Industrial Security Basics

Course Introduction

Introduction

Narrator: 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.

Screen text: National Industrial Security Program

Course Overview

Narrator: 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. Take a moment to review them.

Screen text: 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

NISP Overview and Oversight

Objectives

Screen text: Introduction

Narrator: 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. Take a moment to review them.

Screen text: What is the NISP?

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

What is the NISP?

Screen text: Definition and Purpose of the NISP

Narrator: 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 serve as a single integrated, cohesive industrial security program to protect classified information and to preserve our Nation’s economic and technological interests.

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, 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.

Screen text: The National Industrial Security Program (NISP)

- Serves as a single cohesive industrial security program to protect classified information
- Applies to all contractors with access to classified information
- NISPOM defines industry requirements, restrictions, and safeguards

Screen text (rollover): NISPOM
DoD 5220.22-M, National Industrial Security Program Operating Manual

NISP Overview

Narrator: 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.

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 and preserving our Nation's economic and technological interests.

The GCA is an agency component or subcomponent to which the agency head delegates broad authority regarding acquisition functions. 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.

Screen text: Cognizant Security Agencies (CSAs) text box

- Establish requirements
- Advise and assist
- Provide oversight

Screen text: Government Contracting Activities (GCAs) text box

- Issues the contract
- Provides contract-specific guidance

Screen text: Contractors text box

- Implement NISP requirements

National Level Policy

Screen text: National Policy and Oversight

Narrator: 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. Updates have been applied to these directives and the current updates can be found on the Course Resource page.

The directive provides agencies with guidance for uniform standards throughout the NISP, and specifically outlines CSA and 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.

Select VIEW to access each document from the Resources page. Select the NISPOM to see a list of the topics that it covers.

Screen text:
E.O. 12829

- Establishes the NISP
- Applies to all executive branch departments

32 CFR 2004

- Provides agency guidance and uniform standards
- Outlines CSA and GCA responsibilities
- Rollover text: CSA Cognizant Security Agency

GCA Government Contracting Activity

NISPOM

- Provides policy for contractors
- Ensures uniform security requirements
- Includes detailed operating instructions

NISPOM pop-up text:

NISPOM

NISPOM topics include:

- General provisions and requirements
- Reporting requirements
- Facility clearances (FCLs)
- Personnel security clearances (PCLs)
- Foreign Ownership, Control, or Influence (FOCI) issues
- Security training and briefings
- Classification and 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

Narrator: 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.

Screen text:

<u>NSC</u>

- Oversees NISP policy

ISOO

- Implements and monitors the NISP
- Issues implementing directives
- Produces annual report

NISPPAC

- Advises on NISP policies

Secretary of Defense

- Serves as Executive Agent
- Issues and maintains the NISPOM

Screen rollover text:

ISOO	Information Security Oversight Office
NISPPAC	National Industrial Security Program Policy Advisory Committee
NSC	National Security Council

Cognizant Security Agencies

Narrator: E.O. 12829, along with its implementing directive, 32 CFR 2004, also designates the 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.

Screen text:
CSAs

- Establish Industrial Security programs
- Provide guidance and oversight
- Inspect and monitor cleared companies

- Determine eligibility for access to classified information

Screen rollover text:

CSAs	Cognizant Security Agencies

DoD as CSA

Screen Text: DoD Policy and Oversight

Narrator: 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 33 other Federal agencies to serve as CSA on their behalf.

Through memoranda of agreements, or MOAs, with the Secretary of Defense, these agencies have agreed to recognize the DoD as their CSA. You can find a list of these agencies on the Course Resources page.

Screen Text: MOA

See the Course Resources for a current list of agencies under DoD security cognizance.

Screen rollover text:

MOA	Memoranda of Agreement

DoD Policy

Narrator: 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 Manual 5220.22, Volume 2 National Industrial Security Program: Industrial Security Procedures for Government Activities, 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 Manual 5220.22, 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.

Select VIEW to access each document from the Course Resources page. Select DoD Manual 5220.22, Volume 2 to see a list of the industrial security requirements outlined in the manual.

