Student Guide

Industrial Security Basics

Lesson 1: Course Introduction

Introduction

Opening

In order to protect our National Security, the U.S. government must safeguard its classified information, but at the same time it must also share this information with the thousands of U.S. companies who work as government contractors and require access to classified information while performing on contracts, programs, bids, and research and development efforts. In order to safely and securely share classified information with government contractors, the government established the National Industrial Security Program, or NISP.

To protect the classified information entrusted to industry, the NISP relies on many individuals, from both industry and government, in a wide range of roles and with a variety of responsibilities.

As someone who plays a role in industrial security, it is important for you to understand not only your own duties, but the roles and responsibilities of other key industrial security personnel as well. A shared understanding of the purpose and structure of the NISP, and the roles and responsibilities of its key players, will help you do your part to protect National Security.

Course Overview

Welcome to Industrial Security Basics. This course will provide you with an overview of the NISP, including its structure, and regulatory foundations. It will also introduce you to the key roles involved in the NISP, and will review industrial security responsibilities of each.

Here are the course objectives.

- Identify the purpose of the National Industrial Security Program (NISP), as well as the authorities that oversee its operation

- Identify the purpose of the regulatory documents that form the basis of the NISP, and identify where each document falls in the Industrial Security policy framework
- Identify the primary roles involved in the NISP and the industrial security responsibilities of each

Student Guide

Industrial Security Basics

Lesson 2: NISP Overview and Oversight

Contents

Introduction

Objectives

In order to succeed in your role as an employee with industrial security responsibilities, you need to understand the purpose of the NISP. You should also be familiar with the regulatory documents that establish and guide the NISP, as well as the authorities that oversee the NISP and ensure that it successfully carries out its mission.

Here are the lesson objectives:

- Identify the purpose of the NISP, as well as the authorities that oversee its operation
    - Identify the purpose of the NISP, including the distinct government and industry responsibilities
    - Identify the organizations and roles that have NISP oversight responsibilities
    - Identify the five NISP CSAs
    - Identify the organizations and roles that have DoD Oversight responsibilities
    - Identify key industrial security terminology relating to NISP authority
- Identify the purpose of the regulatory documents that form the basis of the NISP, and identify where each document falls in the Industrial Security policy framework
    - Identify the national level policy that forms the foundation of the NISP
    - Identify the DoD policy documents that implement the NISP for the DoD
    - Identify key industrial security terminology relating to NISP policy

Definition and Purpose of the NISP

What is the NISP?

The majority of our nation's technology is developed and produced by industry – and much of that technology is classified. The government entrusts cleared industry with classified information for use performing work on contracts, programs, bids, and research and development efforts. The National Industrial Security Program, or NISP, was established to ensure that cleared industry protects classified information in its possession.

The NISP applies to all U.S. contractors that require access to classified information, working for all executive branch departments and agencies.

In order to ensure that classified information entrusted to industry is properly protected, DoD 5220.22-M, the National Industrial Security Program Operating Manual, or NISPOM, defines the requirements, restrictions, and safeguards that industry must follow. These protections are in place before any classified work may begin; government agencies have the responsibility to provide security requirements for all requests for proposals and contracts that require access to classified information.

For more information on contract requirements, see Acquisitions and Contracting Basics in the NISP, available through CDSE's Security, Training, Education and Professionalization Portal, or STEPP.

NISP Overview

In order to implement the NISP and protect classified information, government agencies and industry contractors play important but distinct roles. Although we will review the details of these roles later in the course, for now you should understand the basic division of responsibility in the NISP.

On the government side, Cognizant Security Agencies, or CSAs, establish industrial security programs and oversee and administer security requirements. There are five CSAs that are ultimately responsible for the security of all cleared U.S. contractors:

- Department of Defense
- Department of Energy
- Office of the Director of National Intelligence
- Nuclear Regulatory Commission
- Department of Homeland Security

These agencies establish requirements, advise and assist contractors with industrial security, and provide security oversight.

In addition to the relevant CSA, the government contracting activity, or GCA, also plays a key role in protecting classified information entrusted to industry. The GCA has broad authority regarding acquisition functions for its agency, as delegated by the agency head. In addition to issuing the contract, the GCA also provides industry contractors with contract-specific guidance and oversight.

Finally, on the industry side, contractors have one major responsibility – they must implement the NISP requirements to protect classified information.

NISP Overview and Oversight

National Level Policy

Several national-level policy documents establish and support the NISP across all executive agencies.

In 1993, Executive Order 12829 established the NISP in order to provide a comprehensive and government-wide source for the requirements and safeguards used to protect classified information entrusted to industry. This executive order applies to all executive branch departments.

32 CFR 2004, "NISP Implementing Directive," of 2006, and its amendment in 2010, implement this executive order. The directive provides agencies with guidance for uniform standards throughout the NISP, and specifically outlines Cognizant Security Agency (CSA) and Government Contracting Activity (GCA) responsibilities.

