



United States Department of the Interior

OFFICE OF THE SECRETARY

Washington, DC 20240

Memorandum

To: Heads of Bureaus and Offices
Bureau and Office Deputy Directors
Bureau and Office Associate Chief Information Officers
Bureau and Office Associate Chief Information Security Officers
Bureau and Office Department Privacy Officers
Bureau and Office Capital Planners

From: Deborah (June) Hartley
Acting Chief Information Officer
Office of the Chief Information Officer
JENNIFER ACKERMAN
Jennifer Ackerman
Acting Chief Human Capital Officer
Office of Policy, Management, and Budget

Digitally signed by JENNIFER ACKERMAN
Date: 2022.08.03 13:06:00 -04'00'

Subject: Mandatory Annual Information Management and Technology Awareness and Role-Based Training Directive

Purpose

This directive provides actions and guidance that support the U.S. Department of the Interior (DOI, Department) annual Information Management and Technology (IMT) Awareness and Role-Based Training requirements in accordance with the below listed references. Bureaus and offices must ensure that users meet these requirements within established timelines and on an ongoing basis. **Department users will lose most or all network access if they do not complete their annual training requirements.** Data accuracy in DOI Talent and the related systems is essential to ensure appropriate training assignments and accurate reporting.

Authorities and References

1. [Federal Cybersecurity Workforce Assessment Act of 2015](#); pages 735–737
2. [Personnel Bulletin 17-06: Revised National Initiative for Cybersecurity Education \(NICE\) Coding Structure](#)
3. [5 CFR § 930.301, Information systems security awareness training program](#)
4. [Office of Management and Budget \(OMB\) Circular A-130, Managing Information as a Strategic Resource](#)
5. [370 DM 752: Discipline and Adverse Actions](#)
6. [375 DM 19: Information Security Program](#)

Background

Annual privacy and security training courses ensure employees and other users of DOI information assets have access to new and emerging best practices in protecting DOI information systems and data. Without this awareness, the Department faces an increased risk of its ability to accomplish mission objectives. All employees and other users with access to federal information or information systems, including detailees, contractors, grantees, volunteers, interns, and other affiliates must complete annual IMT Awareness Training. Individuals with significant privacy and security responsibilities must complete role-based training. These training practices help ensure that individuals take appropriate actions when using DOI systems and networks.

Annual IMT Awareness Training equips all DOI network users with practical information to protect DOI data. The following annual training programs are currently administered in DOI Talent:

- A. IMT Awareness Training - required for all DOI employees and network users, includes:
 - Cybersecurity - Federal Information Systems Security Awareness (FISSA)
 - Privacy Awareness
 - Records Management
 - Section 508 Compliance
 - Controlled Unclassified Information (CUI)
 - Paperwork Reduction Act
- B. Information Systems Security Rules of Behavior Acknowledgement - required for all DOI network users.
- C. Role-Based Privacy Training (RBPT) - Users with significant privacy responsibilities must complete RBPT and acknowledge their responsibility to protect personally identifiable information (PII) and comply with federal privacy law and policy during their official duties. These RBPT requirements apply to federal employees, detailees, contractors, grantees, volunteers, interns, and other users who handle PII and are in accordance with OMB Circular A-130, National Institute of Standards and Technology (NIST) guidance, and the DOI Security and Privacy Control Standards. See the [DOI RBPT Guide](#) for more information on RBPT requirements.
- D. Role-Based Security Training (RBST) - Users with Significant Information Security Responsibilities (SISR) must adhere to DOI RBST requirements in accordance with 5 CFR § 930.301 (2004), the Federal Information Security Modernization Act of 2014, OMB Circular A-130, NIST guidance, and DOI Security and Privacy Control Standards. The Office of the Chief Information Officer (OCIO) will update DOI Information Technology (IT) Security Training Policies and Procedures in Fiscal Year (FY) 2022.

In addition to the IMT Awareness course in DOI Talent, a more comprehensive [streaming version](#) of the IMT Awareness Training is available for Department-wide usage for new staff who do not have access to DOI Talent. The OCIO will update the Rules of Behavior in FY22. A streaming version of the DOI Incident Response (IR) Overview is also available for new staff with RBPT and RBST requirements.

Effective Date

The requirements outlined in this directive are effective immediately and remain in effect until further notice. The Chief Information Officer (CIO) may change the certification window and content identified in this directive based on evolving requirements to include those identified through ongoing Information Management and Technology Leadership Team (IMTLT) collaboration and discussions.

