Industrial Security Systems and Databases

Course Introduction

Welcome

Narration: U.S. industry develops and produces the majority of our nation's technology — much of which is classified.

The National Industrial Security Program, or 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.

Screen text: Introduction to Industrial Security Databases and Systems

Screen text: Select the Next arrow to proceed.

Objectives

Narration: Here are the course objectives. Take a moment to review them. When you're ready, select the forward arrow to go to the Course Menu.

Screen text: Course Objectives

- Identify the primary databases and systems used to support the National Industrial Security Program (NISP)
- Identify the purpose and use of each database or system
- Identify who has access to each database or system

Overview of NISP Databases and Systems

Objectives

Narration: 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.

Screen text: Lesson Objectives:

- Identify the primary databases and systems used to support the National Industrial Security Program (NISP)
- Describe the role of information systems in the NISP

What is the NISP?

Screen text: Information Systems in the NISP

Narration: Established by Executive Order 12829, the "National Industrial Security Program," or 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.

Screen text: National Industrial Security Program (NISP)

- Created to ensure the protection of classified information entrusted to industry
- Defines requirements, restrictions, and other safeguards used to protect classified information
- Applies to government and contractor entities that require access to classified information

Relies on information systems and databases to collect, store, and facilitate analysis of information and data

Introduction to Information Systems and Databases in the NISP

Narration: A variety of systems and databases are available to support the Defense Security Service, or DSS, and the NISP.

In this course, we will look at 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 additional systems that support other functions of the NISP.
Select each category to see what systems and databases will be covered in the lessons that follow.

Personnel Security and Assurance popup text:

Personnel Security and Assurance

Narration: These systems support personnel security and assurance. Take a moment to review them.

Screen text:

- Electronic Questionnaires for Investigations Processing (e-QIP), or its successor system, electronic Application (eAPP)
- Secure Web Fingerprint Transmission (SWFT)
- Defense Central Index of Investigations (DCII)
- Joint Personnel Adjudication System (JPAS), or its successor system, Defense Information System for Security (DISS)

Facility Clearance popup text:

Facility Clearance

Narration: These systems support facility clearances. Take a moment to review them.

Screen text:

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

Other Systems popup text:

Other Systems

Narration: These systems support other functions of the NISP. Take a moment to review them.

Screen text:

- Enterprise Mission Assurance Support Service (eMASS)
- Security Training, Education and Professionalization Portal (STEPP)
- System for Award Management (SAM)

Review Activity

Narration: Now check your knowledge.

Screen text: Which of the following is a purpose of information systems and databases used in the NIPS? Select all that apply; then select Submit.

Selectable choices:

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

Answer Key:

Which of the following is a purpose of information systems and databases used in the NIPS? Select all that apply; then select Submit.

Selectable choices:

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

Lesson Summary

Screen text: Conclusion

Narration: You have completed the lesson Overview of NISP Databases and Systems. Open the Student Guide to review this lesson or select the forward arrow to proceed.

Screen text: You have completed the Overview of NISP Databases and Systems lesson.
To review, select the Student Guide, or select the forward arrow to proceed to your next lesson.

Personnel Security and Assurance Databases and Systems

Objectives

Screen text: Introduction

Narration: 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. Take a moment to review them.

Screen text: 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), or its successor system, electronic Application (eAPP)
- Secure Web Fingerprint Transmission (SWFT)
- Defense Central Index of Investigations (DCII)
- Joint Personnel Adjudication System (JPAS), or its successor system, Defense Information Systems for Security (DISS)

Overview

Screen text: Electronic Questionnaires for Investigations Processing (e-QIP)

Narration: The first system we will look at related to personnel security and assurance is the Electronic Questionnaires for Investigations Processing, or e-QIP.

Developed and owned by the U.S. Office of Personnel Management, Federal Investigative Service, or 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. This system will be replaced by the electronic Application or eAPP in the future.

Screen text: e-QIP

What is it?

