



Natural Resources Conservation Service  
6013 Lakeside Blvd.  
Indianapolis, Indiana 46278

---

July 18, 2007

INDIANA BULLETIN NO. IN120-7-2

SUBJECT: ADS – USE AND MAINTENANCE OF PRIVATE AND SENSITIVE  
INFORMATION

Purpose: To inform employees of actions needed to comply with National Bulletin 170-7-2.

Expiration Date: September 30, 2007

**Action Required By: July 26, 2007**

**Background.** Recently, there have been several instances within USDA where private or sensitive information has been unintentionally shared with an outside entity. This occurred through stolen laptops or the harvesting of data from websites. Under the Privacy Act of 1974, the Federal Government must ensure the security and confidentiality of records which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual. This includes information that permits the identity of an individual to be determined, personal financial information, and business proprietary information such as production information or farm records.

**Explanation.** In accordance with National Bulletin 170-7-2, states were given three tasks. By July 31, 2007, the State Conservationist must:

- 1) Review all Web site content to ensure that no private or sensitive information is posted. If private or sensitive information is found, remove it immediately. **This item will be handled by Pam Davidson of the Public Affairs Staff.**
- 2) Review all software applications and other electronic files, such as MS Word documents, MS Excel spreadsheets, and MS Access or other databases and electronic forms. If sensitive or private information is found, remove it unless transactions cannot be processed without it. **This item will be completed by the state office key staff members and area conservationists. State office staffs will be responsible for software applications and other databases and electronic forms developed for state use by that staff. Area conservationists will be responsible for software applications, other electronic files such as MS Word documents, MS Excel spreadsheets, and MS Access or other databases and electronic forms developed and used in their area.**

DIST: 0

- 3) Review all paper forms, data collections, and reporting forms or reports such as personnel, financial, program forms, purchase orders, contracts, and employee and customer lists. If private or sensitive information is found, remove it if not needed. **This item will be completed by all employees in the state.**

Examples of Private Data: Social Security numbers, tax I.D. numbers, employee NFC ID, account numbers, farm numbers, tract numbers.

Examples of Sensitive Data: name, address, or other geographic indicators, e-mail address, phone number, race, gender, ethnicity, disability, birth date.

Private and sensitive information must be requested and used only when the transaction cannot be completed without it; it must be entered for that one transaction and not stored for any future use unless it is absolutely necessary. When private and sensitive information must be stored, it must be secured. If this information is on paper, it must be secured in a locked file cabinet or drawer where only authorized employees have access to it. If your office does not have access to locking file cabinets for storing private or sensitive information, then please submit your procurement request to your Supervisor for replacement file cabinets with locks. If this information is in electronic form, the computer system, including laptops, tablets, and desktops; USB drives; external hard drives; and similar devices, whether they are encrypted or not, must be secured in a way that prevents the information from being lost or stolen. If the electronic files cannot be secured, the information must not be stored on that computer. The information may be best secured in an access-controlled, shared-drive folder on a physically secure server that is accessed over the network.

All private and sensitive information to be kept in either hard copy or electronic form must be reviewed and documented (inventoried) on the spreadsheet per the National Bulletin. NHQ has inventoried any information that is included in any national information system, such as WebTCAS, ProTracts, NFC databases, PRS, and the National Conservation Planning (NCP) database, and for standard agency forms, contracts, etc.

The Indiana State Office will inventory any information that is common to all offices within the state such as cooperator case files, supervisory files, Outlook Contact Lists, customer databases, contractor databases, Continuity of Operations Plans, Field Office Emergency Operations Plans, easement databases, program contract databases, employee Official Personnel File, Training Needs Inventories, statewide GIS layers, Planning Tool databases, vendor files, payment files, correspondence files, mailing lists, NRCS-SD forms, and other files, forms, reports, and databases kept on the H: or S: drives.

If there is private and sensitive information other than those that will be included in the national or statewide inventory that you need to maintain on your office's server or computers, then we will have to include an entry on our inventory of private and sensitive information. Submit these to Elana Cass, State Freedom of Information Act/Privacy Act Officer, with a description of any information that you will need to maintain whether it be hard copy or electronic form.

**Anyone who saves private or sensitive information to their laptop or desktop C: drive needs to especially be aware that he or she is a prime candidate for violating the Privacy Act.** This information is not backed up and can be accessed if someone steals or gets into your computer. It is recommended that employees keep this kind of information on the shared drive only. If you need this information to be transportable, burn it to a DVD or other information storage device and take it with you. Store these devices in a secure location, as you are responsible for the information you maintain.

When faxing any document with private or sensitive information on it, ensure that the recipient is waiting on the other side for the document. When emailing information that contains such information, it is best to put the information into a document, attach the file to an email, and then password protect the attachment. Instructions on how to do this will be sent out under a separate bulletin.

Look for the following during your review:

1. A word document (side record) that is on a computer system or on paper that lists employee name and SSN and is used for completing travel vouchers. Delete hard or soft copies of old travel vouchers that still show employees SSN.
2. A list of retired employees with their e-mail addresses and phone numbers.
3. An old form that has a place for the SSN, and where the SSN is no longer needed. For example, review your old leave slips or compensatory time/overtime request forms to ensure that you destroy them if they still have the SSN on them.
4. A paper list of customer information that employees carry with them to the field and may be misplaced or stolen.
5. A list of landowners or contractors with their tax ID number or account information.

Field offices spreadsheets should be sent to the area office for the inventory to be summarized on one spreadsheet. Area offices should then submit their spreadsheet to Brian Eaton, Contract Specialist at the state office. State office staffs should submit their spreadsheets to Brian Eaton. All reviews and inventory spreadsheets must be completed and sent to the state office no later than **July 26, 2007**. For questions regarding the inventory process, please call Elana Cass at the state office.

/s/

JANE E. HARDISTY  
State Conservationist

Attachment