Student Guide

Industrial Security Databases and Systems

Lesson 1: Course Introduction

Contents

Introduction

Welcome

U.S. industry develops and produces the majority of our nation's technology—much of which is classified. The National Industrial Security Program (NISP) was established as a partnership between government and industry to ensure that cleared industry contractors safeguard classified information in their possession while performing government work. In this course, you will learn about the databases and information systems that support the NISP and its goals of protecting classified information.

Welcome to the *Introduction to Industrial Security Databases and Systems* course.

Objectives

Here are the course objectives. Take a moment to review them.

- Identify the primary databases and systems used to support the NISP
- Identify the purpose and use of each database or system
- Identify who has access to each database or system

Student Guide

Industrial Security Databases and Systems

Lesson 2: Overview of NISP Databases and Systems

Contents

Introduction

Objectives

Recall that the purpose of the NISP is to protect classified information entrusted to industry. In this lesson, you will learn about the role that information systems play in the NISP, and you will be introduced to the primary systems and databases used to support the NISP.

Here are the lesson objectives. Take a moment to review them.

- Identify the primary databases and systems used to support the NISP
- Describe the role of information systems in the NISP

Information Systems and the NISP

What is the NISP?

Established by Executive Order 12829, the National Industrial Security Program (NISP) was created to ensure the protection of classified information entrusted to industry contractors performing work on sensitive government contracts, programs, bids, and research and development efforts. The NISP defines the requirements, restrictions, and other safeguards that are used to protect classified information entrusted to industry. The NISP applies to all Executive Branch departments and agencies and to contractors within the U.S. and its territories that require access to classified information. As essential support components of the NISP, information systems and databases provide the means to collect, store, and facilitate analysis of information and data to support the overall purpose of the NISP.

Introduction to IS in the NISP

A variety of systems and databases are available to support the Defense Security Service (DSS) and the NISP. In this course, we will look at 13 of them—some owned and managed by DSS for use within the NISP, and some owned and managed by other federal agencies for use by contractors and agencies across the federal government.

The systems and databases we will learn about in this course fall into three general categories. First, we will discuss the systems and databases that support personnel security and assurance. Then we will discuss the systems and databases that support the facility clearance process. And finally, we will discuss four additional systems that support other functions of the NISP.

The systems and databases in each category will be covered in later lessons and are listed in the sections that follow.

Personnel Security and Assurance

These systems support personnel security and assurance:

- Electronic Questionnaires for Investigations Processing (e-QIP)
- Secure Web Fingerprint Transmission (SWFT)
- Defense Central Index of Investigations (DCII)
- Joint Personnel Adjudication System (JPAS)

Facility Clearance

These systems support facility clearances:

- Electronic Facility Clearance System (e-FCL)
- Industrial Security Facilities Database (ISFD)
- National Industrial Security Program (NISP) Contract Classification System (NCCS)

Other Systems

These systems support other functions of the NISP:

- National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ODAA Business Management System (OBMS)
- Security Training, Education and Professionalization Portal (STEPP)
- System for Award Management (SAM)

Review Activity

Review Activity

Which of the following is a purpose of information systems and databases used in the NISP?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Define the requirements that protect classified information
- ☐ Facilitate analysis of information and data
- ☐ Collect information and data
- ☐ Store information and data

Conclusion

Lesson Summary

You have completed the lesson *Overview of NISP Databases and Systems*.

Answer Key

Review Activity

Which of the following is a purpose of information systems and databases used in the NISP?

- ☐ Define the requirements that protect classified information
- ☑ Facilitate analysis of information and data (correct response)
- ☑ Collect information and data (correct response)
- ☑ Store information and data (correct response)

***Feedback**: Databases and systems used in the NISP collect, store, and facilitate the analysis of information and data to support the purpose of the NISP. The NISP itself defines the requirements, restrictions, and other safeguards that are used to protect the classified information entrusted to industry.*

Student Guide

Industrial Security Databases and Systems

Lesson 3: Personnel Security and Assurance Databases and Systems

Contents

Introduction

Objectives

Each database and system supporting the NISP serves a specific purpose and is accessible to a specific group of users. In this lesson, we will take a look at the databases and systems that support personnel security and assurance in the NISP.

Here are the lesson objectives.

- Identify the purpose and use of each database or system
- Identify who has access to each database or system

This lesson will review the following databases and systems:

- Electronic Questionnaires for Investigations Processing (e-QIP)
- Secure Web Fingerprint Transmission (SWFT)
- Defense Central Index of Investigations (DCII)
- Joint Personnel Adjudication System (JPAS)

Electronic Questionnaires for Investigations Processing (e-QIP)

Overview

The first system we will look at related to personnel security and assurance is the Electronic Questionnaires for Investigations Processing (e-QIP). Developed and owned by the U.S. Office of Personnel Management, Federal Investigative Service (OPM-FIS), e-QIP is a secure, automated, web-based system that facilitates the processing of standard investigative forms that are used in background investigations for federal security, suitability, fitness, and credentialing purposes.