- Secure, automated, web-based system that facilitates the processing of standard investigative forms used in background investigations e-QIP rollover text Electronic Questionnaires for Investigations Processing

What Does It Do?

Narration: 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; and 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 position sensitivity and the eligibility/access requirements for the position.

Screen text:
e-QIP

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

Personal data rollover text:

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

Standard Forms for Investigations rollover text:

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

Who Uses It?

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

Select Applicants and Agencies to learn more.

Screen text: e-QIP

Applicants popup text:

Applicants

Narration: Applicant users are federal and contractor employees who — must meet suitability or "fitness" requirements for employment and who require access to federal facilities, systems, and/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. Take a moment to review the benefits that e-QIP provides to applicants.

Screen text:

- Federal and contractor employees who—
    - Must meet suitability or "fitness" requirements
    - Require access to federal facilities, automated systems, or classified information
- Must complete required Standard Forms and submit required attachments online
- Must be investigated and adjudicated to receive credentials or eligibility

Standard Forms rollover text:

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

Benefits of e-QIP to Applicants

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

Agencies popup text:

Agencies

Narration: 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, or ISP, which is a third party agency that conducts the background investigations.

Take a moment to review the benefits of e-QIP to the requesting agencies.

Screen text:

- Federal agencies and contractors requiring employees to be investigated for personnel security and suitability functions
- Initiate, manage, and submit investigation requests to an Investigative Service Provider (ISP)

Benefits of e-QIP to Agencies

- 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

Narration: Take a moment to review this summary of e-QIP. Select e-QIP Resources to view a list of resources available to you.

Screen text: e-QIP

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

personal data rollover text:

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

Standard Forms for investigations rollover text:

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

Who uses it?

- Applicants
- Agencies

Overview

Screen text: Secure Web Fingerprint Transmission (SWFT)

Narration: The next system we will look at related to personnel security and assurance is the Secure Web Fingerprint Transmission, or SWFT.

SWFT is a web-based system that enables the Department of Defense, or DoD, components and cleared Defense industry users to submit electronic fingerprints, or e-fingerprints, for applicants who require an investigation by NBIB for a personnel clearance (PCL).

Screen text: SWFT

What is it?

- Web-based system that allows users to submit e-fingerprints for PCL applicants

SWFT rollover text: Secure Web Fingerprint Transmission
PCL rollover text: Personnel Clearance

What Does it Do?

Narration: 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, or PII.

Screen text: SWFT

What does it do?

- Streamlines the e-fingerprint submissions process
- Expedites clearance process and provides accountability for PII

PII rollover text: Personally Identifiable Information
Previous System: slow, error-prone
SWFT: fast, accurate

Who Uses It?

Narration: SWFT is used by industry and DoD military and civilian users to process fingerprints as part of a background investigation.

NISP contractors submit e-fingerprints to support security clearance packages that have been reviewed by the Vetting Risk Operations Center, or VROC. E-fingerprints that meet the defined acceptance criteria are then transmitted to the Federal Bureau of Investigation or FBI.

Select More to learn more.

Screen text: SWFT

Who uses it?

- Industry and DoD military and civilian users processing fingerprints as part of background investigation

More popup:

More

DSS does not provide fingerprinting assistance or review fingerprint submissions; rather, DSS ensures that fingerprints are promptly submitted for Key Management Personnel (KMP) at facilities being processed in conjunction with new facility clearances (FCL). If fingerprints are not submitted within 14 days of submission of the SF-86, then the FCL process will be discontinued.

DSS rollover text: Defense Security Service
FCL rollover text: Facility Clearance

Summary

Narration: Take a moment to review this summary of SWFT. Select SWFT Resources to view a list of resources available to you.

Select SWFT Resources to view a list of resources available to you.

Screen text: SWFT

What is it?

- Web-based system that allows users to submit e-fingerprints for PCL applicants

PCL rollover text: Personnel Clearance

What does it do?

