






CYBERSECURITY (FISSA)

DOI is committed to protecting the sensitive information of our organization, partners, and employees. We have multiple security control layers in place to help protect our network and data. However, **YOU** play a critical role in keeping our important data secure. Even small actions you take will make a big difference to everyone.

CYBERSECURITY: WHAT TO DO AND WHAT NOT TO DO

- ✓ Immediately report lost or stolen DOI IT equipment to your supervisor and [local help desk](#).
- ✓ Always keep your DOI Access Card in a shielded card holder when not in use.
- ✓ [Connect to Pulse Secure](#) (VPN) when you're using a public WiFi connection.
- ✓ Lock areas containing sensitive data or equipment when unattended.
- ✓ Backup important DOI data often through approved sources, such as Microsoft OneDrive or network H: Drive.
- ✓ Carefully review emails to ensure they are legitimate before responding, opening attachments, or clicking links.
- ✗ Never use personal devices to access or store DOI data unless you are using the [POE Secure Container](#).
- ✗ Do not use the same passwords for your DOI and personal accounts.
- ✗ Never download or install unauthorized or personal applications on your DOI computer.
- ✗ Avoid giving your GPS location in real time or posting personal information online.
- ✗ Never leave your computer unlocked when not in use or unattended. To lock your computer, press Ctrl+Alt+Delete and select **Lock**.
- ✗ Do not travel internationally with your DOI IT equipment without approval. Learn more on the [International Travel Site](#).

TIPS FOR SPOTTING SUSPICIOUS EMAILS

-  **Review sender and recipient email addresses.**
Pay close attention to emails that contain [EXTERNAL] in the subject. Review the sender, to:, cc:, and bcc: lines to make sure there isn't anything phishy.
-  **Check for spelling and grammar errors.**
It's not uncommon for phishing emails to have poor grammar or spelling. Be on the lookout!
-  **Watch out for emails with links and attachments.**
Only click links or open email attachments from sources you trust and if you're expecting a file. If you aren't expecting a file, confirm with the sender before opening.
-  **Don't simply click!**
Hover your mouse pointer over the link to help determine where the link takes you prior to clicking on it. If a URL shortener is used, such as bit.ly or goo.gl, double check that the email is legitimate.
-  **Be cautious of emails asking for personal information or passwords.**
Never give your DOI passwords or PIN to anyone and be careful about providing personal information. If you're already logged in to a DOI system, you should not be prompted to input your credentials or personal information in an application.

Immediately contact [your local help desk](#) if you receive a suspicious email. Notify DOI-CIRC at DOICIRC@ios.doi.gov and your supervisor if you suspect a cybersecurity or privacy breach. For further guidance review [DOI Rules of Behavior](#), take [training in DOI Talent](#), or contact your [local help desk](#).

PRIVACY

It is important that you understand your responsibility to protect privacy and adhere to privacy policies. [The Privacy Act of 1974](#) controls how Federal agencies collect, use, and share information, and requires agencies to provide notice to individuals on these activities and how they can access or correct their records. These requirements are outlined in DOI Privacy Act regulations at [43 CFR Part 2, Subpart K](#), [383 DM 1-13](#) and [OMB privacy policy](#).

The **DOI Senior Agency Official for Privacy (SAOP)** has oversight responsibility for the DOI Privacy Program and establishes policy and procedures to manage privacy risk in agency activities in accordance with Federal laws, regulations, and policy. The **DOI Privacy Officer** and bureau/office **Associate Privacy Officers (APOs)** support the SAOP and work with responsible officials to ensure privacy legal and policy requirements are implemented. Visit the [DOI Privacy Portal](#) for DOI privacy policies and resources and the [DOI Privacy Contacts](#) page for a list of APOs.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information. Some PII may be non-sensitive such as information found on a business card, official email address, or work-related phone number that generally does not require special handling. Sensitive PII requires handling and must be protected against unauthorized access, use or disclosure at all times, including during storage, transmission, telework, and travel, to prevent harm, embarrassment, or unfairness to an individual. You can [safeguard sensitive PII](#) by limiting access to PII to authorized personnel and physically securing PII in locked drawers, cabinets, or rooms, even while teleworking.