What Does It Do?

e-QIP is designed to automate the data collection portion of the investigation request process. It allows users to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to a requesting agency. The types of data stored in e-QIP include:

- Proof of citizenship
- Employment history
- Personal references
- Family member citizenship information
- Aliases
- Employer
- Foreign activities
- Selective Service ID, if applicable

e-QIP houses the Standard Forms for investigations, which users must complete when applying for a background investigation. The specific form that a user must complete depends on the type and scope of the requested background investigation, which in turn depends on the employment position and the access requirements for the position. The Standard Forms for investigations include:

- SF 85: Questionnaire for Non-Sensitive Positions
- SF 85P: Questionnaire for Public Trust Positions
- SF 86: Questionnaire for National Security Positions

Who Uses It?

e-QIP is used by both applicants and agencies. Applicants use it to supply information, and agencies use it to request information.

Applicants

Applicant users are federal and contractor employees who must meet suitability or "fitness" requirements for employment and who require access to federal facilities, automated systems, or classified information.

After completing and submitting the appropriate Standard Form and all required attachments, all applicants must be properly investigated and adjudicated to be issued a credential or the appropriate eligibility required to access classified information.

The benefits that e-QIP provides to applicants include:

- Convenient, secure access to Standard Forms
- Faster data collection and processing
- Data retention
- Easy completion of new forms

Agencies

Agency users include federal and contractor organizations that require employees to be investigated for personnel security or suitability functions. These agencies initiate, manage, and submit new investigation and re-investigation requests to an Investigation Service Provider (ISP), which is a third party agency that conducts the background investigations. The Office of Personnel Management (OPM) is an example of an ISP, as it conducts security and suitability investigations for requesting agencies.

The benefits of e-QIP to the requesting agencies include:

- Less review time
- Lower rejection rates due to e-QIP validation tables

- Faster scheduling
- Easier re-investigation due to data retention
- Report generation for tracking and analyzing requests
- Reduced mail costs

Summary

What?	Description
What is it?	• Secure, automated, web-based system that facilitates the processing of standard investigative forms used in background investigations
What does it do?	• Automates data collection for background investigations • Allows users to electronically submit personal data to a requesting agency • Houses Standard Forms for investigations
Who uses it?	• Applicants • Agencies

e-QIP Resources

These e-QIP resources are available on the Course Resources page:

- e-QIP website
- e-QIP Quick Reference Guide
- e-QIP Web-Based Training: Investigative Forms and e-QIP Overview

Secure Web Fingerprint Transmission (SWFT)

Overview

The next system we will look at related to personnel security and assurance is the Secure Web Fingerprint Transmission (SWFT). Managed and operated by the Defense Manpower Data Center (DMDC) Personnel Security/Assurance (PSA) Division, SWFT is a web-based system that enables cleared Defense industry users to submit electronic fingerprints, or e-fingerprints, and demographic information for applicants who require an investigation by OPM for a personnel security clearance.

What Does It Do?

SWFT was developed to streamline the process and traceability of e-fingerprint submissions. Previously, the paper-based capture, submission, and processing of fingerprints was time-consuming and prone to errors. By eliminating the manual paper process, SWFT expedites the clearance process and provides end-to-end accountability for personally identifiable information (PII).

Who Uses It?

SWFT is used primarily by industry and military users to process fingerprints as part of a background investigation. NISP contractors submit e-fingerprints to support e-QIP submissions that have been approved by the Personnel Security Management Office for Industry (PSMO-I). E-fingerprints that meet the acceptance criteria defined by the agency authorizing the investigation and OPM are then transmitted to the Federal Bureau of Investigation.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

DSS does not provide fingerprinting assistance or review fingerprint submissions; rather, the DSS role in SWFT is to ensure that fingerprints are promptly submitted for key management personnel (KMP) at facilities being processed for new facility clearances. If fingerprints are not submitted within 14 days of submission of the SF-86, then the FCL process will be discontinued.

Summary

What?	Description
What is it?	• Web-based system that allows users to submit e-fingerprints and demographic information for PCL applicants
What does it do?	• Streamlines the e-fingerprint submissions process • Expedites clearance process and provides accountability for PII
Who uses it?	• Industry and military users processing fingerprints as part of background investigation

SWFT Resources

These SWFT resources are available on the Course Resources page:

- Defense Manpower Data Center (DMDC) website
- SWFT Webinar, March 2015
- SWFT Access, Registration, and Testing Procedures
- Electronic Fingerprint Capture Options for Industry

Defense Central Index of Investigations (DCII)

Overview

The next system we will look at related to personnel security and assurance is the Defense Central Index of Investigations, or DCII. Operated and maintained by the Defense Manpower Data Center (DMDC) on behalf of the DoD components and the Office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence and Security, DCII is an automated central index that catalogs investigations,

including criminal investigations, conducted by DoD investigative agencies as well as personnel security determinations made by DoD adjudicative authorities.

