



United States Department of the Interior

OFFICE OF THE SECRETARY

Washington, DC 20240

FEB 8 2013

Memorandum

To: Heads of Bureaus and Offices

Through: Rhea Suh 
Assistant Secretary – Policy, Management and Budget

Andrew Jackson 
Deputy Assistant Secretary – Technology, Information and Business Services

From: Bernard J. Mazer 
Chief Information Officer

Subject: Annual End-User Federal Information Systems Security Awareness, Privacy and Records Management Training

The purpose of this memorandum is to re-affirm ongoing mandatory information security, records management, and privacy training requirements for the Department of the Interior (DOI). Federal law and regulations require that all Federal employees, and other users of DOI information systems, receive annual information security awareness, privacy, and records management training. Federal employees and other users must also acknowledge a system Rules of Behavior as presented in the course.¹ This training requirement must be met before new users can gain initial access to federal information and/or information systems and must be renewed annually for existing users to maintain continued access. Note that an equivalent process to meet this requirement for Short-Term Emergency Response Personnel is described in the Office of the Chief Information Officer's Directive 2011-005.²

To enforce this mandatory training requirement, Bureaus and Offices must disable network accounts for existing users who do not complete the Federal Information Systems Security Awareness, Privacy and Records Management Training (FISSA+) course thirty (30) days after the due date (e.g., July 31st or a date established by the Bureau or Office before July 31st).

¹ Rules of Behavior requirement comes from Title III of the E Government Act of 2002, the Privacy Act of 1974, the Federal Records Act and 5 C.F.R. § 930.301.

²OCIO Directive 2011-005, *Granting Limited/Controlled Access to DOI Information Systems for Short-term Emergency Response Personnel*, issued April 14, 2011, to Assistant Directors for Information Resources.

The attached FISSA+ Training Instructional Guide provides additional details regarding implementation and reporting for the Fiscal Year (FY) 2013 FISSA+ training activity. The accompanying Security Training Reporting Template should be utilized by Bureau and Office staff to support the training reporting activities defined in the Instructional Guide.

If you have any questions concerning this memorandum, please contact me at [Bernard Mazer@ios.doi.gov](mailto:Bernard_Mazer@ios.doi.gov) or 202-208-6194. Staff may contact Mr. Lance Kelson, Information Assurance Division, IT Security Training Program Manager at lance_kelson@ios.doi.gov or 202-208-5064 or they may contact their respective Bureau/Office DOI Learn Managers/Data Stewards. Technical issues related to DOI Learn or the training course can be directed to DOI's Learn Help Desk via email at doilearn@sumtotalsystems.com or (866) 466-1998.

Attachment 1: Federal Information Systems Security Awareness, Privacy and Records Management Training Instructional Guide

Attachment 2: Security Training Reporting Template

cc: PMB Deputy Assistant Secretaries
Assistant Directors for Information Resources
Bureau Chief Information Security Officers
DOI Learn Managers/Data Stewards
DOI Human Resources Officers
Interior Training Directors Council

Federal Information Systems Security Awareness, Privacy and Records Management Training Instructional Guide

This instructional guide provides detailed information to support Federal Information Systems Security Awareness, Privacy and Record's Management Training (FISSA+). The Department of the Interior (DOI) Learn Managers assigned to each Bureau/Office, in consultation with their respective Bureau Chief Information Security Officer (BCISO), are jointly responsible for:

- Overall coordination and execution of their respective pilot testing of each new version of the FISSA+ course and annual information security awareness training implementation plan;
- Developing and implementing ongoing communication plans and informing employees and contractors of the training initiatives for their Bureau/Office;
- Providing employees, contractors, and other users of DOI's information systems with detailed instructions on the use of the Learning Management System (i.e., DOI Learn);
- Issuing log-on credentials and instructions to employees, contractors, and other users;
- Issuing course registration and activation instructions to employees, contractors, and other users;
- Providing completion status to Bureau/Office security and training officials so they can enforce user compliance to these training requirements; and
- Ensuring associated IT infrastructure environments and end-user systems are configured in accordance with the established DOI Learn minimum workstation configuration requirements.¹

Systems at some user locations may be inadequate to support the training online. To facilitate access to training outlets with better performance, DOI Learn can be accessed through the public internet, outside of the DOI Network, (e.g., at home) at <http://www.doi.gov/doilearn/index.cfm>. In addition, DOI Learn Managers/Data Stewards can provide a downloadable website or paper version of the course to employees and other new staff experiencing difficulties with the online course or without Internet access.

All BCISOs or their designees will submit a report via e-mail to the Information Assurance Division at DOI_IT_Security_Training@ios.doi.gov, no later than the end of January, containing the following information:

- a) The total number of federal employees required to take the combined annual information security awareness, privacy, and records management training; and
- b) The total number of contractors and other users of DOI's information systems required to take this training.

¹<http://www.doi.gov/doilearn!upload/Workstation-Requirements.pdf>.

These totals will be used as the Bureau/Office baseline in reporting for the remainder of each fiscal year and for annual Federal Information Security Management Act reporting to the Department of Homeland Security.

Bureau and Office baseline totals for employees and contractors required to complete annual training should only be changed to reflect employees that are no longer required to take annual awareness training due to job reassignment, termination, or transfers to other agencies or Bureaus/Offices during the applicable reporting period. Any additions to the Bureau/Office workforce will be included in the total for the next fiscal year reporting.

Bureaus and Offices are required to report on training compliance status to the Information Assurance Division, via e-mail to [DOI IT Security Training@ios.doi.gov](mailto:DOI_IT_Security_Training@ios.doi.gov), during the following intervals each fiscal year:

- February -May: Monthly reports due on the 1st day of each month.
- June- July: Bi-weekly reports due on the 1st and 15th day of each month.
- August 1st: Final FISSA+ completion totals due.

Each compliance status report should use the accompanying Security Training Reporting Template and include the following information:

- a) Total number of employees, contractors, and other users of DOI's information systems required to take this awareness training, as previously declared;
- b) Total number of employees, contractors, and other users of DOI's information systems that have completed the required training as of the date of the report; and
- c) Bureau and Office compliance percentage as of the date of the report.

Bureaus and Offices must disable network accounts for those that have not completed the FISSA+ course thirty (30) days after the due date as an enforcement mechanism to ensure compliance with this annual training requirement.