- Streamlines the e-fingerprint submissions process
- Expedites clearance process and provides accountability for PII

PII rollover text: Personally Identifiable Information

Who uses it?

- Industry and DoD military and civilian users processing fingerprints as part of the background investigation

Overview

Screen text: Defense Central Index of Investigations (DCII)

Narration**:** 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, or 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 identifies investigations conducted by Department of Defense investigative agencies.

Screen text: DCII

DCII rollover text: Defense Central Index of Investigations

What is it?

- Automated index that catalogs DoD investigations and personnel security determinations

Who Uses it and Why?

Narration: DCII is used by adjudicators and the Vetting Risk Operations Center (VROC) to check for derogatory information throughout the adjudicative process.

It is also used by the Facility Clearance Branch, or 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.

Screen text: DCII

Who uses it?

- Adjudicators
- Vetting Risk Operations Center (VROC)
- Facility Clearance Branch (FCB)

What do they use it for?

- Check for derogatory information during initial review of e-QIP application
- Check for reciprocity

Industry users do not have access to DCII.

Government

- Adjudication
- Investigation
- Counterintelligence

Summary

Narration: Take a moment to review this summary of DCII. Select DCII Resources to view a list of resources available to you.

Screen text: DCII

What is it?

- Automated index that catalogs DoD investigations and personnel security determinations

What is it used for?

- Check for derogatory information throughout adjudicative process
- Check for reciprocity

Who uses it?

- Adjudicators
- Vetting Risk Operations Center
- Facility Clearance Branch

Overview

Screen text: Joint Personnel Adjudication System (JPAS)

Narration: The final system related to personnel security and assurance is the Joint Personnel Adjudication System, or JPAS, which is maintained by the Defense Manpower Data Center, or DMDC. JPAS is DoD's system of record for personnel security access and eligibility.

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

The Defense Information System for Security, or DISS, will eventually replace JPAS. Select JCAVS and JAMS to learn more about each subsystem.

Screen text: JPAS

JPAS rollover text: Joint Personnel Adjudication System

What is it?

- DoD's system of record for personnel security access and eligibility
- Master repository for DoD personnel security management of:
    - DoD civilian employees
    - Military personnel
    - DoD contractors

Select JCVAS and JAMS to learn more.

JCAVS popup text:

JCAVS

Narration: The Joint Clearance Access and Verification System, or JCAVS, is the JPAS subsystem for the personnel security management 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 view eligibility history.

Screen text:
Clearance Access and Verification System (JCAVS)

- JPAS interface for the personnel security community
- Enables DoD security managers/officers to view current eligibility and access information
- Provides ability to update personnel security information and eligibility history

JAMS popup text:

JAMS

Narration: The Joint Adjudication Management System, or 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.

Screen text: Joint Adjudication Management System (JAMS)

- JPAS interface for DoD adjudicator personnel
- Supports adjudication process
- Records eligibility determinations and unclassified investigation comments
- Automates security information records

Industry does not have access to JAMS.

What Does it Do?

Narration: 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, or PII, security clearance levels, and investigation statuses.

Screen text: JPAS

What is it used for?

- Submit changes in personal information that affect a personnel clearance
- Submit reports of adverse information and security violations for adjudication
- Stores sensitive information

Stores:

- PII
- Clearance levels
- Investigation statuses

PII rollover text: Personally Identifiable Information

Who Uses It?

Narration: JPAS is used by both government and industry users.

Government users include VROC, the Facility Clearance Branch, IS Reps, ISSP/SCAs, and CISAs, 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, or FSOs, who use JPAS to: process personnel clearance requests; grant or remove JPAS access; track and process periodic investigations; and 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. Select More to learn more.