Who Uses It and Why?

DCII is used by adjudicators and DSS Personnel Security Management Office for Industry (PSMO-I) Security Specialists to check for derogatory information during the initial review of an e-QIP application, which is conducted to grant interim security clearance eligibility. It is also used by the Facility Clearance Branch (FCB) to check for reciprocity of individuals cleared by other government agencies.

Access to DCII is limited to the Department of Defense and other federal agencies that have adjudicative, investigative, and/or counterintelligence missions. Note that industry users do not have access to DCII.

Summary

What?	Description
What is it?	• Automated index that catalogs DoD investigations and personnel security determinations
What does it do?	• Check for derogatory information during initial review of e-QIP application • Check for reciprocity
Who uses it?	• Adjudicators • DSS PSMO-I Security Specialists • Facility Clearance Branch

DCII Resources

These DCII resources are available on the Course Resources page:

- Defense Manpower Data Center (DMDC) website
- DCII Account Management Guide

Joint Personnel Adjudication System (JPAS)

Overview

The final system related to personnel security and assurance is the Joint Personnel Adjudication System (JPAS). Maintained by the JPAS Program Management Office (PMO) with technical support provided by the DMDC Contact Center, JPAS is DoD's system of record for personnel security access and eligibility. More specifically, JPAS is the master repository and centralized processing tool that provides the capability to perform personnel security management of DoD civilian employees, military personnel, and DoD contractors.

JPAS is composed of two subsystems that provide customized user interfaces for two distinct user bases. The Joint Clearance Access and Verification System (JCAVS) is the JPAS interface for the personnel security community, and the Joint Adjudication Management System (JAMS) is the JPAS interface for DoD adjudicators.

The Joint Verification System (JVS) is a future centralized database system that the DoD will adopt as part of its new Defense Information System for Security. JVS will eventually replace JPAS.

JCAVS

The Joint Clearance Access and Verification System (JCAVS) is the JPAS interface for the personnel security community. JCAVS enables DoD security managers and officers to view current access and eligibility information. It also permits users to update personnel security information and security history.

JAMS

The Joint Adjudication Management System (JAMS) is the JPAS interface for DoD adjudicator personnel. JAMS supports the adjudication process by recording eligibility determinations and unclassified investigation comments and by automating the processing of security information records. Note that industry does not have access to JAMS.

What Does It Do?

JPAS is used to submit various personnel change conditions, such as changes in name or marital status, as well as adverse information reports and security violation culpability reports. It stores several types of sensitive information, including personally identifiable information (PII), security clearance levels, and investigation statuses.

Who Uses It?

JPAS is used by both government and industry users. Government users include the PSMO-I, the Facility Clearance Branch, IS Reps, ISSPs, and CI specialists, who use JPAS to determine the eligibility and access of personnel at a cleared facility. For example, these government users might use JPAS to verify that employees performing on classified contracts have the correct eligibility and access to access classified information or secure locations.

Industry users include Facility Security Officers (FSOs) who use JPAS to:

- Process personnel clearance requests
- Grant or remove JPAS access
- Track and process periodic investigations

- Submit adverse information reports, security violation culpability reports, and changes in employee personal information

Note that access is granted only to those who require it to complete their current job duties.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Each service, agency, or contractor determines who will have JPAS access on the organization's behalf. In addition, different users have different access levels. For example, PSMO-I employees have higher access than FCB employees, who have higher access than IS Reps, ISSPs, and CI specialists.

Summary

What?	Description
What is it?	• DoD's system of record for personnel security clearances • Master repository and centralized processing tool for DoD personnel security management • Composed of JCAVS and JAMS
What does it do?	• Submit and adjudicate reports of adverse information and security violations • Stores PII, clearance levels, and investigation statuses
Who uses it?	• Government • Industry

JPAS Resources

These JPAS resources are available on the Course Resources page:

- Defense Manpower Data Center (DMDC) website
- JPAS Account Management Policy

Review Activities

Review Activity 1

Question 1 of 4. This is an automated central index that catalogs investigations and personnel security determinations.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Electronic Questionnaires for Investigations Processing (e-QIP)
- ○ Secure Web Fingerprint Transmission (SWFT)
- ○ Defense Central Index of Investigations (DCII)
- ○ Joint Personnel Adjudication System (JPAS)

Question 2 of 4. This is the master repository and centralized processing tool that enables personnel security management of DoD civilian employees, military personnel, and DoD contractors.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Electronic Questionnaires for Investigations Processing (e-QIP)
- ○ Secure Web Fingerprint Transmission (SWFT)
- ○ Defense Central Index of Investigations (DCII)
- ○ Joint Personnel Adjudication System (JPAS)