EXAMPLES OF SENSITIVE PII



Personal Identifiers such as passport, Tribal ID, driver's license, and Social Security numbers



Date of birth, mother's maiden name



Personal email addresses, physical addresses, and phone numbers



Medical history, biometrics, nationality, criminal history



Credit card number, bank account information



Consider sensitive context, such as a list of employees with security clearance or poor performance evaluations

SOCIAL SECURITY NUMBERS (SSNs)

The collection and use of SSNs are authorized only when necessary to meet a legal or regulatory requirement. Where use of SSNs is authorized, program officials should truncate, mask or redact SSNs to protect privacy. The use of SSNs is evaluated by APOs during the privacy compliance process to ensure business practices, systems and forms meet Federal requirements in accordance with [OMB Circular A-130](#) and [OCIO Directive 2007-005](#).

REPORTING A PRIVACY BREACH

If you become aware of a suspected or confirmed breach of PII, **IMMEDIATELY** notify DOI-CIRC at DOICIRC@ios.doi.gov or (703) 648-5655 or your help desk, as well as your supervisor. This applies to breaches in any format: paper, oral, or electronic. Be prepared to provide details on the breach, such as date, time, location, and a description. Do not delay reporting - timely reporting allows DOI to take immediate action to contain the breach and mitigate any potential harm to affected individuals.

CONTRACTORS

Federal privacy requirements also apply to contractors and grant recipients who collect, process, store, maintain or dispose of PII, or operate a Federal information system, on behalf of DOI. Contracts must include terms and conditions for privacy controls and requirements such as safeguards, training, disposal, and authorized use of PII. Responsible officials must also ensure breach reporting and remediation requirements are included in acquisition and grant activities. See the [DOI Privacy Portal](#) for privacy clauses for contracts and contact your APO for questions on privacy requirements.

PRIVACY – WHAT TO DO

- ✓ Encrypt sensitive PII during storage and transmission, including use of authorized portable media and email attachments.
- ✓ Protect SSNs by removing them from forms, reports, emails, databases, or truncating, masking or redacting SSNs where feasible.
- ✓ Mail PII via mailing or courier service that has tracking capability.

PRIVACY – WHAT NOT TO DO

- ✗ DON'T use personal equipment or portable storage devices, such as thumb drives and external hard drives, to store PII.
- ✗ DON'T use personal email accounts to transmit PII. PII may only be transmitted via official DOI accounts to authorized recipients.
- ✗ DON'T collect PII from employees or the public without first consulting your [APO](#).

THE PRIVACY ACT OF 1974

The Privacy Act applies to records about individuals that are maintained in a system of records, which is a group of records about individuals for which information is retrieved by name or some other unique identifier assigned to the individual.

- A **System of Records Notice (SORN)** must be published in the *Federal Register* that describes the purpose of a system of records, authority, categories of individuals, types of records, and how the records will be maintained and used by the Federal agency. DOI SORNs are posted on the [DOI SORN website](#).
- Privacy Act records may not be disclosed to third parties without the individual's consent unless there is a Privacy Act exception or a routine use in the published SORN that authorizes the disclosure. Disclosures may be written, oral, or electronic. The [DI-3710 Disclosure Accounting Form](#) is used to account for disclosures to third parties.
- Contact your APO before collecting information from individuals or creating a system of records, or if you receive a Privacy Act request or complaint.

The Privacy Act contains **civil and criminal penalties** for failing to meet requirements, including a misdemeanor charge and a fine up to \$5,000 if an agency employee knowingly releases a record improperly from a Privacy Act system; willfully maintains a Privacy Act system without publishing a SORN in the *Federal Register*; or if a person knowingly and willfully requests or obtains any record concerning an individual under false pretenses. Civil actions may also be brought against the agency when a Privacy Act violation occurs that results in harm to the individual. Employees may also be subject to disciplinary action such as written reprimand, suspension, and removal, as described in [370 DM 752](#), Discipline and Adverse Actions.

