the system may contain name, address, city, state, country, zip code, email, phone number and fax number of any individual, organization or entity who voluntarily choose to include that information in their submission when submitting comments through Regulations.gov in response to DOI rulemaking and *Federal Register* notices. Individuals may also choose to include other personal information in the body of comments submitted.



B. What is the source for the PII collected? Indicate all that apply.

- Individual
- Federal agency
- Tribal agency
- Local agency
- DOI records
- Third party source
- State agency
- Other: *Describe*

C. How will the information be collected? Indicate all that apply.

- Paper Format
- Email
- Face-to-Face Contact
- Web site
- Fax
- Telephone Interview
- Information Shared Between Systems
- Other: *Describe*

Public comments may be submitted electronically via the Regulations.gov website, through postal mail, and in some cases may also be submitted via email to DOI. Correspondence received through postal mail is scanned and uploaded to FDMS. The public comments extracted from FDMS for sorting and review in DiscoverText are limited to the comments displayed on Regulations.gov.

D. What is the intended use of the PII collected?

DOI considers public comments when modifying a proposed or final rule, or when soliciting opinions on a program initiative, scientific study, respective agency guidance document or proposed standard to improve or develop a program. Any PII voluntarily provided in comments submitted by members of the public or organizations may be used to seek clarification on comments submitted or to facilitate processing of comments during the review process.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

- Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

DOI may share records internally with authorized personnel to organize or analyze, or for consideration when modifying a proposed or final rule, or when soliciting opinions on a program initiative, scientific study, respective agency guidance document or proposed standard to improve or develop a program. Any PII voluntarily provided in comments submitted by members of the public or organizations may be



used to seek clarification on comments submitted or to facilitate processing of comments during the review process.

Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

DOI may share records with its bureaus and offices and authorized personnel to organize, analyze, or for consideration when modifying a proposed or final rule, or when soliciting opinions on a program initiative, scientific study, respective agency guidance document or proposed standard to improve or develop a program. Any PII voluntarily provided in comments submitted by members of the public or organizations may be used to seek clarification on comments submitted or to facilitate processing of comments during the review process.

Other Federal Agencies: *Describe the federal agency and how the data will be used.*

DOI may share records with other agencies or persons as authorized, consistent with the purpose of the activity and the uses permitted under the Privacy Act and the EPA/GOVT-2, Federal Docket Management System (FDMS) system of records notice, 78 FR 60868, October 2, 2013, which may be viewed at <https://www.gpo.gov/fdsys/pkg/FR-2013-10-02/html/2013-24120.htm>.

Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

DOI may share records with Tribal, state or local agencies as authorized, consistent with the purpose of the activity and the uses permitted under the Privacy Act and the EPA/GOVT-2, Federal Docket Management System (FDMS) system of records notice, 78 FR 60868, October 2, 2013, which may be viewed at <https://www.gpo.gov/fdsys/pkg/FR-2013-10-02/html/2013-24120.htm>.

Contractor: *Describe the contractor and how the data will be used.*

DOI may share records with its contractors who support the management or review of public comments available to the public on the [regulations.gov](http://www.regulations.gov) Web site.

Other Third Party Sources: *Describe the third party source and how the data will be used.*

Comments sorted in DiscoverText are also included in the public docket available to any persons or organizations at www.regulations.gov, including any personal or contact information provided. Individuals are directed to not submit information they consider to be sensitive. Comments on www.regulations.gov may be viewed, searched and exported by any member of the public or organization. DOI may share records with third parties as authorized and consistent with the purpose of the activity and the uses permitted under the Privacy Act and the EPA/GOVT-2, Federal Docket Management System (FDMS) system of records notice, 78 FR 60868, October 2, 2013, which may be viewed at <https://www.gpo.gov/fdsys/pkg/FR-2013-10-02/html/2013-24120.htm>.



F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Submitting comments in response to DOI rulemaking or *Federal Register* notices is completely voluntary. The Regulations.gov website does not collect personal data from an individual unless they voluntarily choose to provide it. Individual members of the public voluntarily submitting comments have control over the inclusion of personal information provided when commenting on a notice. Individuals are provided notice on the Regulations.gov website and in published *Federal Register* notices that comments received may be viewed by the public, and individuals may choose not to submit any information they do not want to provide.

No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement: *Describe each applicable format.*

Privacy Notice: *Describe each applicable format.*

The Regulations.gov website contains a Privacy and Security Notice that provides information to visitors on how their information is handled, retained and shared, requirements of the Privacy Act, and links to the governing EPA/GOVT-2 FDMS system of records notice and privacy impact assessment, which may be viewed at <https://www.regulations.gov/privacyNotice>.

Notice is also provided through *Federal Register* publications, which inform individuals that their submitted comments, including any personal or contact information voluntarily provided, will be published.

Other: *Describe each applicable format.*

Individuals are provided notice through the publication of this PIA and the EPA FDMS PIA, which may be viewed at https://www.epa.gov/sites/production/files/2014-03/documents/erulemaking-pia_0.pdf.

None



H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Comments may be searchable by keyword searches and other data elements for the purpose of sorting, grouping and organizing comments to facilitate review and analyze public comments.

I. Will reports be produced on individuals?

- Yes: *What will be the use of these reports? Who will have access to them?*
 No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Comments submitted by members of the public or organizations in response to rulemaking or notices published in the *Federal Register* are not verified for accuracy.

B. How will data be checked for completeness?

Comments submitted by members of the public or organizations in response to rulemaking or notices published in the *Federal Register* are not checked for completeness.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

All public comments are voluntarily submitted via Regulations.gov website, mail, or email within the comment period specified in published *Federal Register* documents, and are presumed to be current at the time of submission.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Retention periods may vary depending on the program, or notice and purpose of the publication. Records of public comments are retained and disposed of in accordance with applicable DOI records schedules, or General Records Schedule (GRS) approved by the National Archives and Records Administration (NARA) for each type of record based on the subject or function and records series. Because of this, it is important for programs to review the specific subject matter with their records officer to ensure the appropriate disposition authority is assigned.

The majority of public comments related to *Federal Register* notices fall into one of the three following schedule items within the DOI Departmental Records Schedule 3 - Policy Records (DAA-0048-2013-0008):



- 0009 - Regulatory Development and Support - 7 Years
- 0010 - Final Regulations - Permanent, transferred to NARA after 15 years
- 0008 - Public Affairs Records - Permanent, transferred to NARA after 15 years

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Records of public comments are disposed of in accordance with the applicable DOI records retention schedules and policy based on the program area and agency needs. When approved for destruction, paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with NARA guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the “information lifecycle” (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a minimal risk to individual privacy for use of DiscoverText to analyze public comments. Public comments submitted through Regulations.gov are available to the public and may be viewed and searched by any person or organization. Members of the public voluntarily submit comments on *Federal Register* rulemaking activities or notices, and have control over the amount of personal information provided through their comments. Notice is provided on the Regulations.gov website and in published *Federal Register* notices that comments received may be viewed by the public, and individuals may choose not to submit any information they do not want to provide.

Members of the public may search for and submit comments on regulations such as a proposed rule, final rule, or *Federal Register* notice through Regulations.gov, which is a centralized Federal government website managed by the EPA that facilitates public access and participation in the Federal regulatory process. The public has access to all the comments published on Regulations.gov, including any PII that may be included in a comment. PII is generally limited to name and contact information provided by members of the public and organizations submitting comments on rulemaking or notices published by DOI for the purpose of clarifying a comment or facilitating the processing of a comment during the review process.

The public comments used by the Office of the Secretary in DiscoverText is limited to the publically available information submitted through Regulations.gov, which may also be exported into a spreadsheet or database by any member of the public or organization. The export contains the docket title, document type and ID, posted date, received date, comment start date, comment due date, and status. Any public user may be able to view each comment by clicking on the link provided in the export spreadsheet.

DiscoverText is a tool developed by Texifter, a company with a government-wide contract under the General Services Administration Schedule. DiscoverText uses publically available data imported by DOI from FDMS to perform advanced keyword searches, metadata filters, duplicate detection, topic modeling, annotations, and other functions in support of DOI rulemaking activities or when soliciting



opinions on a program initiative, scientific study, respective agency guidance document or proposed standard to improve or develop a program. All DOI employees and contractors must complete privacy, security and records management awareness training on an annual basis and sign the DOI Rules of Behavior prior to accessing DOI information and information systems.

DiscoverText is hosted in the FedRAMP authorized Microsoft Azure Commercial Cloud Platform as a Service (PaaS), which provides for a secure, open and flexible cloud computing platform. Azure provides physical and environmental controls for operating systems including secure configuration, patching, vulnerability scanning, audit logging, built-in network load balancing and resiliency to hardware failure.