Question 3 of 4. This is a secure, automated, web-based system that facilitates the processing of background investigations for security, suitability, fitness, and credentialing purposes.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Electronic Questionnaires for Investigations Processing (e-QIP)
- ○ Secure Web Fingerprint Transmission (SWFT)
- ○ Defense Central Index of Investigations (DCII)
- ○ Joint Personnel Adjudication System (JPAS)

Question 4 of 4. This is a web-based system that enables cleared Defense industry users to submit e-fingerprints and demographic information for applicants for a personnel security clearance.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Electronic Questionnaires for Investigations Processing (e-QIP)
- ○ Secure Web Fingerprint Transmission (SWFT)
- ○ Defense Central Index of Investigations (DCII)
- ○ Joint Personnel Adjudication System (JPAS)

Conclusion

Lesson Summary

You have completed the lesson Personnel Security and Assurance Databases and Systems.

Answer Key

Review Activity 1

Question 1 of 4. This is an automated central index that catalogs investigations and personnel security determinations.

- ○ Electronic Questionnaires for Investigations Processing (e-QIP)
- ○ Secure Web Fingerprint Transmission (SWFT)
- ⦿ Defense Central Index of Investigations (DCII) (correct response)
- ○ Joint Personnel Adjudication System (JPAS)

Feedback*: DCII is an automated central index that catalogs investigations, including criminal investigations, conducted by DoD investigative agencies as well as personnel security determinations made by DoD adjudicative authorities.*

Question 2 of 4. This is the master repository and centralized processing tool that enables personnel security management of DoD civilian employees, military personnel, and DoD contractors.

- ○ Electronic Questionnaires for Investigations Processing (e-QIP)
- ○ Secure Web Fingerprint Transmission (SWFT)
- ○ Defense Central Index of Investigations (DCII)
- ⦿ Joint Personnel Adjudication System (JPAS) (correct response)

Feedback*: JPAS is the master repository and centralized processing tool that provides the capability to perform personnel security management of DoD civilian employees, military personnel, and DoD contractors.*

Question 3 of 4. This is a secure, automated, web-based system that facilitates the processing of background investigations for security, suitability, fitness, and credentialing purposes.

- ⦿ Electronic Questionnaires for Investigations Processing (e-QIP) (correct response)
- ○ Secure Web Fingerprint Transmission (SWFT)
- ○ Defense Central Index of Investigations (DCII)
- ○ Joint Personnel Adjudication System (JPAS)

Feedback*: e-QIP is a secure, automated, web-based system that facilitates the processing of standard investigative forms used in background investigations for federal security, suitability, fitness, and credentialing purposes.*

Question 4 of 4. This is a web-based system that enables cleared Defense industry users to submit e-fingerprints and demographic information for applicants for a personnel security clearance.

- ○ Electronic Questionnaires for Investigations Processing (e-QIP)
- ◉ Secure Web Fingerprint Transmission (SWFT) (correct response)
- ○ Defense Central Index of Investigations (DCII)
- ○ Joint Personnel Adjudication System (JPAS)

***Feedback**: SWFT is a web-based system that enables cleared Defense industry users to submit e-fingerprints and demographic information for applicants who require investigation by OPM for a personnel security clearance.*

Student Guide

Industrial Security Databases and Systems

Lesson 4: Facility Clearance Databases and Systems

Contents

Introduction

Objectives

In this lesson, we will take a look at the databases and systems that support facility clearances in the NISP.

Here are the lesson objectives.

- Identify the purpose and use of each database or system
- Identify who has access to each database or system

This lesson will review the following databases and systems:

- Electronic Facility Clearance System (e-FCL)
- Industrial Security Facilities Database (ISFD)
- National Industrial Security Program (NISP) Contract Classification System (NCCS)

Electronic Facility Clearance System (e-FCL)

Overview

The first system we will look at related to facility clearances is the Electronic Facility Clearance System (e-FCL). Owned and managed by DSS, e-FCL is a web-based application that allows contractors to electronically submit facility information to DSS when applying for a new facility clearance (FCL) or when reporting changed conditions for an existing FCL. It also allows DSS Industrial Security personnel to review and process new FCL applications and changed conditions, which are referred to as “packages.”

Note that e-FCL is based on a similar database owned by the Department of Energy (DoE), which is also a cognizant security agency (CSA) under the NISP. e-FCL shares the same infrastructure and oversight as the DoE system.

What Does It Do?

e-FCL collects and stores various types of facility information that is used in processing and maintaining facility clearances. This includes e-FCL packages, user account information, and administrative information. e-FCL packages include:

- All forms and attachments for an FCL submission
- Business documentation
- A tier parents list and exclusion resolution forms, if applicable

Administrative information stored in e-FCL includes a history of packages for each cleared company and general information, such as the business structure, physical address, and assigned DSS Field Office.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

FCL submissions

Forms and attachments for an FCL include:

- e-FCL summary data sheet
- Key management personnel (KMP) list
- SF-328, Certificate Pertaining to Foreign Interests, and applicable attachments
- DD Form 441, the DoD Security Agreement, or DD Form 441-1, Appendage to the DoD Security Agreement

Business documentation

Business documentation includes bylaws, articles of incorporation, meeting minutes, and stock ledgers. The required business documentation will vary based on type of business structure, such as corporation, LLC, or partnership.

