DSS SECURITY RATING PROCESS

IS036.16

This four lesson course is intended to provide a thorough understanding of how the DSS Security Vulnerability Assessment Rating Matrix is used to standardize and improve consistency of the Security Rating process.
Estimated time to complete: 90 minutes

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.

Student Guide

DSS Security Rating Process - IS036.16

Table of Contents

Course Information 3

Course Objectives 3

Course Structure 3

Slide 1: Course Welcome 4

Slide 2: Introduction 4

Slide 4: Course Objective 4

Slide 5: Glossary 4

Slide 6: Standardized Rating Process 6

Slide 7: Security Rating 6

Slide 8: Published Standards 6

Slide 9: Five Possible Ratings 6

Slide 10: Lesson 1 - The Rating Matrix 7

Slide 11: Lesson 1 Objective 7

Slide 12: Rating Matrix 7

Slide 14: Category Codes 7

Slide 15: Starting & Final Scores 7

Slide 17: Vulnerability = Points Lost 8

Slide 19: Multiple Occurrences 8

Slide 20: Corrected on the Spot (COS) 8

Slide 22: Enhancement = Points Added 8

Slide 23: NISP Enhancements 9

Slide 24: Security Rating 9

Slide 25: Red Flags 10

Slide 26: Lesson 1 Summary 10

Slide 27: Knowledge Check Lesson 1 11

Slide 28: Lesson 2: Types of Vulnerabilities 11

Slide 29: Lesson 2 Objectives 11

Slide 30: Vulnerabilities 11
Slide 32: Isolated Acute/Critical Vulnerabilities 12
Slide 33: Systemic Acute/Critical Vulnerabilities 12
Slide 34: Repeat Acute/Critical Vulnerabilities 13
Slide 35: Vulnerabilities - Non-Acute/Non-Critical 14
Slide 36: Red Flag Areas 14
Slide 37: Lesson 2 Summary 14
Slide 38: Knowledge Check Lesson 2 15
Slide 39: Lesson 3: NISP Enhancements 15
Slide 40: Lesson 3 Objectives 15
Slide 41: NISP Enhancements 16
Slide 42: Enhancements 16
Slide 43: Parent/Home Office Enhancements 18
Slide 44: Validation 19
Slide 45: Best Practices 19
Slide 46: Examples 19
Slide 51: Lesson 3 Summary 20
Slide 52: Knowledge Check Lesson 3 20
Slide 53: Lesson 4: Security Review Follow-Up Actions 22
Slide 54: Lesson 4 Objective 22
Slide 55: Formal Exit Briefing 22
Slide 58: Security Review Results Letter 22
Slide 59: Rating Matrix 23
Slide 60: Follow-Up Actions 23
Slide 61: Lesson 4 Summary 23
Slide 62: Knowledge Check Lesson 4 23
Slide 63: Course Summary 24
Slide 64: Course Completion 24
Answer Key 25

Student Guide

DSS Security Rating Process - IS036.16

Course Information

Purpose	Provide a thorough understanding of how the DSS Security Vulnerability Assessment Rating Matrix, more commonly referred to as the Rating Matrix, is used to standardize and improve consistency of the security rating process.
Audience	Facility Security Officers (FSOs) at cleared DoD contractor facilities participating in the NISP, other contractor security personnel, DSS Industrial Security Representatives, and DoD Industrial Security Specialists
Complete/Incomplete	64 slides
Estimated completion time	90 minutes

Course Objectives

Here are the course objectives:

- Describe how the Rating Matrix is used to determine a contractor's security posture following a DSS Security Review.
- Define the different types of security vulnerabilities identified during a security review
- Describe Red Flag areas
- Describe NISP Enhancements
- Explain the intent of each NISP Enhancement
- Compare and contrast NISP Enhancements and Best Practices
- Summarize the Security Review process as it relates to the Rating Matrix and follow-up actions

Course Structure

This course is organized into the lessons listed here:

Introduction
Lesson 1 - The Rating Matrix
Lesson 2 - Vulnerabilities
Lesson 3 - NISP Enhancements
Lesson 4 - Security Review Follow-Up Actions

Student Guide

DSS Security Rating Process - IS036.16

Slide 1: Course Welcome

Welcome to the Defense Security Service (DSS) Security Rating Process online course.

Slide 2: Introduction

DSS administers the NISP on behalf of the Department of Defense (DoD) and other Federal agencies that have agreed to receive industrial security services from DoD.

Slide 3: Introduction

DSS provides Government Contracting Activities (GCAs) and foreign governments with assurances that NISP contractors are eligible for access to classified information and have processes and procedures in place to properly safeguard classified information.

One of the primary means of determining and communicating the requisite level of assurance is through the recurring Security Review process.