Screen text:

DoDI 5220.22

- Establishes NISP policy
- Assigns and outlines responsibilities

DoDM 5220.22 Vol. 2
Describes NISP policies, practices, and procedures
Outlines industrial security requirements

DoDM 5220.22 Vol. 3

- Establishes policies, practices, and procedures for FOCI determination and mitigation

Screen rollover text:

FOCI Foreign Ownership, Control, or Influence

Select DoDM 5220.22 Vol. 2 to see a list of industrial security requirements.

DoDM 5220.22 Vol 2 Pop-up text:

DoD Manual 5220.22, Volume 2

DoD Manual 5220.22, Volume 2 outlines security for:

- General issuance information
- Responsibilities
- Procedures
- Facility and personnel clearances
- Eligibility for Access to Classified Information
- Contracting that Requires Access
- Safeguarding
- Inquiries, Investigations, and Administrative Actions
- Security, Education, Training and Awareness (SETA)
- Visits and Meetings
- Information Systems
- International Security Programs
- Associated Programs or Information
- Security Reviews and Continuing Security Assurance

DoD Oversight

Narrator: In DoD Instruction 5220.22, the Secretary of Defense designates NISP oversight responsibilities to the Under Secretary of Defense for Intelligence and Security, or USD(I&S).

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

DoDI 5220.22 also outlines the responsibilities of the Under Secretary of Defense for Acquisition and Sustainment, or USD(A&S), and of the DoD and non-DoD Components.

Select each office to learn more about its oversight role.

Screen text:

Serves as CSO for DoD
Select each office to learn more

CSO rollover text: Cognizant Security Office

Screen text:
USD(I&S)
USD(A&S)
DoD and non-DoD Components
DCSA

DCSA

DCSA Popup text: ***DCSA***

Defense Counterintelligence and Security Agency (DCSA)

- 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

Screen rollover text: CSO Cognizant Security Office

USD(I&S) Popup text:

USD(I&S)

Under Secretary of Defense for Intelligence and Security (USD(I&S))

- Oversees NISP policy and management
- Develops and updates DoD Manual 5220.22 Volume 2

Screen rollover text:
DoD Manual 5220.22, Volume 2: National Industrial Security Program: Industrial Security Procedures of Government Activities

USD(A&S) Popup text:

USD(A&S)

Under Secretary of Defense for Acquisition, and Sustainment (USD(A&S))

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

DoD and non-DoD Components Popup text:

DoD and non-DoD Components

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 Manual 5220.22, Volume 2 requirements

DoD Manual 5220.22, Volume 2 rollover text: National Industrial Security Program: Industrial Security Procedures for Government Activities

Knowledge Check

Review Activity 1
Narrator: Now, check your knowledge.

Screen text: Select True or False for each statement; then select Submit.

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

Answer Key

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

Narrator: Now, try this question.

Screen text:
Identify the document described by each statement; then select Submit.

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

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

Lesson Summary

Narrator: You have completed the lesson “NISP Overview and Oversight.” Select the Student Guide to review or select the forward arrow to move on.

Screen text:

You have completed the lesson “NISP Overview and Oversight”

To review, select the Student Guide or select Next to choose your next lesson.

NISP Roles and Responsibilities

Objectives

Screen text: Introduction

Narrator: 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 is the lesson objective. Take a moment to review it.

Screen text:

What are my responsibilities?
What do my colleagues do?

Lesson Objective

- Identify the primary roles involved in the National Industrial Security Program (NISP) and the industrial security responsibilities of each
    - Identify the purpose and function of the Defense Counterintelligence and Security Agency (DCSA) as Cognizant Security Office (CSO), including specific DCSA 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

DoD Delegation of Security Cognizance

Screen Text: Organizational Roles and Responsibilities

Narrator: 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 Counterintelligence and Security Agency, or DCSA, and names DCSA as its Cognizant Security Office, or CSO.

As CSO, DCSA administers the NISP, provides security oversight, and conducts security review actions. DCSA provides security education and training; publishes industrial security letters, or ISLs, which provide guidance and clarification on NISP policies and procedures; assesses, authorizes 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.