Who Uses It?

e-FCL is used by both government and industry users. On the government side, e-FCL is used widely throughout DSS, most notably by Industrial Security Representatives (IS Reps) and by Industrial Security headquarters personnel, such as those working in Field Operations and in Industrial Policy and Programs. On the industry side, e-FCL can be used by anyone who is designated an e-FCL user, regardless of clearance status. Industry users include e-FCL users and e-FCL administrators, who have permissions to appoint additional users.

Summary

What?	Description
What is it?	• Web-based database application that allows contractors to submit facility information to DSS and allows DSS to review and process FCL packages
What does it do?	• Collects and stores facility information
Who uses it?	• Government o IS Reps o IS Headquarters personnel – Field Operations – Industrial Policy and Programs • Industry o e-FCL User o e-FCL Administrator

e-FCL Resources

These e-FCL resources are available on the Course Resources page:

- Electronic Facility Clearance System
- Electronic Facility Clearance User Guide

Industrial Security Facilities Database (ISFD)

Overview

The next system we will look at related to facility clearances is the Industrial Security Facilities Database (ISFD). Another system owned and managed by DSS, the ISFD is a web-enabled repository of information about cleared contractor facilities in the NISP that are under the cognizance of DSS.

What Does It Do?

The ISFD provides users a nationwide perspective on NISP-related facilities and facilities under DSS oversight in the DoD conventional Arms, Ammunition, and Explosives (AA&E) program. It also provides source data for the DoD Joint Personnel Adjudicative System (JPAS) and the Facility Verification Request (FVR) application. Such source data includes core facility information, such as CAGE codes, FCL levels, and facility addresses.

The ISFD stores various types of facility information, such as security vulnerability assessment results and advice and assistance information. It also stores facility verification requests (FVRs). Some information stored in ISFD can be accessed only by DSS personnel. The ISFD is also used for User Account Management, to send notifications, and to track other special considerations, such as COMSEC custodians.

Who Uses It?

The ISFD has internal users, who have full access, and external users, who have only limited access. Internal users include DSS personnel, such as IS Reps, who use the ISFD to enter and verify current facility information. Internal users also use the ISFD to enter facility actions and to run reports. External users include all registered federal agencies and contractors participating in the NISP. These external users are eligible to access the FVR external user view, which allows them to verify FCL and safeguarding levels, classified and unclassified mailing addresses, and special limitations.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Facility Verification Request

An FVR is the official method of verifying the FCL and the safeguarding capability of a NISP contractor. The ISFD allows users to submit, search, view, edit, and delete FVRs.

Contents of FVR:

- Facility name
- CAGE code
- Physical location
- Classified mailing address
- FCL status/level
- Document safeguarding level
- Special limitations
- FSO name and contact information
- Assigned DSS field office
- Phone number of assigned IS Rep

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Use	Description
Facility Actions	Facility actions include vulnerability assessments, advise and assists, and security violations.
Reports	Reports include assessments due, facilities assigned, and facility locations by city.

Summary

What?	Description
What is it?	• Web-enabled repository of information about DoD cleared contractor facilities
What does it do?	• Provides a nationwide perspective on— o NISP-related facilities o DoD AA&E facilities under DSS oversight • Provides source data for JPAS and FVR • Stores facility information
Who uses it?	• Internal users • External users

ISFD Resources

These ISFD resources are available on the Course Resources page: Industrial Security Facilities Database and ISFD Job Aid.

National Industrial Security Program (NISP) Contract Classification System (NCCS)

Overview

The final system related to facility clearance is the NISP Contract Classification System (NCCS). A coordinated effort between the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)) and DSS, NCCS is an automated web-based system and centralized repository that allows for the collection and querying of DD Form 254, DoD Contract Security Classification Specification, data.

What Does It Do?

NCCS was built as an application on the DoD Wide Area Work Flow (WAWF) e-Business Suite Module. It automates DD Form 254 processes and workflows and allows for the management of security classification specification information. NCCS is used for the creation, review, certification, and management of DD Form 254 and facilitates the processing and distribution of DD Form 254 for contracts requiring access to classified information.

NCCS is accessible to both federal agencies and industry partners in the NISP.

Summary

What?	Description
What is it?	• Automated web-based system and centralized repository that allows for the collection and querying of DD Form 254 data
What does it do?	• Part of DoD WAWF e-Business Suite • Automates DD Form 254 processes • Allows management of security classification specification information
Who uses it?	• Federal agencies • Industry

NCCS Resources

This NCCS resource is available on the Course Resources page: NCCS website.