Slide 4: Course Objective

By the end of this course you should be able to:

- Describe how the DSS Security Vulnerability Assessment Rating Matrix, more commonly referred to as the Rating Matrix, is used to standardize and improve consistency of the security rating process

This course will cover the following four topics:

Lesson 1 - The Rating Matrix
Lesson 2 - Vulnerabilities
Lesson 3 - NISP Enhancements
Lesson 4 - Security Review Follow-Up Actions

Slide 5: Glossary

Before we get started, let's review the definitions of the following terms used within this course. Select a term on the left: the definition will appear in the window on the right.

Cleared NISP Contractor - A National Industrial Security Program (NISP) contractor is defined as any industrial, educational, commercial, or other entity that has been granted a Facility Security Clearance (FCL) by a Cognizant Security Agency (CSA).

DSS Security Review - The DSS Security Review, also called the DSS Security Vulnerability Assessment (SVA), is the continuing process of providing Government Contracting Activities (GCAs) and foreign governments with assurances that NISP contractors are eligible for access to classified information. It depends upon the IS Rep’s knowledge of the security practices and procedures established and maintained by contractors.

One of the primary means of obtaining that knowledge is through the recurring Security Review process. Whenever possible, vulnerability assessment reviews are accomplished as a collaborative effort with the contractor personnel with an emphasis on creating an atmosphere of candor and with open-minded, flexible approach to problem solving within the requirements of the NISP.

Rating Matrix – Formally known as the DSS Security Vulnerability Assessment Rating Matrix Worksheet, the Rating Matrix is a tool developed to create a more standardized process for the assignment of a Security Rating following a Security Review.

The tool is numerically based, quantifiable, and accounts for all aspects of a facility’s involvement in the National Industrial Security Program.

The ‘DSS Rating Matrix and NISP Enhancement Categories’ provides additional information on the process and how it works and can be accessed through the References Tab at the top-right of this course screen.

Security Rating - The NISP contractor’s security posture shall be rated as a result of each Security Review.

This rating is a summary description for DSS purposes of the contractor’s compliance with the requirements of the DoD 5220.22-M, “National Industrial Security Program Operating Manual” (NISPOM), Industrial Security Letters (ISLs), and any other applicable guidance, and the contractor’s effectiveness in protecting classified information from unauthorized disclosure or compromise.

The NISPOM and the Industrial Security Letters (ISLs) can be accessed through the References Tab at the top-right of the course screen.

Vulnerability - A Vulnerability in the National Industrial Security Program (NISP) is described as an instance where it is identified that a contractor is not in compliance with the NISPOM.

A vulnerability will be categorized as Acute Vulnerability, Critical Vulnerability, or Vulnerability (Non-Acute/Non-Critical) depending on the level of threat posed to national security information.

Timely follow-up and resolution of vulnerabilities identified during Security Reviews is critical to DSS oversight of classified information under the NISP. The goal is to mitigate or eliminate vulnerabilities immediately upon identification. It is essential to validate corrective actions taken to ensure full

resolution of identified vulnerabilities.
DSS does not consider the Security Review complete until all identified vulnerabilities are favorably resolved.

Slide 6: Standardized Rating Process

A security rating takes into account all facets of the contractor's security program, from identified vulnerabilities and enhancements to the size and complexity of the program. The Rating Matrix was developed to create a more standardized rating process.

Slide 7: Security Posture

The NISP contractor's security posture and the effectiveness of the contractor's security program are evaluated and rated against published standards and requirements during each Security Review.

Slide 8: Published Standards

A security rating is a summary description for DSS purposes of the contractor's compliance with:

- The requirements of the DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)"
- Industrial Security Letters (ISLs), and
- Any other applicable guidance

The rating also includes the contractor's effectiveness in protecting classified information from unauthorized disclosure or compromise.

Slide 9: Five Possible Ratings

At the conclusion of each Security Review, DSS will assign one of the following five ratings, identified in Industrial Security Letter (ISL) 2006-02:

- Superior
- Commendable
- Satisfactory
- Marginal
- Unsatisfactory

Now let's take a closer look at the Rating Matrix itself.

Slide 10: Lesson 1 - The Rating Matrix

Slide 11: Lesson 1 Objective

At the end of this lesson you should be able to:

- Describe how the Rating Matrix is used to determine a contractor’s security posture following a DSS Security Review

Slide 12: Rating Matrix

The Rating Matrix was designed to:

- Reduce subjectivity in the Security Review process, and
- Provide for a more standardized approach to assigning security ratings

Slide 13: Rating Matrix

The Rating Matrix assigns point values to Vulnerabilities and NISP Enhancements identified during a Security Review.