Screen text:

Government Users

- VROC, FCB, IS Reps, ISSP/SCAs, and CISAs
- Use JPAS to determine eligibility and access of personnel at cleared facilities

Industry Users

- FSO
- Use JPAS to:
    - Process PCL requests
    - Grant or remove JPAS access
    - Track and process investigations
    - Submit adverse information reports

VROC rollover text:	Vetting Risk Operations Center
FCB rollover text:	Facility Clearance Branch
IS Reps rollover text:	Industrial Security Representatives
ISSP/SCAs rollover text:	Information System Security Professional/Security Control Assessor
CISAs rollover text:	Counterintelligence Special Agent
FSO rollover text:	Facility Security Officer
PCL rollover text:	Personnel Clearance

Access granted only to those whose job duties require it

More popup:

More

Each service, agency, or contractor determines who will have JPAS access on the organization's behalf. In addition, different user accounts have different access levels. For example, VROC employees have higher access than FCB employees, who have higher access than IS Reps, ISSP/SCAs, and CISAs.

Summary

Narration: Take a moment to review this summary of JPAS. Select JPAS Resources to view a list of resources available to you.

Screen text: JPAS

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 is it used for?

- Submit and adjudicate reports of adverse information and security violations
- Stores PII, clearance levels, and investigation statuses

Who uses it?

- Government
- Industry

JCAVS rollover text:	Joint Clearance Access and Verification System
JAMS rollover text:	Joint Adjudication Management System
PII rollover text:	Personally Identifiable Information

Review Activity

Narration: Now, check your knowledge. Match each description to the system it describes.

Screen text:

Question 1 of 4:

This is an automated central index that catalogs investigations and personnel security determinations. Select the best answer; then select Submit.

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

Answer Key

o Electronic Questionnaires for Investigations Processing (e-QIP)
o Secure Web Fingerprint Transmission (SWFT)
✓ Defense Central Index of Investigations (DCII)
o 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 answer; then select Submit.

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

Answer Key

o Electronic Questionnaires for Investigations Processing (e-QIP)
o Secure Web Fingerprint Transmission (SWFT)
o 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 answer; then select Submit.

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

Answer Key

✓ Electronic Questionnaires for Investigations Processing (e-QIP)
o Secure Web Fingerprint Transmission (SWFT)
o Defense Central Index of Investigations (DCII)
o 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 for applicants for a personnel security clearance. Select the best answer; then select Submit.

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

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

Lesson Summary

Screen text: Conclusion

Narration: You have completed the lesson Personnel Security and Assurance Databases and Systems. Open the Student Guide to review this lesson or select the forward arrow to proceed.

Screen text:

You have completed the Personnel Security and Assurance Databases and Systems lesson. To review, select the Student Guide, or select the forward arrow to proceed to your next lesson.

Facility Clearance Databases and Systems

Objectives

Screen text: Introduction

Narration: 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. Take a moment to review them.

Screen text:

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

Overview

Screen text: National Industrial Security System (NISS)

Narration: The first system we will look at related to facility clearances is the National Industrial Security System, or NISS. Owned and managed by DSS, NISS is the system of record for facility clearance information.

NISS is used for facility clearance sponsorship request submissions, facility clearance verifications, facility clearance package submissions, annual self-inspection certifications, reviewing information associated with a facility, and reporting of change conditions, security violations, and suspicious contact reports.

Screen text: NISS

What is it?

- System of record for facility clearances under DSS cognizance
- Applications for new FCLs
- Automates the initial facility clearance workflow
- “One-stop-shop” for activities and interactions with DSS

DSS rollover text:	Defense Security Service
FCL rollover text:	Facility Clearance

Facility - Submit facility information
DSS - Review and process information

What Does It Do?

Narration: NISS collects and stores various types of facility information that is used in processing and maintaining facility clearances. It allows Industry users to review FCL information, requests, communications, and results with DSS in one location. The system also streamlines the FCL business processes.

Additional features include automatic notifications and alerts, the dashboard feature, history of facility security information, reporting features and capabilities, and role based access to information. External Government users can only submit facility verification requests and sponsorship submissions. Select NISS features to find out more.