Note: Basic training will be release at initial operating capability by another entity and will be continually updated as the system matures.

Review Activities

Review Activity 1

Question 1 of 3: This is a web-enabled repository of information about DoD cleared contractor facilities that provides a nationwide perspective on NISP-related facilities.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Electronic Facility Clearance System (e-FCL)
- ○ Industrial Security Facilities Database (ISFD)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

Question 2 of 3: This is an automated web-based system and centralized repository that allows for the collection and querying of DD Form 254 data.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Electronic Facility Clearance System (e-FCL)
- ○ Industrial Security Facilities Database (ISFD)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

Question 3 of 3: This system allows contractors to electronically submit facility information to DSS when applying for new a FCL or when reporting changed conditions for an existing FCL.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Electronic Facility Clearance System (e-FCL) (correct response)
- ○ Industrial Security Facilities Database (ISFD)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

Conclusion

Lesson Summary

You have completed the lesson Facility Clearance Databases and Systems.

Answer Key

Review Activity 1

Question 1 of 3: This is a web-enabled repository of information about DoD cleared contractor facilities that provides a nationwide perspective on NISP-related facilities.

- ○ Electronic Facility Clearance System (e-FCL)
- ⊙ Industrial Security Facilities Database (ISFD) (correct response)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

***Feedback**: The ISFD is a web-enabled repository of information about DoD cleared contractor facilities that provides a nationwide perspective on NISP-related facilities and facilities under DSS oversight in the DoD conventional Arms, Ammunition, and Explosives, or AA&E, program.*

Question 2 of 3: This is an automated web-based system and centralized repository that allows for the collection and querying of DD Form 254 data.

- ○ Electronic Facility Clearance System (e-FCL)
- ○ Industrial Security Facilities Database (ISFD)
- ⊙ National Industrial Security Program (NISP) Contract Classification System (NCCS) (correct response)

***Feedback**: NCCS is an automated web-based system and centralized repository that allows for the collection and querying of DD Form 254 data.*

Question 3 of 3: This system allows contractors to electronically submit facility information to DSS when applying for new a FCL or when reporting changed conditions for an existing FCL.

- ⊙ Electronic Facility Clearance System (e-FCL) (correct response)
- ○ Industrial Security Facilities Database (ISFD)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

***Feedback**: e-FCL allows contractors to electronically submit facility information to DSS when applying for new a FCL or when reporting changed conditions for an existing FCL.*

Student Guide

Industrial Security Databases and Systems

Lesson 5: Additional Databases and Systems

Contents

Introduction

Objectives

In this lesson, we will take a look at some additional databases and systems that support the NISP.

Here are the lesson objectives.

- Identify the purpose and use of each database or system
- Identify who has access to each database or system

This lesson will review the following databases and systems:

- National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ODAA Business Management System (OBMS)
- Security Training, Education and Professionalization Portal (STEPP)
- System for Award Management (SAM)

National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)

Overview

The first system we will look at in this final lesson is the National Industrial Security Program (NISP) Central Access Information Security System (NCAISS). Owned and managed by DSS, NCAISS is a secure web portal that allows users single sign-on access to various DSS applications used in the NISP. Single sign-on access means that users need only one account with a registered CAC or ECA to access all of the systems and services that are integrated within NCAISS.

What Does It Do?

NCAISS is not itself a database and does not store content; rather it is a tool to access other DSS databases and systems that contain content, such as OBMS and STEPP. In addition to providing links to DSS applications, NCAISS is also used to communicate threat advisories. The NCAISS homepage has options to:

- Log in to the DSS Portal
- Register a CAC or ECA
- Enroll

Who Uses It?

Because NCAISS provides single sign-on capability to various DSS systems, it is accessible to all government and industry users requiring access to the component

systems. Government users include DSS IS Reps, DSS ISSPs, DSS CI Special Agents, DSS Industrial Security Headquarters personnel, and other DoD Security Specialists and government entities with Industrial Security responsibilities. Industry users include FSOs and ISSMs.

Summary

What?	Description
What is it?	• Secure web portal that allows single sign-on access to various DSS applications used in the NISP
What does it do?	• Provides single sign-on access to other content-based databases and systems in the NISP • Communicates threat advisories
Who uses it?	• All government and industry users of DSS systems

NCAISS Resources

These NCAISS resources are available on the Course Resources page:

- NCAISS website
- NCAISS User Guide

ODAA Business Management System (OBMS)

Overview

The next system we will look at is the Office of Designated Approving Authority (ODAA) Business Management System (OBMS). Owned and managed by the Industrial Security Field Operations (ISFO) Office of the Designated Approval Authority through the DSS Office of the Chief Information Officer (OCIO), OBMS is a secure, web-based system designed to automate and streamline the information systems Certification and Accreditation (C&A) process for timeliness, accuracy, and efficiency.