These points are aggregated to provide a determination regarding the NISP contractor’s security program based upon an incremental scale.

Slide 14: Category Codes

DSS assigns category levels to facilities based on the complexity of a facility.

Facilities that have approved safeguarding capability in place are ranked from category “AA” and descend by size/complexity through categories “A,” “B,” and “C” to category “D.”

Facilities which are not authorized to store classified are category “E.”

Slide 15: Starting & Final Scores

The Starting Score field remains static at 700 points.

All contractor facilities begin the Security Review with a score of 700.

The Final Score field reflects the final points obtained after all data has been populated in the worksheet.

As additions and subtractions are made through the data input, the 700 points adjust accordingly.

Slide 16: Starting & Final Scores

There are two ways to affect the baseline score of 700: through a Vulnerability or an Enhancement.

Slide 17: Vulnerability = Points Lost

If vulnerabilities are identified, points will be deducted.
Difference in point value is due to size and complexity of the security program; the larger the facility, the greater opportunities for vulnerabilities as well as enhancements.

Slide 18: Vulnerability = Points Lost

Vulnerabilities (Non-Acute/Non-Critical) will result in the following deductions for each facility category.

- A 2-point Deduction for categories AA, A, and B
- A 3- point Deduction for categories C, and D, and
- A 4-point Deduction for category E

Acute/Critical Vulnerabilities will result in these following deductions for each category:

- A 14-point Deduction for categories AA, A, and B
- A 17-point Deduction for categories C, and D, and
- A 20- point Deduction for category E

Slide 19: Multiple Occurrences

When the Security Review results in multiple instances of a vulnerability that relates to the same NISPOM reference, only one vulnerability will be cited.
For example:
If a facility has six documents that are missing NISPOM 4-203 Overall Markings, the vulnerability will be deducted once, not six times or once for each document occurrence. However, the 6 instances will be documented and corrective action needs to be taken for each.

Slide 20: Corrected on the Spot (COS)

All vulnerabilities identified by DSS will be documented and points subtracted on the Rating Matrix form to include “Corrected on the Spot (COS).”
A COS describes situations where mitigations are completed for the specific vulnerabilities during the conduct of the Security Review.
It is important to ensure that the steps taken to correct vulnerabilities and measures to prevent recurrence are fully documented.

Slide 21: Corrected on the Spot

For Example:
It was determined that there was no date recorded within JPAS identifying when the SF 312 was signed. Entering the actual date it was signed into JPAS during the Security Review would be considered having it "Corrected on the Spot."

Slide 22: Enhancement = Points Added

The categories in the NISP Enhancement section allow for additional points to be added to the initial 700 point score.

The number of points added is based upon the selected facility category: AA, A, B, C, D, or E. The Final Score and NISP Enhancement fields are updated with each selected enhancement.

Slide 23: NISP Enhancements

In order for an enhancement to be granted, the facility must meet the baseline NISPOM requirements in that area.

Slide 24: Security Rating

Introduction: A security rating is assigned by DSS to indicate the extent by which a contractor's security program meets, exceeds, or fails to meet the requirements of the NISPOM and other applicable industrial security guidance.

The rating is indicative of how effective the security program is and how well it protects classified information from unauthorized disclosure or compromise.

Click on the arrows at the top of the screen or click on the colored bars below to see more information.

Rating Scale: There are five ratings that can be assigned to indicate the contractor's security posture:

- Superior - 800 points & above
- Commendable - 750 to 799 points
- Satisfactory - 650 to 749 points
- Marginal – 600 to 649 points
- Unsatisfactory - 599 points & below

Superior: The Superior security rating is reserved for contractors who have consistently and fully implemented the requirements of the NISPOM in an effective fashion resulting in a superior security posture of the highest caliber compared with other contractors of similar size and complexity.

The contractor must have documented/implemented procedures that heighten security awareness of employees and foster cooperation in the security community.

This rating also requires a sustained high level of management support for the security program and the absence of any serious security issues.

Commendable: The Commendable rating is assigned to contractors who have fully implemented the requirements of the NISPOM in an effective fashion, resulting in an exemplary security posture compared with other Contractors of similar size and complexity. This rating denotes a security program with strong management support and the absence of any serious security issues.

Satisfactory: The Satisfactory rating is the most common rating and denotes that a contractor's security program is in general conformity with the basic requirements of the NISPOM. This rating may be assigned even though there were Vulnerabilities (Non-Acute/Non-Critical) and/or Acute/Critical Vulnerabilities in one or more of the security program elements.

Marginal: The Marginal rating indicates a substandard security program. This rating signifies a serious Acute/Critical Vulnerability in one or more security program areas that could contribute to the eventual compromise of classified information if left uncorrected. The facility's size, extent of classified activity, and inherent nature of the problem are considered before assigning this rating.