Screen text:
Defense Counterintelligence and Security Agency (DCSA)

- Provides oversight and conducts security review actions
- Provides security education and training
- Publishes Industrial Security Letters (ISLs)
- Assesses, authorizes, and oversees contractor classified information systems
- Funds contractor background investigations and makes interim access determinations

DCSA serves as Cognizant Security Office (CSO) for the DoD.

DCSA Mission: Regional NISP Administration

Narrator: Administration of the NISP is key to the overall DCSA mission, and much of that administration is carried out by DCSA field elements.

These field elements provide oversight and conduct security review actions for approximately 12,500 cleared contractor facilities.

DCSA maintains field offices all over the country, grouped into several geographic regions. Each region has a Regional Director or RD, who oversees the operation of field offices in his or her region.

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

Screen text:
DCSA Field Elements

- Provide oversight
- Conduct security review actions

DCSA Headquarters Functions

Narrator: In addition to field offices and their operations, there are DCSA headquarters components, including the Facility Clearance Branch or FCB, which processes companies for facility clearances, or FCLs, issues FCLs, and monitors companies that hold FCLs.

In addition, there is the National Industrial Security Program Authorization Office, or NAO. NAO carries out DCSA assessment and authorization, or A&A, determinations for contractor information systems to process classified information.
To learn more about each of these headquarters' components, see the DCSA website. Select VIEW to access this website from a list of Course Resources.

Screen text:

Facility Clearance Branch (FCB)

- Processes companies for Facility Clearances (FCLs)
- Issues FCLs
- Monitors companies that hold FCLs

National Industrial Security Program Authorization Office (NAO)

- Carries out DCSA assessment and authorization (A&A) determinations for contractor information systems to process classified information

DCSA Divisions in Support of Industrial Security

Narrator: DCSA field elements and cleared contractors receive industrial security support from other DCSA divisions as well.

These divisions support 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.

Select each to learn more about its role in the NISP.

Screen text:
DCSA Divisions in Support of Industrial Security

- Supports DCSA field elements and cleared contractors in the following areas:
    - Security policy related to the NISP
    - Mitigation of FOCI and implementation of FOCI countermeasures
    - Administration of international programs

FOCI rollover text: Foreign Ownership, Control, or Influence

Policy popup text:

Policy

Policy

- Delivers timely and consistent policy guidance
- Provides effective interpretation of NISP policy to DCSA personnel, GCAs, and cleared contractors

FOCI Mitigation popup text:

FOCI Mitigation

Narrator: 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 Mitigation

- Determines and mitigates FOCI
- Assesses and verifies NISP facility data to highlight vulnerabilities
- Recommends strategies for mitigating risks to National Security
- Prepares FOCI assessments, which recommend the appropriate mitigation tool for each case, including assessments for all Committee on Foreign Investment in the United States (CFIUS) cases involving DCSA equities
- Determines the need for a National Interest Determination (NID) under a Special Security Agreement (SSA)
- Participates in annual meetings with the cleared contractor under a FOCI mitigation agreement

FOCI rollover text: Foreign Ownership, Control, or Influence

International Programs popup text:

International Programs

International Programs

- Oversees involvement with foreign governments, foreign contractors, and the North Atlantic Treaty Organization (NATO)
- Carries out NATO inspections
- Assists with security review actions
- Reviews Transportation Plans
- Validates security assurances
- Issues NATO FCLs and oversees the DoD NATO Direct-Hire program

FCLs rollover text: Facility Clearances

Assessment and Evaluations popup text:

Assessment and Evaluations (A&E)

Assessment and Evaluations (A&E)

- Monitors contractors for changes impacting contractor FCLs
- Analyzes, 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

FCLs rollover text: Facility Clearances

Special Programs popup text:

Special Programs

Special Programs

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

DCSA Counterintelligence

Narrator: DCSA Counterintelligence, or CI, also provides support to field elements and cleared contractors. DCSA CI receives suspicious contact reports, or SCRs, oversees CI awareness and reporting, and, along with field elements, performs advise and assist visits and assists with security review actions.

To learn more, see the DCSA CI website. Select VIEW to access this website from a list of Course Resources.