Certification Process

The Department deploys IMT Awareness Training and Role-Based Trainings using a certification approach in the DOI Talent system, which provides the following benefits:

- A. Facilitates initial certification and re-certification paths
- B. Tracks users' progress
- C. Automates training reminder emails
- D. Reduces network burden on DOI Talent
- E. Satisfies stakeholder requests for routine recurring training
- F. Reinforces training as a user responsibility
- G. Customizes users' annual training schedule based on initial IMT Awareness training completion

Users must complete annual certifications, which are valid for one year. Users may complete recertification 90 days before their due date or 9 months after the last certification. The certification window may be adjusted in the future based on the needs of the IMT Training Programs. DOI Talent sends automated email reminders to each user and the user's supervisor to ensure timely completion of training.

Roles and Responsibilities

- A. Office of the Chief Information Officer
 - Evaluate training and requirements annually
 - Ensure consistency across the DOI for annual training and reporting
 - Work with Human Resources (HR) and Bureau and Office Associate Chief Information Officers (ACIOs) to track training completion, ensure suspension of network access for non-compliance, update procedures, and ensure data integrity for reporting
- B. Bureau and Office Associate Chief Information Officers
 - Ensure staff complete all annual mandatory training in DOI Talent by their certification due date
 - Implement comprehensive procedures and processes for annual training requirements that:
 - Involve key stakeholders including, but not limited to, IT Security, Privacy, Data Stewards, Human Capital, and Personnel Security
 - Utilize DOI Talent for reporting annual training compliance
 - Maintain accurate data in DOI Talent and related systems that update DOI Talent, such as the Federal Personnel and Payroll System (FPPS) and DOI Access

- Ensure the timely onboarding and offboarding procedures for contractors, volunteers, and others accessing DOI networks
- Establish procedures for disabling non-compliant users' network access no later than 14 days after the individual's certification expires or their extension date as outlined in applicable guidance
- Include identifying extenuating circumstances and granting extensions for those who temporarily cannot access the DOI network that must:
 - Not extend beyond 60 days
 - Be documented and maintained as part of the bureaus' and offices' training compliance and completion record, which must be available to the OCIO and auditors upon request
- Provide procedures and processes to the Chief Information Security Officer (CISO) within 30 days of the issuance of this directive and when requested
- Review and update procedures and processes annually to ensure compliance with federal laws and DOI, bureau, and office policies and procedures
- Report on non-compliance quarterly to the OCIO Chief of Staff no later than 15 days after the end of the quarter
- Review mandatory training certification status reports provided by DOI Talent Data Stewards at least monthly
- Work with HR and the OCIO to track training completion, ensure suspension of network access for non-compliance, update procedures, and ensure data integrity for reporting
- Include a certifications statement regarding mandatory FISMA training requirements in the Annual Assurance Statement on Information Technology Controls

C. Human Resources, Bureau and Office Human Capital, and Information Technology Operations

- Maintain accurate data in the systems of record that update DOI Talent, such as FPPS and DOIAccess
- Work with the OCIO and ACIOs to track training completion, ensure suspension of network access for non-compliance, update procedures, and ensure data integrity for reporting

D. Supervisors, Contract Officers, and Contract Officer Representatives

- Monitor email for expiring certification notifications for direct reports and verify that annual training requirements are complete by their due date
- Claim direct reports, including employees and contractors, in DOI Talent
- Ensure direct reports have the correct RBST group, RBPT status, and Cybersecurity Codes in their DOI Talent profiles
- Contact HR to correct RBST, RBPT, and Cybersecurity Codes in FPPS for federal employees

E. Network Users

- Must complete annual training requirements in DOI Talent by the due date

- Must ensure their supervisor has claimed them in DOI Talent and that their DOI Talent profile data is accurate for RBST Group, RBPT status, and Cybersecurity codes
- Must contact their supervisor to correct any missing or inaccurate data

If you have any questions regarding this policy, please contact Lance Kelson at lance_kelson@ios.doi.gov.

cc: Bureau and Office DOI Talent Leads
Bureau and Office Associate Privacy Officers
Cybersecurity Leadership Team
Bureau and Office Data Stewards
DOI Talent Program Managers
Active Directory Personnel
OCIO Resources Management Division-Human Capital Branch
DOI Supervisors
DOI Contract Officers and Contract Officer Representatives