Unsatisfactory: An Unsatisfactory rating is assigned when circumstances and conditions indicate that the contractor has lost, or is in imminent danger of losing, their ability to adequately safeguard classified information in their possession or to which they have access.
The Unsatisfactory rating is the most serious security rating.

For more information on ratings, refer to ISL 2006-02 (item 2) found in the References Tab above.

Slide 25: Red Flags

DSS considers some factors as "Red Flag" areas. If a "Red Flag" is identified, the rating calculation score may not be applicable. Some examples of "Red Flags" are discussed in the next lesson.

Slide 26: Lesson 1 Summary

You should now be able to:

- Describe how the Rating Matrix is used in determining a contractor's security posture following a DSS Security Review

Click the right navigation arrow to check your knowledge of these topics.

Slide 27: Knowledge Check Lesson 1

1. The Rating Matrix assigns point values (to be added or subtracted) to determine a Security Rating following a Security Review for which of the following items:
    a. Classification
    b. Vulnerability
    c. Complexity
    d. Enhancement

2. A vulnerability that was Corrected on the Spot (COS) does not cause points to be subtracted on the Rating Matrix Calculation Worksheet.
    a. True
    b. False

3. Regarding the Rating Matrix, which of the following represents the baseline score used to calculate a Security Rating following a Security Review:
    a. 900
    b. 800
    c. 700
    d. Varies depending on the complexity of the contractor's security program

4. Contractors that have fully implemented the requirements of the NISPOM which results in exemplary security posture is an example of which security rating:
    a. Marginal
    b. Commendable
    c. Satisfactory
    d. None of the above

Slide 28: Lesson 2: Types of Vulnerabilities

Slide 29: Lesson 2 Objectives

At the end of this lesson, you should be able to:

- Define the different types of security vulnerabilities identified during a Security Review
- Give examples of "Red Flag" areas

Slide 30: Vulnerabilities

If the NISP Contractor is not in compliance with the NISPOM, DSS will identify the issue as one of the following types of vulnerabilities:

- Acute Vulnerability

- Critical Vulnerability
- Vulnerability (Non-Acute/Non-Critical)

NOTE: All vulnerabilities require mitigation!

Slide 31: Acute and Critical Vulnerabilities

Acute Vulnerabilities place classified information at imminent risk of loss or compromise, or have resulted in the loss or compromise of classified information. Acute Vulnerabilities require immediate corrective action.

Critical Vulnerabilities are instances of NISPOM non-compliance that are serious, or that may foreseeably place classified information at risk of loss or compromise.

Acute and Critical Vulnerabilities are further sub-categorized as either: Isolated, Systemic or Repeat.

Slide 32: Isolated Acute/Critical Vulnerabilities

ISOLATED ACUTE/CRITICAL VULNERABILITY

Click on the arrows at the top of the screen or click on each button on the left to see more information.

Definition

Isolated vulnerabilities are defined as a single occurrence that resulted in, or could logically lead to, loss or compromise of classified information.

Example

The contractor employee was processing classified information on an unaccredited system connected to the Internet.

Example Mitigation Action

Connection was severed immediately; the system was secured in an approved container: DSS was notified and an Administrative Inquiry (AI) was conducted to determine the extent of the loss of classified information. Additional mitigation actions were taken as appropriate.

Slide 33: Systemic Acute/Critical Vulnerabilities

SYSTEMIC ACUTE/CRITICAL VULNERABILITY

Click on the arrows at the top of the screen or click on each button on the left to see more information.

Definition

Systemic vulnerabilities demonstrate defects in a specific subset of the contractor’s industrial security program (e.g., Security Education and Awareness, Information Security) or in the contractor’s overall security program.

A systemic vulnerability could be the result of not having a required or necessary program in place, the result of an existing process not adequately designed to make the program compliant with NISP requirements, or due to the failure to comply with an existing and adequate contractor policy.

Example

The facility ISSO was unable to produce annual automated audit log records in accordance with NISPOM requirements.

Upon further investigation, it was determined that over half of the accredited information systems were not properly configured, resulting in gaps in recorded audit log information for the Information System (IS).

Example Mitigation Action

The ISSO must ensure audit policy settings are configured so the systems are capable of maintaining at least a twelve month period of events. Additional investigation and mitigation actions should be taken as appropriate.

Slide 34: Repeat Acute/Critical Vulnerabilities

REPEAT ACUTE/CRITICAL VULNERABILITY

Click on the arrows at the top of the screen or click on each button on the left to see more information.

Definition

Repeat vulnerabilities are defined as a specific occurrence identified during the last DSS Security Review that has not been properly corrected.

