DCSA INDUSTRY TRENDS: COMMON ADMINISTRATIVE FINDINGS AND VULNERABILITIES

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

National Industrial Security Program Mission Performance Division
Industrial Security Headquarters

Agenda and Purpose

PURPOSE

To provide most common instances of administrative findings and vulnerabilities.

AGENDA

- ⇨ Trends: Administrative Findings
- ⇨ Trends: Vulnerabilities
- ⇨ Most Common Instances of Non-Compliance
- ⇨ Resources and Training
- ⇨ Questions and Feedback

Trends: Administrative Findings

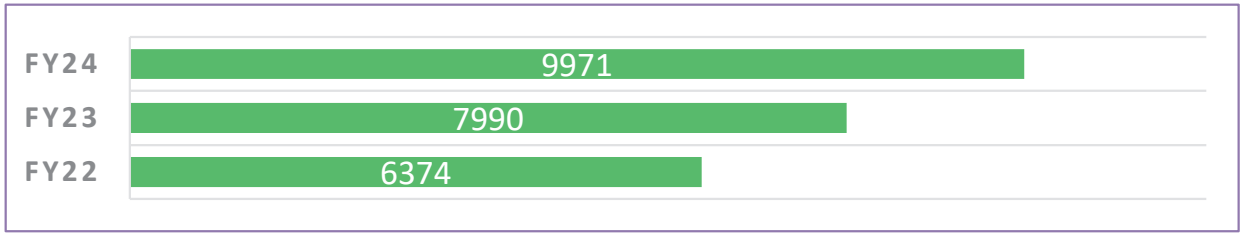
ADMINISTRATIVE FINDING

Non-compliance with the NISPOM that based on collected evidence and implemented supplementary controls could not be exploited to gain unauthorized access to classified information.

Trends: Most Common Instances

- NISPOM 117.7(h): Contractor Reviews
- NISPOM 117.8(c): Reporting Requirements
- NISPOM 117.10(a): DISS Management
- NISPOM 117.12(g): Insider Threat Training
- NISPOM 117.18(b): Information Systems Security Program

Metrics: Fiscal Year Comparison



* DCSA refined the NISPOM non-compliance severity categories in September 2021. The refined definitions directly associates risk to classified material with higher severity levels. As such, the number of identified administrative findings increased year over year and the number of vulnerabilities (shown on the next slide) decreased. This indicates the workforce has appropriately phased-in the refined definitions.

Trends: Vulnerabilities

VULNERABILITY

Non-compliance with the NISPOM that based on collected evidence and implemented supplementary controls could be exploited to gain unauthorized access to classified information.

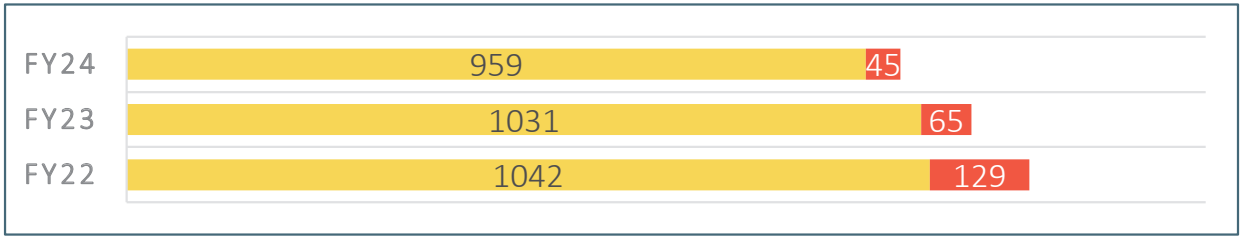
Serious: Classified information was in danger of loss or compromise.

Critical: Classified information was lost or compromised, or loss or compromise was about to occur at any moment.

Trends: Most Common Instances

- NISPOM 117.8(c): Reporting Requirements
- NISPOM 117.8(d): Reports of Loss, Compromise, or Suspected Compromise
- NISPOM 117.10(a): DISS Management
- NISPOM 117.15(a): General Safeguarding
- NISPOM 117.18(b): Information Systems Security Program

Metrics: Fiscal Year Comparison



* DCSA refined the NISPOM non-compliance severity categories in September 2021. The refined definitions directly associates risk to classified material with higher severity levels. As such, the number of identified vulnerabilities decreased year over year and the number of administrative findings (shown on the previous slide) increased. This indicates the workforce has appropriately phased-in the refined definitions.

Most Common Instances of Non-Compliance

NISPOM 117.7(h)(2): CONTRACTOR SECURITY REVIEWS

Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.

Common Issues:

- Not conducting a self-inspection annually (i.e., once a calendar year)
- Not reviewing classified information system elements every 12 months
- Not including all industrial security program elements within the self-inspection process
- SMO not certifying to DCSA, in writing, that a self-inspection has been conducted on an annual basis

Resources:

- eLearning Course: NISP Self-Inspection IS130.16
- FSO Toolkit: Self-Inspections Module
- NISP Tools and Resources: Self-Inspection Handbook for Contractors
- Security Review and Rating Process website

Most Common Instances of Non-Compliance

NISPOM 117.8(c): REPORTING REQUIREMENTS TO DCSA

Contractors will report certain events that may have an effect on the status of a facility's or employee's eligibility for access to classified information; indicate an insider threat to classified information or to employees with access to classified information; and effect proper safeguarding of classified information.