It also outlines requirements for DoD 5200.22-M, the National Industrial Security Program Operating Manual, or NISPOM. The NISPOM provides detailed industrial security policy for contractors. As a national-level document, the NISPOM ensures uniform implementation of the NISP across government contracts. The NISPOM provides detailed operating instructions on a number of specific industrial security areas.

NISPOM

NISPOM topics include:

- General policies and procedures
- Reporting requirements
- Facility clearances (FCLs)
- Personnel security clearances (PCLs)
- Foreign Ownership, Control, or Influence (FOCI) issues
- Security training and briefings
- Classification
- Marking requirements
- Safeguarding of classified information

- Visits and meetings
- Subcontracting
- Information System (IS) security
- Special requirements, including nuclear-related information, Critical Nuclear Weapon Design Information (CNWDI), intelligence information, and communications security (COMSEC)
- International security requirements

National Level Oversight

As you saw, Executive Order 12829 establishes the NISP for all executive branch departments.

This executive order grants the National Security Council, or NSC, overall policy direction for the NISP.

Separately, it grants the Information Security Oversight Office, or ISOO, responsibility for overall implementation of the NISP. The ISOO issues implementing directives, and produces an annual report on the NISP. Chaired by the director of the ISOO, the executive order also establishes the National Industrial Security Program Policy Advisory Committee, or NISPPAC, which advises on all matters concerning NISP policies.

Finally, the executive order designates the Secretary of Defense as Executive Agent for the NISP. As Executive Agent, the Secretary of Defense is responsible for issuing and maintaining the NISPOM.

Cognizant Security Agencies

E.O. 12829, along with its implementing directive, 32 CFR 2004, also designates the Cognizant Security Agencies (CSAs).

As you know, CSAs establish specific industrial security programs and provide industrial security guidance and oversight in order to protect classified information entrusted to industry.

CSAs inspect and monitor cleared companies that require access to classified information, and they determine eligibility for access to classified information.

As you'll recall, there are currently five executive branch agencies that have been designated as CSAs.

The Department of Defense is the largest CSA, with the most classified contracts with industry. As a CSA, the Secretary of Defense has operational oversight of the DoD portion of the NISP and the authority to enter into agreements with GCAs to provide industrial security services.

Other CSAs include the Office of the Director of National Intelligence, the Department of Energy, the Nuclear Regulatory Commission, and the Department of Homeland Security.

DoD Policy and Oversight

DoD as CSA

As you just saw, the DoD is the largest CSA, and has the most classified contracts with industry. The DoD has entered into agreements with more than 28 other Federal agencies to serve as CSA on their behalf. Through memoranda of agreement, or MOAs, with the Secretary of Defense, these agencies have agreed to recognize the DoD as their CSA.

DoD Policy

Several policy documents implement the NISP for the DoD.

DoD Instruction 5220.22, National Industrial Security Program, establishes NISP policy for the DoD in accordance with Executive Orders 10865 and 12829. This instruction assigns and outlines responsibilities for NISP administration.

DoD 5220.22-R, Industrial Security Regulation, or ISR, sets forth the policies, practices, and procedures of the NISP for DoD components and the non-DoD agencies who have entered into agreements with the DoD, and outlines industrial security requirements.

Finally, DoD 5220.22-M, Volume 3, NISP Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence, or FOCI, establishes the policies, practices, and procedures that DoD components must use for FOCI determination and mitigation under the NISP. Until this is fully updated, DTM 15-002, provides policy guidance for the processing of National Interest Determinations, or NIDs, in connection with FOCI.

Industrial Security Regulation (ISR)

ISR outlines security requirements for:

- General security procedures
- Facility and personnel clearances
- Visitors
- Security vulnerability assessments
- Security violations
- Security education
- Security classification and declassification

- International security programs
- Industrial security forms

DoD Oversight

In DoD Instruction 5220.22, the Secretary of Defense designates NISP oversight responsibilities to the Under Secretary of Defense for Intelligence, or USD(I).

USD(I), in turn, establishes the Defense Security Service, or DSS, as the Cognizant Security Office, or CSO, for the DoD. This grants it authority to administer and provide security oversight for the DoD NISP.

DoD 5220.22 also outlines the responsibilities of the Under Secretary of Defense for Acquisition, Technology, and Logistics, or USD(AT&L), and of the DoD and non-DoD Components.

Under Secretary of Defense for Intelligence (USD(I))

- Oversees NISP policy and management
- Develops and updates DoD 5220.22-R (ISR)

Defense Security Service (DSS)

- Serves as the CSO for contractors under DoD security cognizance
- Ensures contractor eligibility for access to classified information
- Administers the NISP
- Provides security oversight
- Provides security education, training, certification, and professional development for DoD and for other U.S. Government personnel, contractor employees, and representatives of foreign governments

Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))

- Establishes acquisition policy, procedures, and guidance, in coordination with USD(I)

DoD and non-DoD Components

- Ensure release of classified information is necessary
- Include the “Security Requirements” clause in contracts
- Provide classification guidance
- Comply with DoD 5220.22-R (Industrial Security Regulation, or ISR) requirements

Review Activities

Review Activity 1

Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

The NISP only applies to contractors working for DoD components and agencies.