Although some repeat vulnerabilities may relate to a previous vulnerability that was administrative in nature, the failure of the contractor to correct the vulnerability shall be documented as a Critical Repeat Vulnerability.

A failure to correct a previous vulnerability can reasonably be said to demonstrate a disregard for NISPOM compliance or an inability to comply with NISP requirements. This raises questions about the contractor’s security program.

Example

A review of JPAS records disclosed 5 individuals with overdue Periodic Reinvestigations (PRs), they were; J. Smith, R. Brown, S. Johnson, H. Jones, and C. Green.

During the previous DSS Security Review, it was noted that 4 of the named individuals had overdue investigation dates and corrective action was not taken.

Example Mitigation Action

The FSO initiated the Periodic Reinvestigations (PRs) for the 4 identified employees, and established a process to review JPAS on a monthly basis to prevent recurrence.

Slide 35: Vulnerabilities - Non-Acute/Non-Critical

VULNERABILITIES (NON-ACUTE/NON-CRITICAL)

Click on the arrows at the top of the screen or click on each button on the left to see more information.

Definition

Vulnerabilities (Non-Acute/Non-Critical) may be administrative in nature, and do not place classified information at risk of loss or compromise.

Example

The FSO failed to inform employees that the DoD Hotline may be used, if necessary, to report matters of national security significance.

Example Mitigation Action

The FSO will inform the employees by posting DoD Hotline information to ensure all employees are aware of this alternate means to report matters of national security significance.

Slide 36: “Red Flag” Areas

DSS considers some items as a “Red Flag” which may negate the Rating Matrix score. These items may be significant enough to impact the overall facility security clearance status.

- Unreported or unmitigated FOCI
- Acute or Critical Systemic Vulnerabilities with actual loss or the potential for loss or compromise
- Appointment of Key Management Personnel (KMP) without required clearance
- Deliberate disregard for security requirements
- Marginal or Unsatisfactory Matrix score
- Any additional items that may invalidate the FCL

This list is ***not*** all inclusive.

Slide 37: Lesson 2 Summary

You should now be able to:

- Define the different types of security vulnerabilities identified during a security review
- Describe “Red Flag” areas

Click the right navigation arrow to check your knowledge of these topics.

Slide 38: Knowledge Check Lesson 2

1. Match the definition with the specific category of vulnerability.
   - A. Acute Vulnerability
   - B. Critical Vulnerability
   - C. Vulnerability (Non-Acute/Non-Critical)
   - 1) Instances of NISPOM non-compliance that are serious, or that may foreseeably place classified information at risk of loss or compromise
   - 2) Instances of NISPOM non-compliance where classified information is not at risk
   - 3) Place classified information at imminent risk of loss or compromise, or have resulted in compromise of classified information

2. Match the definition with the specific type of vulnerability.
   - A. Systemic
   - B. Repeat
   - C. Isolated

   - 1) A single occurrence that resulted in, or could logically lead to, loss or compromise of classified information
   - 2) Specific occurrence identified during a previous DSS Security Review
   - 3) Vulnerability(ies) that demonstrate defects in a specific subset of the contractor's industrial security program

3. Which of the following may negate the calculated Rating Matrix score: Select all that apply

   - a. Reported foreign acquisition
   - b. Appointment of a Senior Management Official without a security clearance
   - c. Termination of a major classified contract
   - d. Deliberate disregard for security requirements

Slide 39: Lesson 3: NISP Enhancements

Slide 40: Lesson 3 Objectives

At the end of this lesson, you should be able to:

- Describe NISP Enhancements
- Explain the intent of each NISP Enhancement
- Compare and contrast NISP Enhancements and Best Practices

Slide 41: NISP Enhancements

NISP Enhancements refer to a security process or measure that directly relates to and enhances the protection of classified information beyond baseline NISPOM standards.

The result is to give credit to the true impact of the security enhancements, rather than to attempt to consistently break-down each individual isolated event.

There is a link to the Vulnerability Assessment Rating Matrix (Rating Matrix) and Enhancements under the References Tab above.

Slide 42: Enhancements

Introduction

The categories outline the intent of the enhancement allowing for ease in identifying items which may receive credit. Point credits are given for these procedures and factored into the overall assigned security rating.

On the Rating Matrix, a NISP Enhancement falls into one of several categories.

Dependent upon the category of the facility (e.g., AA, B), the contractor is awarded points for each NISP Enhancement category.

Regardless of the amount of enhancements identified in each category, facilities receive only the number of points shown for that enhancement category (15 or 17).

Click on the arrows at the top of the screen or click on the numbers at the bottom of the page to see more information.