Screen text: NISS

What does it do:

- Collects and stores facility information
- Provides ability for users to review information
- Streamlines business processes
- Provides Notifications and alerts
- Provides information dashboard
- Includes additional features

NISS Features popup text:

NISS Features

Narration: The NISS provides increased transparency for industry and government stakeholders; the ability for stakeholders to review facility clearance information, requests, communications, and results with DSS in one location; a streamlined business processes, including facility clearance processing; automatic notifications and alerts; a dashboard feature; the ability to monitor and track tasks and view real time facility data; history of the facility information; Single Sign-On (SSO) capabilities; reporting features and capabilities; And, employs role-based access control to information.

Screen text:
NISS Features

- Increased transparency for Industry and Government stakeholders
- Ability for stakeholders to review facility clearance information, requests, communications, and results with DSS in one location
- Streamlined business processes, including facility clearance (FCL) processing
- Automatic notifications and alerts
- Dashboard feature
- Ability to monitor and track tasks and view real time facility data

- History of facility security information
- Utilizes Single Sign-On (SSO) Capabilities
- Reporting features and capabilities
- Role based access to information

Who Uses It?

Narration: NISS is used by external and internal users to include government and industry personnel.

Externally, NISS can be used by Government Contracting Activities or GCAs, Other Government Activities, or OGAs, and Industry Security Staff designated in one or more roles as their job requires. These roles include Facility Clearance Verifier, Sponsor, a member of the Security Staff, and Key Management Personnel, or KMP.

Internally, NISS is used widely throughout DSS, most notably by Industrial Security Representatives, or IS Reps, ISSP/SCAs, CISAs, and the Facility Clearance Branch and by DSS headquarters personnel. Mouse over each of the types of user for more information.

Screen text:

External Users

- Government Contracting Activities (GCA)
- Other Government Activities (OGA)
- Industry Security Staff

Government Contracting Activities (GCA) rollover text:

- Facility Clearance Verifier
- Sponsor

Other Government Activity (OGA) rollover text:

- Facility Clearance Verifier

Industry Security Staff rollover text:

- Facility Clearance Verifier
- Sponsor
- Security Staff
  - Corporate Security Officer
  - Facility Security Officer (FSO)
  - Assistant Facility Security Officer (AFSO)
  - Other Security Staff
- Key Management Personnel (KMP)

Internal Users

- DSS Field Personnel
- DSS Headquarters Personnel

Summary

Narration: Take a moment to review this summary of NISS.

Select NISS Resources to view a list of resources available to you.

Screen text: NISS

NISS rollover text: National Industrial Security System

Screen text:

What is it?

- System of record for facility clearance under DSS cognizance

What does it do?

- Collects and stores facility information
- Automates workflows
- Provides Alerts, Banners, Notifications and a user Dashboard

Who uses it?

- External
- Internal

External rollover text:

- Government Contracting Activity
- Other Government Activity
- Industry Security Staff

Internal rollover text:

- DSS Field Personnel
- DSS Headquarters Personnel

Overview

Screen text: National Industrial Security Program (NISP) Contract Classification System (NCCS)

Narration: The second system related to facility clearances is the NISP Contract Classification System, or NCCS.

A coordinated effort between the Office of the Under Secretary of Defense for Acquisition, and Sustainment or OUSD (A&S), 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.

Screen text:

NCCS

NCSS rollover text: NISP Contract Classification System

Screen text:

What is it?

- Automated web-based system and centralized repository that allows for the collection and querying of DD Form 254 data

DD Form 254 rollover text: DoD Contract Security Classification Specification

What Does It Do?

Narration: NCCS was built as an application on the DoD Procurement Integrated Enterprise Environment or PIEE, 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.

Screen text:

NCSS

NCSS rollover text: NISP Contract Classification System

What does it do?

- Part of DoD PIEE e-Business Suite
- Automates DD Form 254 processes
- Allows management of security classification specification information
- Creation, review, certification, and management of DD Form 254
- Facilitates processing and distribution of DD Form 254

PIEE rollover text: Procurement Integrated Enterprise Environment
DD Form 254 rollover text: DoD Contract Security Classification Specification

Who uses it?