- ○ True
- ○ False

CSAs establish industrial security programs and provide security oversight.

- ○ True
- ○ False

Because CSAs have security oversight, after the contract is issued GCAs do not have any NISP responsibilities.

- ○ True
- ○ False

Review Activity 2

Identify the document described by each statement. Then check your answers in the Answer Key at the end of this Student Guide.

Outlines CSA and GCA responsibilities, and provides national-level guidance and standards.

- ○ NISPOM
- ○ 32 CFR 2004
- ○ DoDI-5220.22

Establishes NISP policy for the DoD and outlines responsibilities for DoD NISP administration

- ○ NISPOM
- ○ 32 CFR 2004
- ○ DoDI-5220.22

Provides policy requirements and operating instructions for contractors.

- ○ NISPOM
- ○ 32 CFR 2004
- ○ DoDI-5220.22

Answer Key

Review Activity 1

The NISP only applies to contractors working for DoD components and agencies.

- ○ True
- ⊙ False (correct response)

Feedback: *The NISP applies to ALL executive branch departments.*

CSAs establish industrial security programs and provide security oversight.

- ⊙ True (correct response)
- ○ False

Feedback: *CSAs establish industrial security programs and provide security oversight.*

Because CSAs have security oversight, after the contract is issued GCAs do not have any NISP responsibilities.

- ○ True
- ⊙ False (correct response)

Feedback: *In addition to issuing the contract, GCAs provide industry contractors with contract-specific guidance and oversight.*

Review Activity 2

Outlines CSA and GCA responsibilities, and provides national-level guidance and standards.

- ○ NISPOM
- ⊙ 32 CFR 2004 (correct response)
- ○ DoDI-5220.22

Feedback: *32 CFR 2004 outlines CSA and GCA responsibilities, and provides national-level guidance and standards.*

Establishes NISP policy for the DoD and outlines responsibilities for DoD NISP administration

- ○ NISPOM
- ○ 32 CFR 2004
- ⊙ DoDI-5220.22 (correct response)

Feedback: *DoDI-5220.22 establishes NISP policy for the DoD and outlines responsibilities for DoD NISP administration.*

Provides policy requirements and operating instructions for contractors.

- ⊙ NISPOM (correct response)
- ○ 32 CFR 2004
- ○ DoDI-5220.22

Feedback: *The NISPOM provides policy requirements and operating instructions for contractors.*

Student Guide

Industrial Security Basics

Lesson 3: NISP Roles and Responsibilities

Contents

Introduction

Objectives

In order to succeed in its mission to protect classified information entrusted to industry, the NISP relies on a variety of organizations and on individuals in a variety of roles. In order to succeed in your role, you should understand not only your own responsibilities – you should also be aware of the functions carried out by others working to support the NISP.

Here are the lesson objectives:

- Identify the primary roles involved in the NISP and the industrial security responsibilities of each
    - Identify the purpose and function of DSS as Cognizant Security Office, including specific DSS mission areas and functions
    - Identify the Government Contracting Activity (GCA) roles and responsibilities in NISP implementation
    - Identify the individual roles that support the NISP, along with their industrial security responsibilities
    - Identify key industrial security terminology relating to NISP roles and responsibilities

Organizational Roles and Responsibilities

DoD Delegation of Security Cognizance

Before exploring the roles that individuals play in the NISP, let's take a moment to review the roles and responsibilities of the organizations that support the NISP.

As you saw in the last lesson, Cognizant Security Agencies, or CSAs, oversee and administer industrial security requirements, and are ultimately responsible for the security of classified information used by contractors who hold classified contracts.

As the largest of the CSAs, the DoD delegates this security cognizance to the Defense Security Service, or DSS, and names DSS as its Cognizant Security Office, or CSO.

As CSO, DSS administers the NISP, provides security oversight, and conducts vulnerability reviews. DSS provides security education and training; publishes industrial security letters, or ISLs, which provide guidance and clarification on NISP policies and procedures; certifies, accredits, and oversees information systems used to store classified information; and finally, funds background investigations for contractor personnel and makes interim determinations for contractor personnel who require access to classified information.

DSS Mission: Regional NISP Administration

Administration of the NISP is key to the overall DSS mission, and much of that administration is carried out by DSS Industrial Security Field Operations, or ISFO.

ISFO provides oversight and conducts security vulnerability assessments for approximately 13,000 cleared contractor facilities.

ISFO maintains industrial security field offices all over the country, grouped into 4 geographic regions. Each region has a regional director, who oversees the operation of field offices in his or her region.

Each field office is locally managed by a Field Office Chief, and staffed by Industrial Security Representatives, or IS Reps. The Field Office Chief assigns an IS Rep to each contractor facility.