What Does It Do?

OBMS is designed to improve Information System Security Managers' (ISSMs') ability to submit and track system security plans (SSPs), produce reports and metrics, and automate the Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) tracking process. It also facilitates the management and monitoring of C&A activities and pushes accreditation information to ISFD. OBMS uses single sign-on capabilities that allow user access with Common Access Card (CAC) authentication or External Certification Authority (ECA).

Who Uses It?

OBMS is used by both government and industry users for various purposes. On the government side, DSS ISSPs use OBMS to track and approve submissions for classified information system accreditation, reaccreditation, changes, and disestablishments. On the industry side, FSOs and ISSMs use OBMS to submit applications for information system accreditation and reaccreditation, submit changes, and request disestablishments.

Summary

What?	Description
What is it?	• Secure, web-based system designed to automate and streamline the information security C&A process
What does it do?	• Improves ISSMs' ability to track and submit SSPs, produce reports, and automate MOU or MOA tracking • Facilitates management and monitoring of C&A activities • Pushes accreditation information to ISFD
Who uses it?	• Government: DSS ISSPs • Industry: FSOs and ISSMs

OBMS Resources

This OBMS resource is available on the Course Resources page: OBMS website.

Security Training, Education and Professionalization Portal (STEPP)

Overview

The next system we will look at is the Security Training, Education and Professionalization Portal (STEPP). Owned and operated by DSS, STEPP is the Center for Development of Security Excellence (CDSE) learning management application that enables users to find training, manage learning, and track professional development in the security disciplines.

What Does It Do?

Used to meet the professional development needs of both internal and external audiences, STEPP contains security education, training, and certification products and services to support the protection of National Security and the professionalization of the DoD security workforce. STEPP contains course schedules, online training courses, details about instructor-led learning activities, performance support tools, and knowledge documents.

It is accessible to both DoD and non-DoD government and industry users within the NISP.

Summary

What?	Description
What is it?	• CDSE's learning management application
What does it do?	• Provides security education, training, and certification products and services • Contains: o Course schedules o Online training courses o Course information o Performance support tools o Knowledge documents
Who uses it?	• Government and industry users within the DoD • Other agencies and contractors within the NISP

STEPP Resources

This STEPP resource is available on the Course Resources page: STEPP website.

System for Award Management (SAM)

Overview

The last system we will look at in this course is the System for Award Management (SAM). Owned and operated by the General Services Administration (GSA), SAM is a secure web portal that consolidates various government acquisition and award capabilities into one overarching system. SAM was designed to streamline processes, eliminate the need to enter the same data multiple times, and consolidate hosting to make the process of doing business with the government more efficient.

SAM is organized into six key functional areas:

- Entity management
- Award management
- Wage data
- Performance information
- Assistance program catalog
- Support

What Does It Do?

SAM changes the way the government does business by merging nine legacy, siloed systems into one and providing users single sign-on access to all the capabilities

previously found in the legacy systems. SAM also consolidates data from these systems into a single database, eliminating data overlap while sharing the data across the award lifecycle. By centralizing and normalizing data, SAM eliminates redundancies, eliminates the need to enter data multiple times in different systems, and provides the flexibility to handle future changes to data. It also consolidates hosting, which in turn reduces operation and maintenance costs while providing improved capability and efficiency.

All federal contractors must be registered with SAM if they want to do business with the federal government, seek out opportunities or assistance programs, or report subcontract information.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

SAM Legacy Systems

SAM merges nine legacy systems into one:

- Central Contractor Registration (CRR)/Federal Agency Registration (FedReg)
- Online Representations and Certifications Application (ORCA)
- Excluded Parties List System (EPLS)
- Electronic Subcontracting Reporting System (eSRS)/ Federal Funding Accountability and Transparency Act (FFATA) Subaward Reporting System (FSRS)
- Catalogue of Federal Domestic Assistance (CFDA)
- FedBizOpps (FBO)
- Wage Determination On Line (WDOL)
- Federal Procurement Data System (FPDS)
- Past Performance Information Retrieval System (PPIRS)/Contractor Performance Assessment Reporting System (CPARS)/Federal Awardee Performance and Integrity Information System (FAPIIS)

Who Uses It?

SAM is used by anyone interested in the business of federal contracting and thus serves multiple user communities, including entities, government contracting and grants officials, and public users searching for government business information.

Note that DSS is included as one specific entity of interest to the industrial security community.

Entities

Entities include:

- Contractors
- Federal assistance recipients
- Potential award recipients
- Loan recipients

- Sole proprietors, corporations, and partnerships
- Businesses
- Federal agencies

Contracting and Grants Officials

Government contracting and grants officials are responsible for the following activities:

- Contracts
- Grants
- Past performance reporting
- Suspension and debarment activities

Public Users

SAM includes data at varying sensitivity levels, so public users may view public information without a SAM account. Public data is available to search and view without having to log in or register for a SAM account.