- Federal agencies
- Industry

Summary

Narration: Take a moment to review this summary of NCCS.

Select NCCS Resources to view a list of resources available to you.

Screen text:

NCCS

NCCS rollover text: NISP Contract Classification System

What is it?

- Automated web-based system and centralized repository that allows for the collection and querying of DD Form 254 data

DD Form 254 rollover text: DoD Contract Security Classification Specification

What does it do?

- Part of DoD PIEE e-Business Suite
- Automates DD Form 254 processes
- Allows management of security classification specification information

PIEE rollover text: Procurement Integrated Enterprise Environment
Secure web-based system for electronic invoicing, receipt, and acceptance

Who uses it?

- Federal agencies
- Industry

Review Activity

Narration: Now, check your knowledge. Match each description to the system it describes.

Screen text:

Question 1 of 2:

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 answer, then select Submit.

- ○ National Industrial Security System (NISS)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

Answer Key:

- ○ National Industrial Security System (NISS)
- ✓ National Industrial Security Program (NISP) Contract Classification System (NCCS)

Question 2 of 2:

This is the system of record for facility clearances under DSS cognizance. Select the best answer; then select Submit.

- ○ National Industrial Security System (NISS)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

Answer Key:

- ✓ National Industrial Security System (NISS)
- ○ National Industrial Security Program (NISP) Contract Classification System (NCCS)

Lesson Summary

Screen text: Conclusion

Narration: You have completed the lesson Facility Clearance Databases and Systems. Open the Student Guide to review this lesson or select the forward arrow to proceed.

Screen text: You have completed the Facility Clearance Databases and Systems lesson. To review, select the Student Guide, or select the forward arrow to proceed to your next lesson.

Additional Databases and Systems

Objectives

Screen text: Introduction

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

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

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:

- Enterprise Mission Assurance Support Service (eMASS)
- Security Training, Education and Professionalization Portal (STEPP)
- System for Award Management (SAM)

Overview

Screen text: Enterprise Mission Assurance Support Service (eMass)

Narration: The next system we will look at is the Enterprise Mission Assurance Support Service, or eMASS. The Defense Information Systems Agency, or DISA, established an instance of eMASS for Industry which is owned and managed by the National Industrial Security Program Authorization Office, or NAO. eMASS is a secure, web-based system designed to automate and streamline the information systems Assessment and Authorization, or A&A, process for timeliness, accuracy, and efficiency

Screen text:

eMASS – Fielded by NAO

What is it?

- Secure web-based system designed to automate and streamline the information systems A&A process

eMASS rollover text: Enterprise Mission Assurance Support Service

NAO rollover text: National Industrial Security Program Authorization Office

A&A rollover text: Assessment and Authorization

Ensures:

- Timeliness
- Accuracy
- Efficiency

What Does It Do?

Narration: eMASS is designed to improve Information System Security Managers', or ISSMs', ability to submit and track system security plans, or SSPs, produce reports and metrics, and automate the Interconnection Security Agreement, or ISA, tracking process. It also facilitates the management and monitoring of A&A activities and uses single sign-on capabilities to allow user access with Common Access Card, or CAC, authentication, or External Certification Authority, or ECA.

Screen text:

What does it do:

- Improves ISSMs' ability to submit and track SSPs, produce reports, and automate ISA tracking
- Facilitates management and monitoring of A&A activities

ISSM rollover text: Information System Security Manager
SSP rollover text: System Security Plans
A&A rollover text: Assessment and authorization
CAC rollover text: Common Access Card
ECA rollover text: External Certification Authority
eMASS rollover text: Enterprise Mission Assurance Support Service
NISS rollover text: National Industrial Security System

Who Uses it?