ISFO Headquarters Functions

In addition to overseeing the field offices and their operations, Industrial Security Field Operations (ISFO) oversees headquarters components including the Facility Clearance Branch, which processes companies for facility security clearances, or FCLs, issues FCLs, and monitors companies that hold FCLs.

ISFO also oversees the Personnel Security Management Office for Industry, or PSMO-I, which processes personnel security clearances.

Finally, ISFO oversees the Office of Designated Approving Authority, or ODAA. ODAA carries out DSS certification and accreditation, or C and A, determinations for contractor information systems to process classified information.

To learn more about each of these headquarters components, see the DSS ISFO website.

Industrial Policy and Programs

Industrial Security Field Operations (ISFO) and cleared contractors receive industrial security support from another DSS organization, Industrial Policy and Programs, or IP.

IP supports the NISP in the areas of NISP security policy, Foreign Ownership, Control, or Influence, or FOCI, issues, the administration of international programs, and other areas.

IP is composed of several divisions.

Policy

- Supports DSS ISFO with timely and consistent policy guidance
- Provides effective interpretation of NISP policy to DSS personnel, GCAs, and cleared contractors

FOCI Operations

- Determines and mitigates FOCI
- Determines the need for a National Interest Determination (NID) under a Special Security Agreement (SSA)
- Participates in security vulnerability assessments and annual meetings

To learn more about FOCI and the NISP, see the Understanding FOCI course, available through CDSE's Security, Training, Education and Professionalization Portal, or STEPP, and the National Interest Determinations and FOCI Shorts, available through CDSE's website.

FOCI Analytics

- Assesses and verifies NISP facility data to highlight vulnerabilities
- Recommends strategies for mitigating risks to National Security
- Coordinates with ISFO and the FOCI Operations Division and provides the following services:
    - Prepares FOCI assessments, which recommend the appropriate mitigation tool for each individual case, including assessments for all Committee on Foreign Investment in the United States (CFIUS) cases involving DSS equities
    - Executes and removes FOCI Board Resolution mitigation plans
- Proposes National Interest Determinations (NIDs) on behalf of the GCA

International Programs

- Oversees involvement with foreign governments, foreign contractors, and NATO
- Carries out NATO inspections
- Assists with security vulnerability assessments
- Reviews Transportation Plans
- Validates security assurances
- Issues NATO Facility (Security) Clearances (FCLs) and oversees the DoD NATO Direct-Hire program

Assessments and Evaluations (A&E)

- Monitors contractors for changes impacting contractor Facility (Security) Clearances (FCLs)
- Analyses, reports, and certifies data for Personnel Security Investigations (PSIs):
    - Plans, programs, and budgets for contractor PSI requirements
    - Conducts annual surveys of contractors to estimate PSI requirements
    - Monitors expenditures and provides analysis and oversight of PSI funding for cleared industry
- Oversees NISP compliance reporting and business integrity:
    - Assesses and verifies self-reported financial information in support of the NISP
    - Proactively monitors data and events pertinent to NISP reporting through continuous mining of commercial and government data sources
    - Conducts and reports on the annual NISP Cost Collection Survey, which captures security costs incurred by contractor facilities

Special Programs

- Manages the security oversight function of DSS's direct and indirect support to the Special Access Program (SAP) community

Counterintelligence Directorate

The Counterintelligence, or CI, Directorate also provides support to Industrial Security Field Operations (ISFO) and cleared contractors. The CI directorate receives suspicious contact reports, or SCRs, oversees CI awareness and reporting, and, along with ISFO, performs advise and assist visits and assists with security vulnerability assessments.

To learn more, see the DSS CI website.

DSS Mission: SETA

As you just saw, DSS performs a variety of critical functions as CSO. DSS's mission also includes Security Education, Training and Awareness, or SETA, which is administered by the Center for Development of Security Excellence, or CDSE.

CDSE's mission is the professionalization of the security community, and to accomplish this, CDSE provides security education and training for both DoD and industry.

To learn more, see the DSS CDSE website.

GCA Role and Responsibilities

Remember that, although DSS has security cognizance for the DoD, Government Contracting Activities, or GCAs, play an important role in the NISP. The designation of a CSA does not relieve the GCA of its NISP responsibilities.

As you know, the GCA issues the contract and ensures the security requirements clause (Federal Acquisition Regulation, or FAR, Security Requirements clause) is included in contracts that will require access to classified information.

The GCA also provides contract-specific guidance for contracts that require access to classified information, including the DoD Contract Security Classification Specification, or DD Form 254, and classification and declassification information.

In addition, the GCA sponsors facilities for facility clearances; ensures the Original Classification Authority, or OCA, conducts damage assessments in the case of loss, compromise, or suspected compromise of classified information; and provides appropriate education and training to any department or agency personnel who have NISP responsibilities.