Common Issues:

- Not reporting changes in ownership, operating name, address, information previously submitted for KMP, or material changes concerning FOCI through NISS
- Not reporting unofficial foreign travel through DISS
- Not reporting suspicious contacts
- Not reporting changes in storage capability

Resources:

- eLearning Course: NISP Reporting Requirements IS150.16
- FSO Toolkit: Reporting module
- Industrial Security Letter 2021-02: Clarification and Guidance on Reportable Activities
- CDSE NISPOM Reporting Requirements Job Aid

Most Common Instances of Non-Compliance

NISPOM 117.8(d): REPORTING LOSS, COMPROMISE, OR SUSPECTED COMPROMISE

Contractors will report any loss, compromise, or suspected compromise of classified information, U.S. or foreign, to the CSA.

Common Issues:

- Not reporting loss, compromise, or suspected compromise of classified information when required
- Not reporting information concerning an employee or other individual, determined to be responsible for an incident, when the information is requested to prove a security violation

Resources:

- FSO Toolkit: Reporting module
- NISP Tools and Resources: Security Incident Job Aid
- CDSE Security Short: Cybersecurity Incident Response
- CDSE Security Short: Security Incidents Reporting Requirements

Most Common Instances of Non-Compliance

NISPOM 117.10(a)(3): DISS MANAGEMENT

Contractors will annotate and maintain the accuracy of their employees' records in the system of record for contractor eligibility and access to classified information.

Common Issues:

- Not maintaining a DISS or NBIS account when required
- Not having an alternate user resulting in lack of records management
- Not maintaining personnel clearance records such as access, special briefings, and separation

Resources:

- FSO Toolkit: Personnel Clearances module
- NISP Tools and Resources: DISS Management Guidance Job Aid
- DISS Resources webpage
- NBIS page on the Security Training, Education, and Professionalization Portal (STEPP)

Most Common Instances of Non-Compliance

NISPOM 117.12(g): INSIDER THREAT TRAINING

The designated ITPSO will ensure that contractor program personnel assigned insider threat program responsibilities and all other cleared employees complete training.

Common Issues:

- Not providing all newly cleared employees with insider threat awareness training before granting access to classified information
- Not providing insider threat awareness training to all cleared employees every 12 months that includes the minimum requirements
- Not providing training to insider threat program personnel, including the ITPSO, that includes the minimum requirements

Resources:

- eLearning Course: Insider Threat Awareness INT101.16
- eLearning Course: Establishing an Insider Threat Program for Your Organization INT122.16
- Insider Threat Toolkit: Training and Awareness module
- CDSE Insider Threat Program for Industry Job Aid

Most Common Instances of Non-Compliance

NISPOM 117.15(a): SAFEGUARDING CLASSIFIED INFORMATION

Contractors will safeguard classified information in their custody or under their control, with approval for such storage of classified information by the applicable CSA.

Common Issues:

- Not protecting oral discussions from interception by unauthorized persons
- Not conducting end of day security checks to verify all classified information and security repositories have been appropriately secured
- Not providing the extent of protection to classified information sufficient to reasonably protect it from loss or compromise

Resources:

- eLearning Course: Safeguarding Classified Information in the NISP IS109.16
- FSO Toolkit: Safeguarding module
- NISP Tools and Resources: Open Storage Area Approval Checklist, Open Storage Area Approval Checklist Guide, DCSA 147 Process Overview Guide, Security Incident Job Aid

Most Common Instances of Non-Compliance

NISPOM 117.18(b): INFORMATION SYSTEM SECURITY REQUIREMENTS

Contractors will maintain an information system (IS) security program that supports the overall information security by incorporating a risk-based set of management, operational, and technical security controls.

Common Issues:

- Not maintaining procedures that reduce information security risks to an acceptable level and address information security throughout the IS lifecycle
- Not maintaining plans and procedures to assess, report, isolate, and contain data spills and compromises
- Not providing IS security training for authorized users
- Not implementing processes to continually evaluate threats and vulnerabilities to contractor activities, facilities, and IS to ascertain the need for additional safeguards

Resources:

- eLearning Courses: Introduction to the Risk Management Framework CS124.16, Continuous Monitoring CS200.16
- ISSM Toolkit: All modules
- NISP Cybersecurity Office webpage

Resources and Training

Resources

Industry security professionals are encouraged to review the DCSA website frequently for updates and important reminders.

- DCSA Website
  - DCSA Industrial Security Letters under NISP Resources dropdown
  - DCSA NISP Tools and Resources webpage
  - DCSA Voice of Industry Newsletters
- CDSE Website
  - CDSE Toolkits
  - Video: You're a New FSO: Now What?
  - Virtual Instructor-Led Course: Getting Started Seminar for New FSOs IS121.10
  - Curricula: FSO Orientation for Non-Possessing Facilities IS020.CU, FSO Program Management for Possessing Facilities IS030.CU
  - Security Short: Industrial Security for Senior Management

Questions and Feedback

Questions

Send facility specific questions to your DCSA assigned Industrial Security Representative.

Presentation Feedback:

Send questions or feedback related to this presentation to the DCSA NISP Mission Performance Division Mailbox at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil