THIS PRODUCT WAS PUBLISHED BY THE NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE & THE NATIONAL OPERATIONS SECURITY PROGRAM (NOP) OFFICE

ADVISORY:
National Operations Security Program Training Standards

NOP PMO-ADVISORY-2022-001
DATE: July 21, 2022

Purpose

The basic requirements for operations security program personnel and general workforce awareness training are contained in National Security Presidential memorandum-28 (NSPM-28) "The National Operations Security (OPSEC) Program" dated January 13, 2021.

NSPM-28 designates the NCSC as the National OPSEC Program Office (NOP) and assigns responsibility to develop and issue minimum training and awareness standards under NSPM-28, 6 (c) (ii).

Therefore, the NOP Office is issuing this Advisory to provide information on training and awareness minimum standards and recommended resources.

OPSEC TRAINING STANDARDS

Agency heads shall ensure personnel assigned to the OPSEC program are fully trained in:

1. The fundamentals of operations security, security, counterintelligence awareness, protection of controlled unclassified information, unauthorized disclosures, insider threat, and cybersecurity to include applicable legal issues.
2. Risk management principles.
3. Developing and maintaining an OPSEC program.
4. Integrating OPSEC into the planning, execution, and assessments of their organizations' operations, processes, and activities.

Agency heads shall:

1. Provide OPSEC awareness training, synchronous or asynchronous, to all employees within 30 days of initial employment or entry on duty and annually thereafter. Training shall address the current risk environment and shall include, at a minimum, the following topics:

    a. The importance of protecting sensitive information, including unclassified information, which could provide an adversary an avenue to collect your organization's critical information.
    b. Methodologies adversaries use to collect information.
    c. Organizational requirements to protect information, in and outside of the work environment, which could allow an adversary to target you or your organization.
    d. How to recognize and report attempts to elicit information or other suspicious contacts.

2. Verify all employees have completed initial and annual recurring training for employees to include documentation.

TRAINING RESOURCES

Although each agency has unique needs, the following resources may assist agencies that do not have existing training to meet the minimum standards. These courses are potential resources, not requirements.

Operations Security Program Personnel

1. The fundamentals of operations security, security, counterintelligence awareness, protection of controlled unclassified information, unauthorized disclosures, insider threat, and cybersecurity to include applicable legal issues.

    - OPSEC Awareness for Military Members, DOD Employees and Contractors GS130.16, CDSE, e-learning, 25 min
    - Counterintelligence Awareness and Security Brief CI112.16, CDSE, e-learning, 30 min
    - CUI Program Overview, NARA, video, 12 min
    - CUI Briefing, NARA, video, 60 min
    - Insider Threat Awareness INT101.16, CDSE, e-learning, 60 min

- Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI) IF130.16, CDSE, e-learning, 60 min
- Cybersecurity Awareness CS130.16, CDSE, e-learning, 30 min
- Unauthorized Disclosures: Prevention and Reporting, NARA, video, 9 min
- Freedom of Information Act, NARA, video, 7 min

2. Developing and maintaining an OPSEC program.

- OPSEC Analysis OPSE-2380, NOP, virtual instructor led, two days
- OPSEC Program Management OPSE 2390, NOP, virtual instructor led, one day

3. Risk management principles.

- Introduction to Risk Management GS150.06, CDSE, e-learning, 30 min
- Enterprise Threat Management Workshop, ETD, in-person, one day

4. Implementing OPSEC into the planning, execution, and assessments of their organizations' operations, processes, and activities.

- Critical Thinking for Insider Threat Analysts INT250.16, CDSE, e-learning, 90 min
- OPSEC Contract Requirements CLC 107, DAU, e-learning, 60 min
- OPSEC Program Management OPSE 2390, NOP, virtual instructor led, one day

Organizational Workforce

The OPSEC for All scripted briefing available from the NOP Office website may be used to satisfy this requirement. Additional options that address the required awareness training elements are recommended below:

- The importance of protecting sensitive information, including unclassified information that could provide an adversary an avenue to collect your organization's critical information.
  OPSEC Awareness for Military Members, DOD Employees and Contractors
  GS130.16, CDSE, e-learning, 25 min

- Methodologies adversaries use to collect information.
  Counterintelligence Awareness and Security Brief
  CI112.16, CDSE, e-learning, 30 min
  Surveillance Awareness: What You Can Do
  IS-914, FEMA, e-learning, 60 min
- Organizational requirements to protect information, in and outside of the work environment, which could allow an adversary to target you or your organization.
- How to recognize and report attempts to elicit information or other suspicious contacts.
  Counterintelligence Awareness and Security Brief
  CI112.16, CDSE, e-learning, 30 min
  Cyber OPSEC Awareness, IOSS, e-learning, 60 min

LINKS TO RESOURCES

- Center for Development of Security Excellence (CDSE) Home (cdse.edu)
- Defense Acquisition University (DAU) DAU Home
- Federal Emergency Management Agency (FEMA) FEMA - Emergency Management Institute (EMI) | National Preparedness Directorate National Training and Education Division
- National Archives & Records Administration (NARA) CUI Training | National Archives
- National Counterintelligence & Security Center (NCSC) National OPSEC Program (NOP) Operations Security (dni.gov)

The NOP Office recognizes that some departments and agencies may possess legacy training programs that already comply with these standards. In this case, departments and agencies may choose to use an existing program, or switch to one of the recommended resources identified above.

National OPSEC Program POC: If you have any questions regarding this Advisory or the training resources, please contact the National OPSEC Program Office at ETD_Assistance@dni.gov or on JWICS at ETD_Assistance.wma@cia.ic.gov.