Individual Roles and Responsibilities

Introduction to Individual Roles and Responsibilities

As you have already seen, in order to protect classified information, government agencies, including the GCA who issued the classified contract, DSS in its role as the CSA for the DoD, and the industry contractor, all have a role to play in the NISP. Within each of these organizations, different individuals do their part to make sure that classified information is protected.

On the government side, DoD Security Specialists or Activity Security Managers act as the GCA representatives to the NISP and serve as resident security experts.

As part of the organization with security oversight responsibility, DSS employees have a range of key responsibilities in implementing the NISP. These employees include Industrial Security Representatives, or IS Reps, Information System Security Professionals, or ISSPs, Counterintelligence, or CI, Personnel, including Counterintelligence Special Agents, or CISAs, and other Industrial Security Headquarters Personnel, including Field Operations and Policy and Programs.

Finally, on the contractor side, Facility Security Officers, or FSOs, oversee the day-to-day operation of the contractor's security program, while Information System Security Managers, or ISSMs, are responsible for managing information system security.

GCA Employees

DoD Security Specialists or Activity Security Managers are the GCA representatives to the NISP. They serve as security experts, and maintain security cognizance over all activity information, personnel, information systems, physical security and – most importantly for the NISP – industrial security.

DoD Security Specialists or Activity Security Managers review, and may also complete, the DD Form 254, which provides classification and declassification information to contractors, and they receive security violation and administrative inquiry reports in cases of loss, compromise, or suspected compromise of classified information.

In cases where the contractor accesses classified information at the *government* base or installation, the DoD Security Specialist or Activity Security manager must ensure compliance with DoD Policies, and is responsible for conducting security inspections on the government installation.

If, however, the contractor accesses classified information at their own facility *on* the installation, a Memorandum of Agreement or Memorandum of Understanding (MOA/MOU) between the GCA and DSS will identify specific responsibilities. If DSS retains responsibility then the NISPOM applies; if the GCA retains responsibility, then DoD policy applies.

DSS Employees

As CSO for DoD, DSS provides security support to a large number of military services, defense agencies, non-DoD Federal Agencies, and cleared contactor facilities. To do this, it relies on individuals in a variety of roles.

Industrial Security Representatives (IS Reps) are DSS employees and there are over 200 located throughout the country. They serve as the contractor's primary point of contact for security matters;

Information System Security Professionals (ISSPs) work with IS Reps and contractor personnel on all matters related to the accreditation and maintenance of accredited contractor information systems;

Each geographic region has a Region Counterintelligence, or CI, Chief who oversees the activities of the CI Special Agents, or CISAs, who provide advice, oversight, and training regarding CI issues.

Finally, headquarters personnel support the various DSS operational elements – ISFO, IP, CI, and CDSE – as well as cleared contractors in a wide range of security areas.

IS Rep

Major Industrial Security Representative (IS Rep) Responsibilities

- Works closely with the Facility Security Officer (FSO) to provide advice, assistance, and oversight
- Conducts facility surveys before issuance of Facility (Security) Clearances (FCLs)
- Conducts security vulnerability assessments and reviews of the contractor's security program
- Coordinates with other entities within the Defense Security Service (DSS) to oversee all aspects of contractor security, including
    - Foreign Ownership, Control, or Influence (FOCI)
    - International security
    - Accredited information systems
    - Special programs (e.g., Special Access Programs (SAP), Arms, Ammunition, and Explosives (AA&E))
- Receives reports of security violations from FSO
- Conduct administrative inquiries, when appropriate
- Reports security violations to Government Contracting Activity (GCA)

ISSP

Major Information System Security Professional (ISSP) Responsibilities

- Works with Industrial Security Representatives (IS Reps), Facility Security Officers (FSOs), and Information System Security Managers (ISSMs) on all matters related to the maintenance of accredited classified contractor information systems
- Performs assessments of classified information systems and makes recommendations to the RDAA
- Participates in security vulnerability assessments of facilities with accredited classified information systems
    - Evaluates vulnerabilities
    - Identifies potential cyber security threats
    - Helps develop mitigation strategies
- Responds to security violations involving accredited classified information systems
- Develops and maintains technical proficiency of ever changing technology developments

CI Personnel (CI Chief and CISA)

Major Counterintelligence (CI) Personnel Responsibilities

Counterintelligence Special Agents (CISAs) work with Facility Security Officers (FSOs) to:

- Identify potential threats to U.S. technology
- Develop employee CI awareness/reporting
- Assist with foreign travel briefings and debriefings

CISAs work with Industrial Security Representatives (IS Reps) to:

- Conduct Advise and Assist visits
- Provide advice and guidance regarding CI best practice
- Help conduct vulnerability assessments Evaluates vulnerabilities

Headquarters Personnel

Headquarters personnel include Field Operations and Policy and Program Personnel, who support Industrial Security Field Office (ISFO) and Industrial Policy and Programs (IP) functions.

Contractor Employees

At contractor facilities, individuals in two roles are primarily responsible for overseeing the NISP: the Facility Security Officer (FSO) and the Information System Security Manager (ISSM).