Screen text:

DCSA Counterintelligence (CI)

- Receives suspicious contact reports (SCRs)
- Oversees CI awareness and reporting
- Along with field elements, performs advise and assist visits
- Along with field elements, assists with security review actions

Field elements rollover text: ISFO Industrial Security Field Operations

Defense Vetting Directorate (DVD)

Narrator: The Defense Vetting Directorate, or DVD, establishes a holistic end-to-end personnel vetting enterprise for processing personnel clearances, or PCL.

DVD also includes the continuous evaluation, or CE, program, which reviews the background of a cleared individual at any time during the period of eligibility and the insider threat program, which oversees the mitigation of insider threats to DoD.

To learn more, see the DCSA DVD website. Select VIEW to access this website from a list of Course Resources.

Screen text:

Defense Vetting Directorate (DVD)

- Establishes a holistic end-to-end personnel vetting enterprise for processing personnel clearances (PCL)
- Reviews the background of a cleared individual at any time during the period of eligibility
- Oversees the mitigation of insider threats to DoD

DCSA Mission Areas: SETA

Narrator: As you just saw, DCSA performs a variety of critical functions as CSO. DCSA'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 DCSA CDSE website. Select VIEW to access this website from a list of Course Resources.

Screen text:

Center for Development of Security Excellence (CDSE)

- Mission: Professionalization of the security community
- Provides security education and training for DoD and industry

GCA Role and Responsibilities

Narrator: Remember that, although DCSA 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 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.

Screen text:

GCA Contracting Responsibilities

- Issues the contract for classified work
  - Includes the FAR Security Requirements clause
- Provides contract-specific guidance
  - DD Form 254
  - Classification/declassification guidance

FAR rollover text:	Federal Acquisition Regulation
GCA rollover text:	Government Contracting Activity

Other GCA Responsibilities

- Sponsors facilities for FCLs
- Ensures the OCA conducts damage assessments in the case of loss/compromise/suspected compromise
- Provides education and training for embedded contractors

FCLs rollover text:	Facility Clearances
OCA rollover text:	Original Classification Authority

The designation of a CSA does not relieve the GCA of its NISP responsibilities.

Introduction to Individual Roles and Responsibilities

Screen text: Individual Roles and Responsibilities

Narrator: As you have already seen, in order to protect classified information, government agencies, including the GCA who issued the classified contract, DCSA 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, DCSA employees have a range of key responsibilities in implementing the NISP. These employees include IS Reps, Information System Security Professionals/Security Control Assessors, or ISSP/SCAs, Counterintelligence Special Agents, or CISAs, and other Industrial Security Headquarters Personnel.

Finally, on the contractor side, Facility Security Officers, or FSOs, oversee the day-to-day operation of the contractor's security program. Insider Threat Program Senior Officials, or ITPSOs, are responsible for establishing and maintaining a contractor's effective insider threat program, and Information System Security Managers, or ISSMs, are responsible for managing information system security.

Screen text:

CISA rollover text: Counterintelligence Special Agent

FSO rollover text: Facility Security Officer

IS Rep rollover text: Industrial Security Representative

ISSM rollover text: Information System Security Manager

ISSP/SCA rollover text: Information System Security Professional/Security Control Assessor

ITPSO rollover text: Insider Threat Program Senior Official

GCA Employees

Narrator: 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 between the GCA and DCSA will identify specific responsibilities.

If DCSA retains responsibility, then the National Industrial Security Program Operating Manual, or NISPOM, applies; if the GCA retains responsibility, the DoD policy applies.

Screen text:

DoD Security Specialist/Activity Security Manager

- Maintains cognizance over industrial security functions
- Reviews, at a minimum, and may complete the DD Form 254
- Receives security violation/administrative inquiry reports in cases of loss, compromise, or suspected compromise

Conducts security inspections

MOA/MOU identifies GCA and DCSA responsibilities

MOA/MOU rollover text: Memorandum of Agreement/Memorandum of Understanding

DCSA Employees

Narrator: As CSO for DoD, DCSA 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.

