Print Form

INFORMATION TECHNOLOGY AND SECURITY IN NRCS

Section Overview: Upon completion of this section you will become familiar with the basics of NRCS policy privacy and security issues as they relate to granting access to employees and non-employees, use of computers, etc.

USDA and NRCS have several established regulations and policies to ensure comprehensive protections are in place to safeguard all information technology resources. These apply to all USDA organizational elements and their employees, other Federal agencies, State agencies, contractors, and sub-contractors who are involved in development of systems, obtaining, transmitting, using, and processing USDA information, data, on behalf of USDA. They also apply to USDA computers operated on behalf of the USDA by State and local government or other private organizations to accomplish a USDA function.

Several steps are involved in granting access to employees and non-employees. Initially, individuals receive a letter from the Human Resources (usually) staff specifying the requirements and documentation required to grant computer and records access. That documentation includes: SF-85 Background Investigation (recently changed to an electronic process); SF-87 Fingerprint Chart, OF-306 Declaration for Federal Employment, OF-612 Application form or a resume (from non-employees), Computer Security and Privacy Basics test, and a Computer User Security Agreement. All of these must be completed and accepted as complete by the HR staff before an employee or affiliate may enter on duty.

FAQ on SF-85 Background Investigation Fact Sheet

With recent emphasis within NRCS and USDA on personnel and information systems security, considerable attention has been paid to background investigation for employees, partners, contractors, and other affiliates. The requirement for background investigations is the result of three separate but related Federal and Departmental directives: Employment Suitability (5 CFR 731), Cyber Security (DM 3500) and Homeland Security Presidential Directive 12 (HSPD 12). NRCS has committed to comply with each mandate. Agency security measures also are taken in accordance with the Federal Information Security Management Act (FISMA) of 2002. FISMA directs agencies to determine levels of information security to protect information and information systems and to apply methods to reduce risks to those systems.

Who must have a background investigation?

All employees, partners, contractors, and affiliates working in NRCS or USDA facilities for six months or more, and/or requiring access to the USDA network for 30 days or more, must have a minimum level National Agency Check and Inquiry (NACI).

Is there other authority, other than those mentioned above, that authorizes investigations for NRCS partners, contractors, and other affiliates?

Yes, Code of Federal Regulations 5 CFR 736.101 – Personnel Investigations (http://www.access.gpo.gov/nara/cfr/waisidx_02/5cfr731_02.html)

If an employee, partner, contractor or affiliate already has an investigation through a state agency, can NRCS use that instead of requesting new forms for an OPM investigation?

USDA policy states that OPM is the only valid source for background investigations. This means that background investigations performed by state or private agencies are not valid for these purposes.

Do the background investigation policies govern part-time partner, contractor, or other affiliate personnel?

Yes. Any person anticipated to have access to federal facilities for six months and/or IT resources for more than 30 days will be required to submit paperwork for a background investigation. This requirement applies equally to full time, part time, and seasonal access.

Who pays for background investigations and what is the process for payment?

The mechanics of the process involves OPM billing the NRCS budget allowance holder for the cost of the background investigation for employees, partners, contractors, and other affiliates.

NRCS budget allowance holders (state conservationists) should enter into an agreement in advance with their non-federal partners to collect the funds for background investigations. As each is completed, OPM bills NRCS. NRCS must pay the bill. States may collect the money in advance from their non-federal partners or after the investigation is completed. The NRCS contracting officer or agreement specialist should be consulted on how to write the agreement. For money already collected, the NRCS budget and finance officer should be consulted on how to process those funds into the proper account.

For example, for volunteers the NRCS budget allowance holder may elect to assume the burden of paying for its volunteers or request reimbursement through the volunteer agreement.

In most cases, conservation districts are expected to incur the cost of background investigations for their employees. The applicable NRCS budget allowance holder should enter into a reimbursable agreement for these partner employees.