Category 1: Company Sponsored Events

In addition to the annual required security refresher briefings, the cleared contractor holds company sponsored events such as security fairs, interactive designated security-focused weeks, security lunch events, hosting guest speakers on security related topics, and webinars with the security community.

The intent of this category is to encourage cleared contractors to actively set time aside to highlight security awareness and education. This should not be a distribution of a paper or email briefing, but rather some type of interactive in-person activity.

Category 2: Internal Education Brochures/Products

A Security Education and Awareness Program that provides enhanced security education courses or products to employees beyond initial and annual refresher training requirements; e.g., CD/DVD, web-based interactive tools, newsletters, security games/contests, and international security alert program.

The intent of this category is to encourage cleared contractors to generate and distribute relevant security materials to employees who then incorporate the content into their activities.

Category 3: Security Staff Professionalization

Security staff training exceeds NISPOM and DSS requirements and incorporates that knowledge into NISP administration.

The intent of this category is to encourage security program's key personnel to actively strive to learn more and further their professional security expertise beyond mandatory requirements.

Category 4: Information & Product Sharing within Security Community

Facility Security Officer (FSO) provides peer training support within the security community and/or shares security products/services with other cleared contractors outside their corporate family.

The intent of this category is to encourage cleared contractors to actively reach out to other cleared contractors to assist those who may not have the expertise or budget and provide them with security products and services.

Category 5: Active Membership in Security Community

Security personnel are members and actively participate with NISP/security-related professional organizations.

The intent of this category is to encourage cleared contractors to actively collaborate with their local security community to identify best practices to implement within their own NISP security programs.

Verification of enhancement should be aimed at asking what were the take-aways from events, how do they apply to the contractor's security program and how is the security staff implementing any take-away information.

Security personnel unable to attend meetings on a regular basis can collaborate virtually via the organization's website, email, etc.

Category 6: Contractor Self-Review

Contractors sustain a thorough, impactful review of their security posture.

The intent of this category is to encourage cleared contractors to maintain an effective, on-going, self-review program to analyze and identify any threats or vulnerabilities within their program and coordinate with DSS to address those issues prior to the Annual Security Review.

Category 7: Counterintelligence Integration

Contractors build a Counterintelligence (CI) focused culture by implementing processes within their security program to detect, deter, and expeditiously report suspicious activities to DSS through submission of Suspicious Contact Reports (SCRs).

The intent of this category is to encourage cleared contractors to develop vigorous and effective CI programs that thwart foreign attempts to acquire classified and sensitive technologies. Critical elements of a vigorous and effective CI program include timely reporting, understanding the threat environment, and agile and authoritative decision making to neutralize or mitigate vulnerabilities and threats.

Evidence of a vigorous and effective CI program is reporting to DSS resulting in the:

- Identification of actionable information leading to the initiation of investigations or activities by Other Government Agencies (OGAs)
- Implementation of measures to identify and prevent recurrence of reported suspicious activities
- Demonstration of immediate response to a suspicious or illegal act to neutralize or mitigate risks to targeted technologies and facilities

Category 8: FOCI/International

Cleared contractor implements additional effective procedures to mitigate risk to export controlled items and/or FOCI.

The intent of this category is to encourage cleared contractors to implement an enhanced export control program increasing the effectiveness.

For FOCI mitigated facilities, intent is to encourage activities above mitigation instrument requirements to further minimize foreign influence at the facility.

Items which are required of the mitigation instrument may not be counted as enhancements.

Category 9: Classified Material Controls and Physical Security

Facility has deployed an enhanced process for managing classified information and/or has implemented additional physical security measures.

The intent of this category is to encourage cleared contractors to maximize the protection and accountability of classified material on-site by implementing effective processes, regardless of quantity of classified holdings.

Category 10: Information Systems (IS)

Incorporating process enhancements and leveraging tools to expand the overall security posture of accredited information systems.

The intent of this category is to encourage cleared contractors to maximize protection of classified information on IS.

Slide 43: Parent/Home Office Enhancements

Procedures, tools, or processes developed by the Parent/Home Office that enhance or exceed NISPOM requirements that are effectively implemented at the subsidiary/division sites, can be considered as an enhancement during the Security

Review.

Slide 44: Validation

DSS will validate!

NISP Enhancements must be validated during the Security Review as having an effective impact on the overall NISP security program.

This is usually accomplished through employee interviews and review of procedures and processes.

Slide 45: Best Practices

Often, Best Practices are implemented in order to adequately manage a security program due to the size or complexity of the facility.

During Security Reviews, IS Reps may identify Best Practices that are not necessarily related to the NISP or only meet baseline NISP requirements.

Although it is important to recognize these efforts, Best Practices are not counted as an enhancement.