Narration: eMASS is used by both government and industry users for various purposes. On the government side, DSS ISSPs/SCAs use eMASS to track and approve submissions for classified information system authorization, reauthorization, changes, and disestablishments. On the industry side, FSOs and ISSMs use eMASS to submit security authorization packages for information system authorization and reauthorization, submit changes, and request disestablishments.

Screen text:

Government users:

- ISSPs/SCAs
  - Use eMASS to track and approve classified IS authorizations

Industry users

- FSO and ISSMs
  - Use eMASS to submit security authorization packages for IS authorizations

ISSP/SCA rollover text: Information System Security Professional/Security Control Assessor
FSO rollover text: Facility Security Officer
ISSM rollover text: Information System Security Manager
eMASS rollover text: Enterprise Mission Assurance Support Service

Summary

Narration: Take a moment to review this summary of eMASS. Select eMASS Resources to view a list of resources available to you.

What is it?

- Secure web-based system designed to automate and streamline the information systems A&A process

What does it do?

- Improves ISSMs' ability to submit and track SSPs, produce reports, and automate ISA tracking
- Facilitates management and monitoring of A&A activities

Who uses it?

- Government: ISSPs/SCAs
- Industry: FSOs and ISSMs

A&A rollover text: Assessment and Authorization
ISSM rollover text: Information System Security Manager
SSP rollover text: System Security Plans
ISA rollover text: Interconnection Security Agreement
ISSP/SCA rollover text: Information System Security Professional/Security Control Assessor
FSO rollover text: Facility Security Officer

Overview

Screen text: Security Training, Education and Professionalization Portal (STEPP)

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

Screen text:
STEPP

What is it?
CDSE's learning management application

Find training
Manage learning
Track professional development

CDSE rollover text: Center for the Development of Security Excellence
STEPP rollover text: Security Training, Education and Professionalization Portal

What Does it Do?

Narration: 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.

Screen text:
What does it do?

- Contains security education, training, and certification products and services
- Contains:
  - Course schedules
  - Online training courses
  - Course information
  - Performance support tools
  - Knowledge documents

Who uses it?

- Government users (DoD and non-DoD)
- Industry users (DoD and non-DoD)

STEPP

STEPP rollover text: Security Training, Education and Professionalization Portal

Summary

Narration: Take a moment to review this summary of STEPP. Select STEPP Resources to learn more.

Screen text:

STEPP

STEPP rollover text: Security Training. Education and Professionalization Portal

What is it?
CDSE's learning management application

CDSE rollover text: Center for Development of Security Excellence

What does it do?

- Provides security education, training, and certification products and services
- Contains:
    - Course schedules
    - Online training courses
    - Course information
    - Performance support tools
    - Knowledge documents

Who uses it?

- Government and industry users within the DoD
- Other agencies and contractors within the NISP

NISP rollover text: National Industrial Security Program

Overview

Screen text: System for Award Management (SAM)

Narration: The last system we will look at in this course is the System for Award Management, or SAM.

Owned and operated by the General Services Administration, or 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, and support.

Screen text: SAM

SAM rollover text: System for Award Management

What is it?

- Secure web portal that consolidates various government acquisition and award capabilities into one system

Designed to —

- Streamline processes
- Eliminate redundancy
- Consolidate hosting

SAM Functional Areas:

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

What Does It Do?

Narration: SAM changes the way the government does business by merging various 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.

Screen text: <u>SAM</u>

SAM rollover text: System for Award Management

What does it do?

- Merges various 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

Benefits:

- Eliminates redundancy
- Provides flexibility
- Consolidates hosting
- Reduces costs
- Improves capabilities

Must register with SAM to do business with federal government!

Select MORE to learn more.

MORE popup:

MORE

SAM merges various legacy systems into one:

- Central Contractor Registration (CCR)/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?

Narration: 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. Select each user community to learn more.

Screen text:

Who uses it?

- Anyone interested in the business of federal contracting

Entities popup text:

Entities

Narration: Entities include those listed here. Take a moment to review them.