The FSO has ultimate responsibility for the administration, oversight, and day-to-day operation of the contractor security program. FSOs must ensure compliance with the NISP, follow NISPOM Guidelines, and remain compliant with the terms outlined in DD 441. More information about the FSO's role and responsibilities can be found in the FSO Role in the NISP course available in STEPP.

The ISSM works very closely with the FSO to manage contractor-owned information systems. The ISSM ensures that NISPOM Information System Security, or ISS, requirements are met.

FSO

Major FSO Responsibilities

To ensure compliance with the NISP, FSO responsibilities include, but are not limited to:

- Monitoring approved classified information systems, including information storage, processing, and removal
- Working with DSS to maintain a viable security program

- Maintaining procedures for incoming and outgoing classified visits
- Educating all cleared personnel on their security responsibilities

The FSO oversees facility security, including but not limited to:

- Facility clearance
- Personnel clearances
- Security education
- Safeguarding of classified information
- Reporting to the government
- Self-inspections

ISSM

Major ISSM Responsibilities

ISSM responsibilities include, but are not limited to:

- Information System Security (ISS) education, awareness, and training
- Establishment, documentation, maintenance, and monitoring of ISS programs and procedures
- Identification/documentation of unique local information security threats and vulnerabilities
- Periodic self-inspections
- Notification to the CSA of security relevant changes to information systems

The ISSM develops facility procedures for:

- Handling of media and equipment containing classified information
- Implementation of security features
- Incident reporting
- User acknowledgment of responsibility
- Threat detection (auditing and monitoring for malware, phishing attempts, etc.)

Review Activities

Review Activity 1

Which of these are DSS responsibilities or functions?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Provide security education and training
- ☐ Certify, accredit, and oversee information systems
- ☐ Provide contract-specific classification guidance
- ☐ Fund contractor background investigations

Review Activity 2

Identify the role described by each statement. Then check your answers in the Answer Key at the end of this Student Guide.

This DSS employee serves as the contractor's primary point of contact for security.

- ISSP
- FSO
- ISSM
- IS Rep

This DSS employee oversees accredited contractor information system use.

- ISSP
- FSO
- ISSM
- IS Rep

This contractor employee administers and oversees the contractor security program.

- ISSP
- FSO
- ISSM
- IS Rep

This contractor employee manages information systems and ensures ISS requirements are met.

- ISSP
- FSO
- ISSM
- IS Rep

Answer Key

Review Activity 1

Which of these are DSS responsibilities or functions?

- ☑ Provide security education and training (correct response)
- ☑ Certify, accredit, and oversee information systems (correct response)
- ☐ Provide contract-specific classification guidance
- ☑ Fund contractor background investigations (correct response)

***Feedback**: DSS provides security education and training, certifies, accredits, and oversees information systems, and funds contractor background investigations. GCAs provide contract-specific classification guidance.*

Review Activity 2

Identify the role described by each statement.

This DSS employee serves as the contractor's primary point of contact for security.

- ○ ISSP
- ○ FSO
- ○ ISSM
- ⊙ IS Rep (correct response)

Feedback: *IS Reps serve as the contractor's primary point of contact for security.*

This DSS employee oversees accredited contractor information system use.

- ⊙ ISSP (correct response)
- ○ FSO
- ○ ISSM
- ○ IS Rep

Feedback: *ISSPs oversee accredited contractor information system use.*

This contractor employee administers and oversees the contractor security program.

- ○ ISSP
- ⊙ FSO (correct response)
- ○ ISSM
- ○ IS Rep

Feedback: *FSOs administer and oversee contractor security programs.*

This contractor employee manages information systems and ensures ISS requirements are met.

- ○ ISSP
- ○ FSO
- ⊙ ISSM (correct response)
- ○ IS Rep

Feedback: *ISSMs manage information systems and ensure ISS requirements are met.*

Student Guide

Industrial Security Basics

Lesson 4: Course Conclusion

Course Conclusion

Course Summary

In this course, you learned about the purpose of the NISP, the regulatory documents that establish and guide the NISP, the authorities that oversee the NISP, and the organizations and individuals who ensure that the NISP succeeds in its mission to protect classified information entrusted to industry.

Lesson Review

Here is a list of the lessons in the course:

- Lesson 1: Course Introduction
- Lesson 2: NISP Overview and Oversight
- Lesson 3: NISP Roles and Responsibilities
- Lesson 4: Course Conclusion.

Course Objectives

Congratulations. You have completed the Industrial Security Basics course. You should now be able to perform all of the listed activities:

- Identify the purpose of the National Industrial Security Program (NISP), as well as the authorities that oversee its operation
- Identify the purpose of the regulatory documents that form the basis of the NISP, and identify where each document falls in the Industrial Security policy framework
- Identify the primary roles involved in the NISP and the industrial security responsibilities of each

To receive course credit, you MUST take the Industrial Security Basics examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.