Because use of this PIA to analyze public comments, received through Regulations.gov, using DiscoverText is constrained to only that information which is already made publicly available through Regulations.gov, a determination of low risk has been made with respect to the use of DiscoverText and all publically available data/information extracted from Regulations.gov that is imported into, and created within, DiscoverText, in association with reviews conducted that adhere to these constraints. Consequently, minimum security controls are necessary to ensure that:

- access is granted to only those individuals that are authorized and is controlled with username and password, and
- system and data/information integrity are maintained through the period in which reviews are being conducted.

The system security objectives for Confidentiality, Integrity and Availability are based on the following rationale/justification:

Confidentiality - the information will be constrained to that which is already publicly available and has already been released on Regulations.gov.

Integrity - controls associated with ensuring data/information accuracy rely on the primary authoritative source from which the already publicly available information is sourced (i.e., Regulations.gov and FDMS).

Availability - controls associated with ensuring data/information availability rely on the primary authoritative source from which the already publicly available information is sourced (i.e., Regulations.gov and FDMS) to provide access to the original data in the event it becomes inaccessible through DiscoverText.

Section 4. PIA Risk Review

- A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**



Yes: *Explanation*

The use of data is relevant and necessary for DOI to filter, organize and analyze comments received from members of the public in response to notices published in the *Federal Register* when soliciting opinions on a program initiative, scientific study, respective agency guidance document or proposed standard, to improve or develop a program, gain valuable insight, and conduct better and more accurate analysis of public comments.

No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

No

C. Will the new data be placed in the individual's record?

Yes: *Explanation*

No

D. Can the system make determinations about individuals that would not be possible without the new data?

Yes: *Explanation*

No

E. How will the new data be verified for relevance and accuracy?

Not applicable, the system does not create new data about individuals.

F. Are the data or the processes being consolidated?

Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

No, data or processes are not being consolidated.



G. Who will have access to data in the system or electronic collection? Indicate all that apply.

- Users
- Contractors
- Developers
- System Administrator
- Other: *Describe*

Data in the system is an extract of the public comments posted on Regulations.gov, which are available to the public. Public access to comments submitted via Regulations.gov requires no login to search, view, and post comments, and any member of the public or organization can view, search and export the same public comments on Regulations.gov.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access to the system is restricted to authorized DOI officials and contractors on a need-to-know basis in order to perform official duties.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

- Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act and Privacy Training clauses were included in the contract.

- No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

- Yes. *Explanation*
- No

K. Will this system provide the capability to identify, locate and monitor individuals?

- Yes. *Explanation*
- No

The system sorts and organizes text to facilitate review and use of data, and was not designed to identify, locate and monitor individuals. However, there are audit features that track authorized user access and activities within the system to ensure system security and efficiency.



L. What kinds of information are collected as a function of the monitoring of individuals?

The system utilizes audit features that capture username, and date and time of access.

M. What controls will be used to prevent unauthorized monitoring?

The system uses access controls and audit logs to prevent unauthorized monitoring. Staff with access also complete security and privacy training, and sign the DOI Rules of Behavior.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- Security Guards
- Key Guards
- Locked File Cabinets
- Secured Facility
- Closed Circuit Television
- Cipher Locks
- Identification Badges
- Safes
- Combination Locks
- Locked Offices
- Other. *Describe*

(2) Technical Controls. Indicate all that apply.

- Password
- Firewall
- Encryption
- User Identification
- Biometrics
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)
- Public Key Infrastructure (PKI) Certificates
- Personal Identity Verification (PIV) Card
- Other. *Describe*

Microsoft Azure provides for maintenance controls over the operating systems.

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Backups Secured Off-site



- Rules of Behavior
- Role-Based Training
- Regular Monitoring of Users' Security Practices
- Methods to Ensure Only Authorized Personnel Have Access to PII
- Encryption of Backups Containing Sensitive Data
- Mandatory Security, Privacy and Records Management Training
- Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Chief Technology Officer, Office of the Chief Information serves as the DiscoverText Information System Owner and the official responsible for oversight and management of security controls and the protection of agency information processed and stored in DiscoverText. The Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in DiscoverText, in consultation with the Departmental Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The DiscoverText Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, and ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The DiscoverText Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with Federal policy and established DOI procedures.