IS Reps are DCSA employees and are located throughout the country. They serve as the contractor's primary point of contact for security matters; ISSPs/SCAs work with IS Reps and contractor personnel on all matters related to the authorization and maintenance of authorized contractor information systems.

Each geographic region has a Region 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 DCSA operational elements as well as cleared contractors in a wide range of security areas. Select each role to learn more.

Screen text:

Select each role to see a detailed list of responsibilities.

IS Rep

- Serves as primary contact for security

IS Rep rollover text: Industrial Security Representative

CI Personnel (CI Chief and CISA)

- Offers CI advice, oversight, and training

CI rollover text: Counterintelligence
CISA rollover text: Counterintelligence Special Agent

ISSP/SCA

- Oversees IS use and maintenance

ISSP/SCA rollover text: Information System Security Professional/Security Control Assessor

Headquarters Personnel

- Support DCSA Operational Elements and cleared contractors

IS Rep popup text:

IS Rep

Major IS Rep Responsibilities

- Works closely with the FSO to provide advice, assistance, and oversight
- Conducts facility orientation actions before issuance of FCLs
- Conducts security review actions of the contractor's security program
- Coordinates with other entities within DCSA to oversee all aspects of contractor security, including
    - FOCI
    - International security
    - Authorized information systems
    - Special programs (e.g., SAP, AA&E)
- Receives reports of security violations from FSO
    - Conducts administrative inquiries, when appropriate
- Reports security violations to GCA

FSO rollover text: Facility Security Officer
FCLs rollover text: Facility Clearances
DCSA rollover text: Defense Counterintelligence and Security Agency
FOCI rollover text: Foreign Ownership, Control, or Influence
SAP rollover text: Special Access Programs
AA&E rollover text: Arms, Ammunition, and Explosives
GCA rollover text: Government Contracting Activity

CI Personnel (CI Chief and CISA) popup text:

CI Personnel (CI Chief and CISA)

Major CI Personnel Responsibilities
CISAs work with FSOs to:

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

CISAs work with IS Reps to:

- Conduct advise and assist visits
- Provide advice and guidance regarding CI best practice
- Help conduct security review actions

CI rollover text: Counterintelligence
FSOs rollover text: Facility Security Officers
IS Reps rollover text: Industrial Security Representatives

ISSP/SCA popup text:

ISSP/SCA

Major ISSP/SCA Responsibilities

- Works with IS Reps, FSOs, and ISSMs on all matters related to the maintenance of authorized classified contractor information systems
- Performs assessments of classified information systems and critical program unclassified information systems
- Participates in security review actions of facilities with authorized classified information systems and/or critical program unclassified information systems
    - Evaluates vulnerabilities
    - Identifies potential cyber security threats
    - Helps develop mitigation strategies
- Responds to security violations involving authorized classified information systems
- Develops and maintains technical proficiency of ever-changing technology

developments IS Reps rollover text: Industrial Security Representatives

FSOs rollover text: Facility Security Officers
ISSMs rollover text: Information System Security Managers

Headquarters Personnel popup text:

Headquarters Personnel

Major Headquarters Personnel Responsibilities

- Headquarters personnel support various DCSA operational elements and cleared contractors with security related functions.

DCSA rollover text: Defense Counterintelligence and Security Agency

Contractor Employees

Narrator: At contractor facilities, individuals in three roles are primarily responsible for overseeing the NISP: the FSO, the ITPSO, and the 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 ITPSO works closely with the FSO to establish and maintain an insider threat program and ensures that the program is effective and in compliance with insider threat requirements.

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

Select the FSO, ITPSO and ISSM to learn more.
Screen text:

Select the FSO, ITPSO or ISSM to see a detailed list of their responsibilities.