Slide 46: Examples

The following scenarios provide examples of the process to categorize enhancements as either NISP Enhancements or Best Practices, and the different types of supporting evidence to make the determination. Read each scenario and decide if it describes a Best Practice or a NISP Enhancement.

Slide 47: Scenario 1

Scenario 1: A company installs alarms in high theft areas where no classified information is maintained.

While this is a good company security measure, it does not have a direct impact on the protection of classified information. Therefore, it is not a NISP Enhancement, but a Best Practice.

Slide 48: Scenario 2

Scenario 2: A company, in addition to using alarms as supplemental protection for closed areas, adds guard patrols every 3 hours around the clock.

It is not adding an additional impact to the overall program. With or without the additional guard round patrol, the classified information within the closed areas is required to be adequately protected. Therefore, it is not a NISP Enhancement, but a Best Practice.

Slide 49: Scenario 3

Scenario 3: Several employees currently possess a certification, but none of them have taken training or ongoing certification maintenance within the assessment cycle. This is a Best Practice.
Scenario 4: Obtaining and maintaining professional certifications such as CPP, SPēD Certification, CISSP is considered to be… a NISP Enhancement.

Slide 50: Scenario 5

Scenario 5: A member of a cleared contractor's security staff is a guest speaker at a security event provided by a security related professional organization. This is considered to be a NISP Enhancement.
Scenario 6: The President of a cleared facility speaks at an event hosted by a university, but the audience is not familiar with or part of the NISP. This is a Best Practice.

Slide 51: Lesson 3 Summary

You should now be able to:

- Describe NISP Enhancements
- Explain intent of a NISP Enhancement
- Compare and contrast NISP Enhancements and Best Practices

Click the right navigation arrow to check your knowledge of these topics.

Slide 52: Knowledge Check Lesson 3

Read each of the following scenarios and determine if it describes a NISP Enhancement or Best Practice. Drag your response to the blank space provided.

1. The facility hosted a Security Fair Day which included a guest speaker briefing on the "Cyber Threat" topic and a "movie" lunch event in which employees were able to watch a special on Espionage/Insider Threat indicators.
   a. NISP Enhancement
   b. Best Practice

2. The facility has installed CCTV throughout the facility to capture potential theft and drug use.
   a. NISP Enhancement
   b. Best Practice

3. Organizational management published a press release stating the company has continued interest and a high level of support for enhanced security.
   - NISP Enhancement

- Best Practice

4. Security staff distributes relevant security education information provided by government activities or security organizations and the workforce incorporates the content into their activities.
    a. NISP Enhancement
    b. Best Practice

Slide 53: Lesson 4: Security Review Follow-Up Actions

Slide 54: Lesson 4 Objective

At the end of this lesson, you should be able to:

- Summarize the Security Review process as it relates to the Rating Matrix and follow-up actions

Slide 55: Formal Exit Briefing

During the formal exit briefing, the company's FSO and senior management are presented with security vulnerabilities, required corrective actions, NISP Enhancements, and recommended improvements.

The priority is to ensure immediate corrective action is taken to mitigate vulnerabilities.

Slide 56: Formal Exit Briefing

All Acute/Critical Vulnerabilities and required corrective actions are briefed during the formal exit briefing.

Vulnerabilities (Non-Acute/Non-Critical) are typically only communicated to the FSO and not the Senior Management Official (SMO) at the formal exit briefing.

Slide 57: Security Review Results Letter

The Security Review Results Letter is the official written notification to the contractor's SMO of the overall rating of the Contractor's security posture.

The letter is sent to the contractor's SMO and copied to the FSO. The FSO also receives:

- A complete listing of vulnerabilities
- Required corrective actions
- NISP Enhancements granted
- A copy of the Rating Matrix

Slide 58: Security Review Results Letter

Contractors are advised to provide a written response specifying corrective actions taken as follows:

- Within 15 business days of the Security Review for Acute/Critical Vulnerabilities, or
- Within 30 business days of receipt of the results letter for Vulnerabilities (Non-Acute/Non-Critical).

Slide 59: Rating Matrix

A copy of the populated Rating Matrix and Results Letter are provided to the FSO in all instances.

Slide 60: Follow-Up Actions

Security Reviews with Acute/Critical Vulnerabilities

The IS Rep/ISSP will schedule a follow-up action for the company with a goal of 15 business days from the original Security Review completion date to validate the effectiveness of corrective actions taken. Acute Vulnerabilities are given priority.

Security Reviews with Vulnerabilities (Non-Acute/Non-Critical)

A follow-up action for the company by the IS Rep/ISSP is not required unless the company fails to provide a written response specifying corrective actions taken or the corrective actions are deemed to be insufficient.