Are background investigations necessary for students and scholars?

Yes. Students and scholars connecting to the USDA network must have background investigations. Student background investigations are the financial responsibility of the employing NRCS budget allowance holder. Human resource management specialists should work with the student liaison to ensure timely submission of paperwork. Payment of investigations for scholars, while they are scholars, is the responsibility of NRCS national headquarters.

Why am I asked to submit two sets of fingerprints when the Office of Personnel Management (OPM) requires only one set of fingerprints?

For the majority of NRCS employees, partners, contractors, and other affiliates whose paperwork is submitted directly to OPM, only one set is required. The two-set requirement only applies to those positions and individuals that require a higher level background investigation. However, most offices request two cards to better ensure that one will be acceptable quality for OPM. Fingerprint cards can be ordered via fax (724-794-0012) from Michelle Pennington/OPM. Please indicate the form number, quantity, and mailing address.

Are non-federal employees required to complete the OF 306, Declaration for Federal Employment?

Yes, but only a few answers are required. Complete items 1, 2, 8 through 13, 16 and 17a.

Questions should be directed to your state's Human Resources Specialist.

Questions to ask yourself:

1. What information has your state provided to managers on what is involved in hiring employees, bringing volunteers and other partners on board?

2. Do you keep one of the many releases regarding procedures for lost passwords, where to go for assistance with specific issues, etc. on hand?

PERSONALLY IDENTIFIABLE INFORMATION (PII)

OMB Memorandum **M-07-16**, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," requires agencies to implement a breach notification policy to protect personally identifiable information in possession of the government. Additionally, the memorandum discusses new and existing security and privacy requirements to reduce the risks related to data breach and mitigate the effects when a breach occurs.

<u>USDA Examples of Personally Identifiable Information (PII)</u>

PII is information that can be used to uniquely identify an individual. The following are some examples of data which when combined with an individual's name constitute PII. For a decision on other data elements not indicated on this list, you should contact the USDA Chief Privacy Officer.

- Social Security number
- Place of Birth
- Date of birth
- Mother's maiden name
- Biometric record (such as fingerprint, iris scan, DNA)
- Medical history information (including medical conditions and metric information, e.g. weight, height, blood pressure)
- Criminal history
- Employment information to include ratings, disciplinary actions, performance elements and standards
- Financial information
- Credit card numbers
- Bank account numbers
- Security clearance history or related information (Not including actual clearances held).

WHAT ISN'T PII: The identification of PII requires an analysis of material in context. The following examples, taken alone, would generally not constitute PII. However, combined examples, or examples included in specific databases or other record systems may constitute PII.

- An individual's name
- EIN/TIN as a business identifier
- Phone numbers (Work, Home, Cell)
- Street addresses (Work and personal)
- Email addresses (Work and personal)
- Digital pictures
- Resumes, unless they include an SSN
- Employee present and past position titles and occupational series
- Employee present and past grades (and salary privacy)
- Security clearances held
- Written biographies (like the ones used in pamphlets of speakers)
- Academic information (credentials, areas of study)

HSPD-12 AND LINC PASS

Homeland Security Policy Directive 12 directs that all federal agencies will implement a two-factor identify card system for all employee, contractors, partners, etc. Two-factor means that two sets of data are needed to use the system: identifying name and a password. Every individual who accesses NRCS computer equipment (and eventually buildings) will need a "LincPass" card to enter public buildings or do their computer work. LincPass cards contain a person's picture, agency, a card expiration date, and whether or not the person is an Emergency Response Official. The chip in the card also stores a PIN (personal identification number), fingerprint data, and digital certificates for authentication and encryption. These cards will require a computer that either has a built-in card reader or an external reader attached through a USB port. The final implementation date for NRCS is targeted for October 21, 2009.

Summary: You should now be familiar with the basics of NRCS policy privacy and security issues as they relate to granting access to employees and non-employees, use of computers, etc.