Glossary

Course: Industrial Security Basics

Access: The ability and opportunity to gain knowledge of classified information

Arms, Ammunition and Explosives (AA&E): Program that provides guidance regarding the safety of arms, ammunitions and explosives.

Assessment and Evaluations (A&E): Monitors contractors for changes impacting their Facility Clearance (FCL) and analyses, reports and certifies data for Personnel Security Investigations (PSIs).

Certification and Accreditation (C&A): The standard Department of Defense (DoD) approach for identifying information security requirements, providing security solutions, and managing the security of DoD Information Systems (IS).

Classified Contract: Any contract requiring access to classified information by a contractor in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.

Classified Information: Official information that has been determined, pursuant to Executive Order 13526 or any predecessor order, or pursuant to the Atomic Energy Act of 1954, to require protection against unauthorized disclosure in the interest of national security which has been designated.

Classified Visit: A visit during which a visitor will require, or is expected to require, access to classified information.

Cleared Employees: All contractor employees granted PCLs and all employees being processed for PCLs.

Cognizant Security Agencies (CSAs): Agencies of the Executive Branch that have been authorized by Executive Order 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense, Office of the Director of National Intelligence, Department of Energy, Nuclear Regulatory Commission, and Department of Homeland Security.

Cognizant Security Office (CSO): The organizational entity delegated by the head of a CSA to administer industrial security on behalf of the CSA.

Committee on Foreign Investment in the United States (CFIUS): an Interagency committee chaired by the Treasury Department, conducts reviews of proposed mergers, acquisition or takeovers of U.S. persons by foreign interests under section 721 (Exon-Florio amendment) of the Defense Production Act (reference (m)).

Communications Security (COMSEC): Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. government relating to national security and to ensure the authenticity of such communications.

Compromise: An unauthorized disclosure of information.

Contract Security Classification Specification – DD Form 254: DD Form 254 provides to the cleared contractor, or cleared subcontractor the security requirements and the classification guidance that are necessary to perform on a specific classified contract.

Contractor: Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

DD Form 254: Contract Security Classification Specification

DD Form 441 (Security Agreement): A Department of Defense Security Agreement that is entered into between a contractor who will have access to classified information, and the DoD in order to preserve and maintain the security of the U.S. through the prevention of unauthorized disclosure of classified information.

Defense Security Service (DSS): The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction and control over DSS. DSS provides the military services, Defense Agencies, 30 federal agencies and approximately 13,500 cleared contractor facilities with security support services. DSS is the CSO for most DoD classified contracts.

DSS supports the National Security and the warfighter, secures the nation's technological base, and oversees the protection of U. S. and foreign classified information in the hands of industry. DSS accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

Defense Security Service, Center for Development of Security Excellence (CDSE): The Center for Development of Security Excellence is responsible for providing security education and training to DoD and other U.S. Government personnel, DoD contractors, and sponsored representatives of foreign governments.

Defense Security Service, Counterintelligence (CI) Office: Office within the Defense Security Service that provides counterintelligence support to DSS through CI reviews, assessments, analysis, and reports.

Defense Security Service, Facility Clearance Branch (FCB): The Defense Security Service (DSS) Facility Clearance Branch processes contractors for Facility Security Clearance (FCL) based upon procurement need, issues FCLs, and monitors the contractor's continued eligibility in the NISP.

Defense Security Service, Field Counterintelligence Specialist (FCIS): Assists FSOs in identifying potential threats to U.S. technology and developing CI awareness and reporting by company employees.

Defense Security Service, Field Office Chief (FOC): Manages the field offices that are staffed by Industrial Security Representatives, or IS Reps. The Field Office Chief is responsible for ensuring that each facility is assigned an IS Rep.

Defense Security Service, Foreign Ownership Control or Influence (FOCI) Office: This office within the Defense Security Service works with the local IS Rep to resolve issues that arise when a cleared facility or a facility being processed for a facility clearance is subject to foreign ownership, control or influence.

Defense Security Service, Industrial Policy and Programs (IP): This office within the Defense Security Service supports the Industrial Security Field Operations branch in the areas of NISP security policy, Foreign Ownership, Control, or Influence, or FOCI issues and the administration of international program.

Defense Security Service, Industrial Security Field Operations (ISFO): Provides oversight and conducts security vulnerability assessments for approximately 13,500 cleared contractor facilities. They maintain industrial security field offices all over the country.

Defense Security Service, Industrial Security Representative (IS Rep): Local representative from the Defense Security Service that provides advice and assistance on security matters and with establishing your security program to ensure your facility is in compliance with the NISP.

Defense Security Service, Information Systems Security Professional (ISSP): Local representative from the Defense Security Service, Office of Designated Approving Authority (ODAA) that provides advice and assistance visits to improve the security posture with regard to Information Systems and help facilitate the process of getting your information systems accredited to process classified information.

Defense Security Service, International Programs: An office within the Defense Security Service that oversees involvement with foreign governments, foreign contractors

and NATO. They carry out NATO inspections, issues NATO FCLs and oversees the DoD NATO Direct-Hire program.