<u>FSO</u>

FSO

- Administers and oversees the security program
- Ensures NISP compliance
- Follows NISPOM Guidelines
- Ensures continued compliance with DD 441 responsibilities

FSO rollover text: Facility Security Officer

ITPSO

ITPSO

- Establish and maintain an insider threat program
- Ensures program is effective and in compliance with insider threat requirements

ITPSO rollover text: Insider Threat Program Senior Official

ISSM

ISSM

- Works closely with the FSO
- Manages contractor-owned information systems
- Ensures ISS requirements are met

ISSM rollover text:	Information System Security Manager
ISS rollover text:	Information System Security

FSO popup text:

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 DCSA 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 and unclassified information related to a classified contract
- Reporting to the government
- Self-inspections

ITPSO popup text:

ITPSO

Major ITPSO Responsibilities

ITPSO responsibilities include, but are not limited to:

- Provide management, accountability, and oversight to effectively implement and manage the requirements of the NISPOM related to insider threat.

- Report relevant and credible information coming to their attention regarding cleared employees. Such reporting includes information indicative of a potential or actual insider threat that is covered by any of the 13 personnel security adjudicative guidelines.
- Provide internal training for insider threat program personnel and cleared personnel that satisfies insider threat training requirements.

ISSM popup text:

ISSM

Major ISSM Responsibilities
ISSM responsibilities include, but are not limited to:

- Information Systems 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.)

Knowledge Check

Review Activity 1

Narrator: Now, check your understanding.

Screen text:
Which of these are DCSA responsibilities or functions? Select all that apply.

□ Provide security, education, and training
□ Assess, authorize, and oversee information systems
□ Provide contract-specific classification guidance
□ Fund contractor background investigations

Answer Key:
✓ Provide security, education, and training
✓ Assess, authorize, and oversee information systems
□ Provide contract-specific classification guidance

- ✓ Fund contractor background investigations

Review Activity 2

Narrator: Now try this one.

Screen text:
Identify the role described by each statement; then select Submit.

This DCSA employee serves as the contractor’s primary point of contact for security.

- ○ ITPSO
- ○ ISSP/SCA
- ○ FSO
- ○ ISSM
- ○ IS Rep

This DCSA employee oversees authorized contractor information system use.

- ○ ITPSO
- ○ ISSP/SCA
- ○ FSO
- ○ ISSM
- ○ IS Rep

This contractor employee administers and oversees the contractor security program.

- ○ ITPSO
- ○ ISSP/SCA
- ○ FSO
- ○ ISSM
- ○ IS Rep

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

- ○ ITPSO
- ○ ISSP/SCA
- ○ FSO
- ○ ISSM
- ○ IS Rep

This contractor employee implements and manages the requirements of the NISPOM related to insider threat.

- ○ ITPSO
- ○ ISSP/SCA
- ○ FSO
- ○ ISSM
- ○ IS Rep

Answer Key

This DCSA employee serves as the contractor’s primary point of contact for security.

- ○ ITPSO
- ○ ISSP/SCA
- ○ FSO
- ○ ISSM
- ● IS Rep

This DCSA employee oversees authorized contractor information system use.

- ○ ITPSO
- ● ISSP/SCA
- ○ FSO
- ○ ISSM
- ○ IS Rep

This contractor employee administers and oversees the contractor security program.

- ○ ITPSO
- ○ ISSP/SCA
- ● FSO
- ○ ISSM
- ○ IS Rep

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

- ○ ITPSO
- ○ ISSP/SCA
- ○ FSO
- ● ISSM
- ○ IS Rep

This contractor employee implements and manages the requirements of the NISPOM related to insider threat.

- ● ITPSO
- ○ ISSP/SCA
- ○ FSO
- ○ ISSM
- ○ IS Rep

Lesson Summary

Narrator: You have completed the lesson “NISP Roles and Responsibilities.” Select the Student Guide to review or select the forward arrow to move on.

Screen text:

You have completed the lesson "NISP Roles and Responsibilities"

To review, select the Student Guide or select the forward arrow to choose your next lesson.

Course Conclusion

Course Summary

Narrator: 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

Narrator: Here is a list of the lessons in the course. Select Student Guide to review any lesson.

Screen text:

Lessons

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

Select Student Guide to review any lesson.

Course Objectives

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

To receive course credit, you MUST take the Industrial Security Basics examination.

Follow the instructions on screen to access the online exam.

Screen text:

Industrial Security Basics
You should now be able to:

- ✓ 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 take the online exam.