Security Training

All users of federal information systems must receive security awareness training before accessing IT resources. This ensures that users understand their responsibilities to protect the data and information systems they use. The term "all users" is inclusive of employees, contractors, students, guest researchers, visitors and others who need access to federal IT resources. OPM also requires that individuals with significant IT responsibilities receive training appropriate for their roles and responsibilities.

Information Security Training and Awareness

Contract staff with access to NIH computer systems must meet a number of computer security training requirements. Initially, contractors must complete the NIH Computer Security Awareness Training at http://irtsectraining.nih.gov prior to beginning work on a contract. Following that, there are requirements for annual computer security awareness refresher courses that must be completed on a schedule announced by NIH each year. Contract personnel designated by the government as having “significant IT security responsibilities” will also be required to take security training related to their role.

Training requirements are as follows:

- Information Security Awareness - Full course is required for all users before accessing NIH/NCI IT systems.
- Information Security Awareness Refresher - Annual requirement for all users.
- Role Based Training - Required every year for individuals designated as having “Significant IT Security Responsibilities” within NCI.

Consult the HHS CISO Memorandum on Role-Based Training (RBT) of Personnel with Significant Security Responsibilities which provides guidance on what roles should be included. This document lists mandatory roles; however for others, it also give you the latitude to make local decisions about whether a person’s security responsibilities are significant enough to warrant this designation. It’s always helpful to review the list with your CIO.

- Executives - All SES (Senior Executive Service). These are usually IC directors, scientific directors, executive officers etc.
- Chief Information Officers and ISSOs and their support staff (e.g., alternate ISSOs).
- Stewards of systems/information assets during development and operation - System Owners, Data Steward, Data Owners, IT Program or Project Managers.
- Information Technology Auditors - Personnel engaged in the auditing of HHS or OPDIV systems or networks.
- Administrators - network, LAN, system and database administrators.

Below are some courses provided on the NIH Security Training Portal that can be used to fulfill Role Based Training Requirements.

Trainings for System Owners and Project Managers

- NCI SDLC Integration Roadmap
- FISMA in Acquisition Training (NIH only) (2008)

Trainings for System Developers and Software Engineers

- NIH Web Application Security Training Video (2013)
- Introduction to Web Application Security for Java Developers (Day 1 Course)
- Introduction to Web Application Security for Java Developers (Day 2 Course)

Trainings for General Users

- IRT Security and Privacy Training and Page
- US-CERT’s Security Tips Page(link is external)
- Identifying Hoaxes and Urban Legends(link is external) (A useful security tip from US-CERT on why hoaxes and legends are a security problem and how to help identify them)
- Recognizing Fake Antivirus(link is external) (A useful security tip from US-CERT on how to recognize and avoid fake AV)
- Avoiding Social Engineering and Phishing Attacks(link is external) (A useful tip from US-CERT on avoiding social engineering and phishing attacks)