Defense Security Service, Office of Designated Approving Authority (ODAA): Office within the Defense Security Service that facilitates the certification and accreditations process for information systems at cleared contractor facilities.

Defense Security Service, Personnel Security Management Office for Industry (PSMO-I): Office within the Defense Security Service that processes requests for, and other actions related to personnel security clearances for personnel from facilities participating in the NISP.

Defense Security Service, Special Programs: Manages the security oversight function of DSS' direct and indirect support to the Special Access Program (SAP) community.

Director of National Intelligence (DNI): Retains authority over access to intelligence sources and methods.

DoD Security Specialist: Also called Activity Security Managers act as the GCA representatives to the NISP and serve as resident security subject matter experts (SMEs).They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.

Eligibility: A DoD Consolidated Adjudication facility (DoD CAF) has made an adjudicative determination of member's Personnel Security Investigation (PSI) and that member may have access to classified information equal to the level of their adjudicated investigation.

Executive Order (EO): An order issued by the President to create a policy and regulate its administration within the Executive Branch.

Facility: A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For the purposes of industrial security, the term does not include Government installations.

Facility (Security) Clearance (FCL): An Administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories).

Facility Security Officer (FSO): A U.S. citizen employee, appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information.

Federal Acquisition Regulation (FAR): Contains the rules for government acquisition. These rules provide instruction, forms and guidance on government contracting.

Federal Bureau of Investigations (FBI): The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities—the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community.

Foreign Interest: Any government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.

Foreign Ownership, Control, or Influence, (FOCI): Whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of a company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

Government Contracting Activity (GCAs): An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Industrial Security: That portion of information security concerned with the protection of classified information in the custody of U.S. industry.

Industrial Security Letters (ISLs): Documents that provide detailed operational guidance and notification of changes to or clarification of existing policies or requirements to the NISPOM.

Information Security: The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.

Information Security Oversight Office (ISOO): Office responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

Information System Security Manager (ISSM): An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.

Information System Security Officer (ISSO): ISSOs may be appointed by the ISSM in facilities with multiple accredited information systems. The ISSM will determine the responsibilities to be assigned to the ISSO in accordance with NISPOM Chapter 8.

Memoranda of Agreement (MOAs): A written agreement among relevant parties that specifies roles, responsibilities, terms and conditions for each party to reach a common goal.

National Industrial Security Program (NISP): The National Industrial Security Program (NISP) was established by Executive Order 12829 for the protection of classified information released or disclosed to industry in connection with classified contracts. The NISP applies standards for the protection of classified information released or disclosed to contractors of all federal executive branch departments and agencies. Requirements of the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM), (DoD 5220.22-M).

National Industrial Security Program Operating Manual (NISPOM): A manual issued in accordance with the National Industrial Security Program that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified of classified information.

National Industrial Security Program Policy Advisory Committee (NISPPAC): The Committee members shall advise the Chairman of the Committee on all matters concerning the policies of the National Industrial Security Program, including recommended changes to those policies as reflected in E.O. 12829, its implementing directives, or the operating manual established under E.O. 12829, and serve as a forum to discuss policy issues in dispute.

National Interest Determination (NID): Is a written statement by the Government Contracting Activity or GCA, affirming that the release of proscribed information to the company will not harm the National Security interests of the U. S.

National Security Council (NSC): A governing entity responsible for providing overall policy direction for the National Industrial Security Program.

North Atlantic Treaty Organization (NATO): All classified information – military, political, and economic – circulated within North Atlantic Treaty Organization (NATO), whether such information originated in NATO or is received from member nations or from international organizations.

Original Classification Authority (OCA): An individual authorized in writing, either by the United States (U.S.) President, or by agency heads or other officials designated by the President, to initially classify a piece of information. OCAs must receive training to perform this duty.

Personnel (Security) Clearance (PCL): An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Proscribed Information: Includes Top Secret, Communications Security except classified keys used to data transfer, Restricted Data (RD) as defined in reference (c) of the NISPOM, Special Access Programs (SAP) and Sensitive Compartmented Information (SCI).

Security Training Education and Professionalization Portal (STEPP): The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses is maintained and where student information and course transcripts are maintained.

Special Access Program (SAP): Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to the NISPOM.

Special Security Agreement (SSA): Is used when a cleared company is effectively owned or controlled by a foreign entity with majority interest.

Subject Matter Expert (SME): An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.

Suspicious Contact Reports (SCRs): A report of CI concern that likely represents efforts by an individual to obtain illegal or unauthorized access to classified information or technology.

Under Secretary of Defense for Acquisition, Technology and Logistics (USD (ATL)): This office within the Department of Defense establishes acquisition policy, procedures and guidance in coordination with USD (I).

Under Secretary of Defense for Intelligence (USD (I)): Office within the Department of Defense that is responsible for overseeing NISP policy and management. It also develops and updates the DoD 5220.22-R, Industrial Security Regulation.