Screen text:

- Contractors
- Federal assistance recipients
- Potential award recipients
- Loan recipients
- Sole proprietors, corporations, and partnerships
- Businesses
- Federal agencies

Contracting and Grants Officials popup text:

Contracting and Grants Officials

Narration: Government contracting and grants officials are responsible for the activities shown here.

Screen text:

Responsible for activities related to —

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

Public Users popup text:

Public Users

Narration: SAM includes data at varying sensitivity levels, so public users may view public information without a SAM account.

Screen text:
Public data is available to search and view without having to log in or register for a SAM account.

DSS popup text:

DSS

Narration: The DSS user community uses SAM to check that facilities are registered, that facility information is correct, and that the facility registration is current. DSS also uses SAM to verify the debarment status of cleared facilities and their KMPs for possible effects on the FCL, to push facility address data to NCCS, and to search CAGE codes.

Screen text:

Uses SAM to —

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

KMP rollover text:	Key Management Personnel
NCCS rollover text:	NISP Contract Classification System
CAGE rollover text:	Commercial and Government Entity

Summary

Narration: Take a moment to review this summary of SAM.

Select SAM Resources to learn more.

What is it?

- Secure web portal that consolidates various government acquisition and award capabilities into one system

What does it do?

- Merges various 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

Review Activity

Narration: Now, check your knowledge. Match each description to the system it describes.

Screen text:

Question 1 of 3:
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 answer; then select Submit.

○ Enterprise Mission Assurance Support Service (eMASS)
○ Security Training, Education and Professionalization Portal (STEPP)
○ System for Award Management (SAM)

Answer Key:
○ Enterprise Mission Assurance Support Service (eMASS)
✓ Security Training, Education and Professionalization Portal (STEPP)
○ System for Award Management (SAM)

Question 2 of 3:
This is a secure web portal that consolidates various government acquisition and award capabilities into one overarching system. Select the best answer; then select Submit.

○ Enterprise Mission Assurance Support Service (eMASS)
○ Security Training, Education and Professionalization Portal (STEPP)
○ System for Award Management (SAM)

Answer Key:
○ Enterprise Mission Assurance Support Service (eMASS)
○ Security Training, Education and Professionalization Portal (STEPP)
✓ System for Award Management (SAM)

Question 3 of 3:
This is a secure, web-based system designed to automate and streamline the information security Assessment and Authorization (A&A) process for timeliness, accuracy, and efficiency. Select the best answer; then select Submit.

- o Enterprise Mission Assurance Support Service (eMASS)
- o Security Training, Education and Professionalization Portal (STEPP)
- o System for Award Management (SAM)

Answer Key:

- ✓ Enterprise Mission Assurance Support Service (eMASS)
- o Security Training, Education and Professionalization Portal (STEPP)
- o System for Award Management (SAM)

Lesson Summary

Screen Text: Conclusion

Narration: You have completed the lesson Additional Databases and Systems. Open the Student Guide to review this lesson, or select the forward arrow to proceed.

Screen text: You have completed the Additional Databases and Systems lesson. To review, select the Student Guide, or select the forward arrow to proceed to your next lesson.

Course Conclusion

Course Summary

Narration: 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.

Screen text: National Industrial Security Program (NISP)

Lesson Review

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

Screen text:

Lessons

- 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

NISP rollover text: National Industrial Security Program

Select Student Guides to review any lesson.

Lesson Summary

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

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

To receive credit for this course, you must take the Industrial Security Databases and Systems examination. Follow the instructions on screen to access the online exam.
Screen text:
Industrial Security Databases and Systems

You should now be able to—

- ☑ Identify the primary databases and systems used to support the National Industrial Security Program (NISP)
- ☑ Identify the purpose and use of each database or system
- ☑ Identify who has access to each database or system

To receive course credit, you must take the Industrial Security Databases and Systems examination. Please use the STEPP system from the Center for Development of Security Excellence to take the exam.