Slide 61: Lesson 4 Summary

You should now be able to:

- Summarize the Security Review process as it relates to the Rating Matrix and follow up actions

Click the right navigation arrow to check your knowledge of these topics.

Slide 62: Knowledge Check Lesson 4

1. Contractors are advised to provide a written response specifying corrective actions taken. Select the response from the drop-down options to match the response requirements to each category of vulnerability.

   A. Within 15 business days of the Security Review
      I. Acute/Critical Vulnerability
      II. Non-Acute/Non-Critical Vulnerability

   B. Within 30 business days from receipt of the Security Review results letters
      I. Acute/Critical Vulnerability
      II. Non-Acute/Non-Critical Vulnerability

2. Select response from the drop-down options to match the exit briefing requirements to each category of vulnerability.

   A. Non-Acute/Non-Critical Vulnerability
      I. Typically only communicated to the FSO
      II. Must be identified in the exit briefing

   B. Acute/Critical Vulnerability

I. Typically only communicated to the FSO
II. Must be identified in the exit briefing

3. At the formal exit briefing the Senior Management Official and the Facility Security Officer are presented with: (Select all that apply)
   a. Security Rating
   b. NISPOM changes
   c. Corrective Actions
   d. Recommended Improvements

Slide 63: Course Summary

You should now be able to:

- Describe how the Rating Matrix is used to standardize and improve consistency of the Security Review Rating Process

Slide 64: Course Completion

Congratulations! You have completed the instructional portion of the DSS Security Rating Process Course. Now, you will need to return to STEPP to complete the Final Assessment: DSS Security Rating Process exam IS036.06.

Student Guide

DSS Security Rating Process - IS036.16

Answer Key

Questions are followed by the correct answer(s) only.

Knowledge Check Lesson 1

1. The Rating Matrix assigns point values (to be added or subtracted) to determine a Security Rating following a Security Review for which of the following items:
    - Vulnerability
    - Enhancement

2. A vulnerability that was Corrected on the Spot (COS) does not cause points to be subtracted on the Rating Matrix Calculation Worksheet.
    - False

3. Regarding the Rating Matrix, which of the following represents the baseline score used to calculate a Security Rating following a Security Review:
    - 700

4. Contractors that have fully implemented the requirements of the NISPOM which results in an exemplary security posture is an example of which security rating:
    - Commendable

Knowledge Check Lesson 2

1. Match the definition with the specific category of vulnerability.
    - Acute Vulnerability - Place classified information at imminent risk of loss or compromise, or have resulted in compromise of classified information
    - Critical Vulnerability - Instances of NISPOM non-compliance that are serious, or that may foreseeably place classified information at risk of loss or compromise
    - Vulnerability (Non-Acute/Non-Critical) - Instances of NISPOM non-compliance where classified information is not at risk

2. Match the definition with the specific type of vulnerability.
    - Systemic - Vulnerability(ies) that demonstrate defects in a specific subset of the contractor's industrial security program
    - Repeat - Specific occurrence identified during a previous DSS Security Review
    - Isolated - A single occurrence that resulted in, or could logically lead to, loss or compromise of classified information

3. Which of the following may negate the calculated Rating Matrix score: Select all that apply:

- Appointment of a Senior Management Official without a security clearance
- Deliberate disregard for security requirements

Knowledge Check Lesson 3

Click and drag response to determine if scenario describes a NISP Enhancement or Best Practice.

1. The facility hosted a Security Fair Day which included a guest speaker briefing on the “Cyber Threat” topic and a “movie” lunch event in which employees were able to watch a special on Espionage/Insider Threat indicators.
   - NISP Enhancement

2. The facility has installed CCTV throughout the facility to capture potential theft and drug use.
   - Best Practice

3. Organizational management published a press release stating the company has continued interest and a high level of support for enhanced security.
   - Best Practice

4. Security staff distributes relevant security education information provided by government activities or security organizations and the workforce incorporates the content into their activities.
   - NISP Enhancement

Knowledge Check Lesson 4

1. Contractors are advised to provide a written response specifying corrective actions taken. Select the response from the drop-down options to match the response requirements to each category of vulnerability.

   Within 15 business days of the Security Review
   Acute/Critical Vulnerability

   Within 30 business days from receipt of the Security Review results letters
   Non-Acute/Non-Critical Vulnerability

2. Select response from the drop-down options to match the exit briefing requirements to each category of vulnerability.

   Non-Acute/Non-Critical Vulnerability
   Typically only communicated to the FSO

   Acute/Critical Vulnerability
   Must be identified in the exit briefing

3. At the formal exit briefing the Senior Management Official and the Facility Security Officer are presented with: (Select all that apply)
   - ○ Security Rating
   - ○ Corrective Actions
   - ○ Recommended Improvements