DSS

The DSS user community uses SAM to:

- Check that facilities are registered
- Check that facility information is correct
- Check that the facility registration is current
- Verify the debarment status of cleared facilities and their KMPs for possible effects on the FCL
- Push facility address data to NCCS
- Search CAGE codes

Summary

What?	Description
What is it?	• Secure web portal that consolidates various government acquisition and award capabilities into one system
What does it do?	• Merges nine legacy systems into one • Provides single sign-on access to all capabilities found previously in the legacy systems • Consolidates data into a single database • Centralizes and normalizes data
Who uses it?	• Entities, including DSS • Government contracting and grants officials • Public users

SAM Resources

These SAM resources are available on the Course Resources page:

- SAM Database
- SAM User Guide
- GSA SAM Overview Briefing

Review Activities

Review Activity 1

Question 1 of 4: This is CDSE's learning management application that enables users to find training, manage learning, and track professional development in the security disciplines.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ○ ODAA Business Management System (OBMS)
- ○ Security Training, Education and Professionalization Portal (STEPP)
- ○ System for Award Management (SAM)

Question 2 of 4: This is a secure web portal that allows users single sign-on access to various DSS applications used in the NISP.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ○ ODAA Business Management System (OBMS)
- ○ Security Training, Education and Professionalization Portal (STEPP)
- ○ System for Award Management (SAM)

Question 3 of 4: This is a secure web portal that consolidates various government acquisition and award capabilities into one overarching system.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ○ ODAA Business Management System (OBMS)
- ○ Security Training, Education and Professionalization Portal (STEPP)
- ○ System for Award Management (SAM)

Question 4 of 4: This is a secure, web-based system designed to automate and streamline the information security Certification and Accreditation process for timeliness, accuracy, and efficiency.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ○ ODAA Business Management System (OBMS)
- ○ Security Training, Education and Professionalization Portal (STEPP)
- ○ System for Award Management (SAM)

Conclusion

Lesson Summary

You have completed the lesson Additional Databases and Systems.

Answer Key

Review Activity 1

Question 1 of 4: This is CDSE's learning management application that enables users to find training, manage learning, and track professional development in the security disciplines.

- ○ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ○ ODAA Business Management System (OBMS)
- ⊙ Security Training, Education and Professionalization Portal (STEPP) (correct response)
- ○ System for Award Management (SAM)

***Feedback**: STEPP is CDSE's learning management application that enables users to find training, manage learning, and track professional development in the security disciplines.*

Question 2 of 4: This is a secure web portal that allows users single sign-on access to various DSS applications used in the NISP.

- ⊙ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) (correct response)
- ○ ODAA Business Management System (OBMS)
- ○ Security Training, Education and Professionalization Portal (STEPP)
- ○ System for Award Management (SAM)

***Feedback**: NCAISS is a secure web portal that allows users single sign-on access to various DSS applications used in the NISP, such as OBMS, ISFD, and STEPP.*

Question 3 of 4: This is a secure web portal that consolidates various government acquisition and award capabilities into one overarching system.

- ○ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ○ ODAA Business Management System (OBMS)
- ○ Security Training, Education and Professionalization Portal (STEPP)
- ⊙ System for Award Management (SAM) (correct response)

***Feedback**: SAM is a secure web portal that consolidates various government acquisition and award capabilities into one overarching system.*

Question 4 of 4: This is a secure, web-based system designed to automate and streamline the information security Certification and Accreditation process for timeliness, accuracy, and efficiency.

- ○ National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)
- ◉ ODAA Business Management System (OBMS) (correct response)
- ○ Security Training, Education and Professionalization Portal (STEPP)
- ○ System for Award Management (SAM)

Feedback*: OBMS is a secure, web-based system designed to automate and streamline the information security Certification and Accreditation process for timeliness, accuracy, and efficiency.*

Student Guide

Industrial Security Databases and Systems

Lesson 6: Course Conclusion

Contents

Course Conclusion

Course Summary

In this course, you learned about the NISP databases and systems that support personnel security and assurance, the facility clearance process, and other NISP functions.

Lesson Review

Here is a list of the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: Overview of NISP Databases and Systems
- Lesson 3: Personnel Security and Assurance Databases and Systems
- Lesson 4: Facility Clearance Databases and Systems
- Lesson 5: Additional Databases and Systems
- Lesson 6: Course Conclusion

Lesson Summary

Congratulations. You have completed the *Industrial Security Databases and Systems* course.

You should now be able to perform all of the listed activities.

- Identify the primary databases and systems used to support the NISP
- Identify the purpose and use of each database or system
- Identify who has access to each database or system

To receive credit for this course, you must take the *Industrial Security Databases and Systems* examination.

Glossary

Industrial Security Databases and Systems

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 12958 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 classify information in the first instance. 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 SERCRET, 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.