PRIVACY ACT STATEMENT

A **Privacy Act Statement (PAS)** must be provided when PII is collected directly from individuals for a Privacy Act system and applies to any collections conducted through a web or paper form, phone interview, or in person. The PAS must describe:

- Legal authority for the collection
- Purpose(s) for which PII is collected
- Intended disclosures or routine uses
- Citation to the applicable SORN
- Whether providing the information is voluntary or mandatory, and any consequences for not providing information

Note: A Privacy Notice must be provided where a PAS is not required but members of the public could provide PII through an online interface and should include a description of the organization's practices with respect to the collection and use of PII.

Privacy Impact Assessments (PIAs) are conducted pursuant to Section 208 of the [E-Government Act of 2002](#) to evaluate privacy risk when developing and operating systems, programs, and projects that maintain PII. PIAs are also conducted on use of third-party websites, social media applications, and mobile applications developed by or on behalf of DOI. The **Privacy Threshold Analysis (PTA)** helps APOs identify PIA and other privacy compliance requirements for the collection, maintenance, storage, use, processing, sharing or disposal of PII. See the DOI PIA Guide and PTA Guide on the [DOI Privacy Portal](#) and contact your APO for questions on PIA and PTA requirements.

For more information visit [DOI Privacy Program site](#), contact your [Associate Privacy Officer](#), or take [training in DOI Talent](#).

RECORDS MANAGEMENT

UNDERSTANDING A RECORD

[Records](#) are all recorded information, regardless of form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business. Records Management within the Federal Government is mandated by the Federal Records Act ([44 U.S.C. Chapters 29-33](#)).

LEARN ABOUT ARCHIVING YOUR RECORDS

- Many of your emails are also records. DOI's email Enterprise Records and Document Management System (eERDMS) captures all your emails, so there's no need to print out to archive or digitize them for archival purposes.
- Use the [Quick Guide to using the Departmental Records Schedule](#) to help determine how to manage your Administrative and Policy Records. All other records are covered by bureau specific schedules and policies, so consult with your [bureau Records Officer](#) with any questions.

LEGAL HOLDS

- The U.S. judicial system obligates the Department to preserve certain information that is related to active or foreseeable litigation. These preservation obligations, which are referred to as "legal holds" or "litigation holds," supersede all records schedules, and any failure to comply with them could negatively impact the Department.
- As litigation arises, attorneys in the Office of the Solicitor will contact you via email if you are likely to have information that must be preserved. It is very important that you carefully follow the instructions in these notices and that you respond to them promptly. If you are subject to a legal hold, you must retain unmodified versions of all hardcopy or electronic materials that contain the information identified in the hold notice until you have been released from the hold by the Office of the Solicitor.
- DOI employees and contractors, and their Records and IT support staff, can consult the [Legal Hold Dashboard](#) which lists all the Department's active legal holds and provides the contact information of the SOL attorney managing each hold.

RECORDS MANAGEMENT DO'S AND DON'TS

✓ **DO** preserve both electronic and required paper Federal Records appropriately.

✓ **DO** ensure any documents removed from DOI while teleworking or traveling are returned to the office.

✓ **DO** separate your files by Federal Records, Non-Records, and Personal Papers and organize by subject and date.

✓ **DO** forward any DOI-related emails from your personal email to your .gov account, as required by law (P.L. 113-187).

✓ **DO** use your DOI email account rather than text messages or chats to discuss official government business when possible.

✓ **DO** ensure you transition all your Federal Records to your successor or supervisor, when leaving the bureau or office.

✗ **DON'T** create government social media accounts without [proper approval](#).

✗ **DON'T** dispose of any documents if you are unsure if they are a Federal record. Contact your [records officer](#) for clarification.

✗ **DON'T** print email since they are archived automatically.

✗ **DON'T** commingle personal files, including documents, texts, emails, and photos, on your DOI computer or equipment.

✗ **DON'T** destroy records under a preservation hold. Contact the [Solicitor's Office](#) with questions.

✗ **DON'T** destroy any temporary and permanent records without proper approval. Contact your [records officer](#) for assistance.

RECORDS MANAGEMENT

EXAMPLES OF RECORDS



EMAIL



TEXT MESSAGES



MAPS



PICTURES



DOCUMENTS

CAN YOU SPOT THE RECORD?

A video distributed to all employees that contains the Secretary's holiday message?

This is not a record for all employees and can be deleted when no longer needed. The video is a record for the Office of Communications who is responsible for the creation, editing, and distribution of the video.

The original documented rule that governs offshore oil drilling safety requirements that has just been replaced by a new final rule?

This **is** a record. Even though the rule has been made obsolete, there is still a preservation requirement according to the Federal Records Act. A rule is a form of policy and must be maintained PERMANENTLY and transferred to the National Archives according to the approved records schedule.

A meeting invitation that you receive in email and accept?

This **is** a record. Technically this invitation is a record but is considered transitory in nature and can be deleted when you act on the invitation. Your electronic calendar in BisonConnect is considered the official record of your calendar and is what should be maintained for longer term record keeping purposes.

The SF-50 form you received as a result of a recent pay raise?

This is not a record. Your copy of the SF-50 is considered a personal paper and you can retain or dispose of that copy as necessary. The SF-50 maintained in the electronic Official Personnel Folder (eOPF) system is maintained as the official record copy.

A text message sent to a coworker making plans for lunch?

This is not a record. While records can be in the form of text messages, this is considered a personal message since it is not about the conducting of government business.

The binder you received at a training class that Human Resources conducted about supervisory best practices?

Your copy of the binder is not a record. It's considered a reference copy which you can retain or dispose of based on your own individual needs. Even though the content of the binder includes instructions on how to conduct government business, Human Resources is responsible for maintaining the official record copy of the training materials.

A book you sign out from the DOI Library about history of the Department?

This is not a record. Library and museum material preserved solely for reference or exhibition purposes are specifically excluded from the definition of a Federal Record. If the book was written by a component office of DOI, that office would have been responsible to retain the original text as a federal record.

An email received on your personal email account requesting updates to guidance recently issued by your office?

This **is** a record. However, you should only use your personal email account to conduct government business when necessary. According to Section 10 of the Amendments to the Federal Records Act ([44 U.S.C. § 2911](#)), you need to forward a complete copy of the correspondence to your official DOI email account to ensure proper preservation. Any intentional violation of this requirement can result in disciplinary action. The Office of the Chief Information Officer also released [OCIO Directive 2015-003](#) on May 21, 2015 documenting this requirement.

NEED MORE INFORMATION?

If you are ever in doubt as to whether something is a Federal Record, retain it until you can get clarification from your [bureau Records Officer](#) or their staff. You may search using keywords "records management" in DOI Talent for a listing of training you may take.

SECTION 508 COMPLIANCE

It's important that information is accessible to everyone, including those with disabilities. Here at DOI, we provide training in compliance with the [Section 508 of the Rehabilitation Act of 1973](#), [375 Departmental Manual 8](#) and [U.S. Access Board Accessibility Standards](#) to help ensure that **all** Information and Communication Technology (ICT) developed or procured is accessible.

The mission of the [Departmental Section 508 Program](#) is to:

- Ensure that DOI employees and members of the public with disabilities have access to government information and government information technology.
- Improve the accessibility of DOI's Information and Communication Technology (ICT) such as software, hardware, websites, audio/visual media, telecommunications, electronic documents, and other IT products and services in an effective and efficient manner.

TIPS FOR CREATING ACCESSIBLE CONTENT



Images, drawings, and other graphic must have alternative text which provides a description of the graphic or image.



Use tables for presenting data, not for changing the visual layout of the page. Be sure to include a heading row rather than placing data in the first row.



Use headings to organize your document. Headings divide your document into sections, making it easier for people to navigate to a section.



Check your documents, spreadsheets, presentations and PDFs to ensure they meet Section 508 requirements. [Learn how to create accessible files.](#)



Ensure you have a high color contrast between the text and background. When in doubt, use the [Color Contrast Checker](#).



Do not rely on color alone to communicate meaning (for example, red text for important content). You may use color with text or symbol to convey meaning.



Videos must have audio description and closed captioning. View our [Standard Operating Procedure](#) and guidance for creating [Accessible Audio and Visual Content](#).



Additional resources include: [Guide to Accessible Web Design and Development](#), [Adobe Acrobat Accessibility Training](#), and [Microsoft Office Accessibility Center](#).

PROGRAM SERVICES

Policy: Develops Section 508 policy and procedures consistent with Federal policy and industry best practices.

Consultations: Provides consultations on implementation requirements, tools, and resources and IT procurement solicitations to ensure accessibility standards are incorporated.

Training and Outreach: Provides training and materials to increase awareness of Section 508 policies and procedures, and how to make technology accessible.

Testing Activities: Conducts Section 508 hands-on testing of technology, website, web/mobile applications, and electronic documents to reduce the risk of unknowingly implementing inaccessible technology. Guidance is provided for making documents accessible for individuals with disabilities.

NEED MORE INFO?

Consult your bureau/office [Section 508 coordinator](#), or take training in DOI Talent for creating accessible [Word and PDF documents](#), and [Excel spreadsheets](#). Additional [training](#) is available to help you understand and comply with the law!

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

WHAT IS THE CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM?

The Controlled Unclassified Information (CUI) Program standardizes the way all sensitive information must be safeguarded, marked, and handled according to a laws, regulations, or government-wide policy in the Executive Branch of the Federal Government.

KEEP CUI SECURE

CUI must be physically and electronically secured at all times. Using a controlled environment that ensures only an “Authorized Holder” with a lawful government purpose can access. Controlled environments include physical and electronic barriers such as sealed envelopes, file cabinets, locked doors, dedicated network drives, file folders, and internal sites.

PROPER CUI MARKING

CUI markings are required on every page for all documents and all media where CUI is present.

- *CUI Basic* indicates that a category has no specified safeguarding and/or handling requirements articulated in its authorities; and thus, defaults to 32 CFR, Part 2002 standards and is marked as “CONTROLLED” or optionally as “CUI.”
- *CUI Specified* indicates that a category has specified safeguarding and/or handling requirements articulated in its authorities; and thus, follow additional safeguarding and/or handling requirements and is marked using the CUI marking syntax appropriately (CUI//<CUI category list>//DISSEM-<control>).

EXAMPLE OF A PROPERLY MARKED CUI BASIC DOCUMENT

CONTROLLED

U.S. Department of Interior

May 3, 2018

MEMORANDUM

From: Harry Bison
Subject: Example of proper CUI marking

It is important to properly mark documents that contain Controlled Unclassified Information.

We have resources available to help you.

EXAMPLE OF A PROPERLY MARKED CUI SPECIFIED DOCUMENT

CUI//<CUI categories>//DISSEM-<Control>

U.S. Department of Interior

May 3, 2018

MEMORANDUM

From: Harry Bison
Subject: Example of proper CUI marking

It is important to properly mark documents that contain Controlled Unclassified Information.

We have resources available to help you.

Any unclassified sensitive information marked with other designations such as Sensitive but Unclassified (SBU) or For Official Use Only (FOUO) must be replaced with proper CUI markings.

RESOURCES

- [Federal CUI Registry](#), which includes the CUI category list
- [CUI Marking Handbook](#)
- [CUI Notice 2018-02: Notice on CUI Compliant Basic Training](#)

For further guidance, take [training in DOI Talent](#) or reach out to your bureau/office [CUI Coordinator](#).