SECURITY RATING CRITERIA REQUIREMENTS

IMPLEMENTATION DATE: OCTOBER 1, 2024

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NISP Mission Performance Division, Mission Branch

AGENDA

- Define security rating and explain where to find security rating requirements
- Explain refinements related to security rating criteria
- Explain the purpose of the supporting guidance section
- Explain the requirements to achieve each criterion
- Explain where to find security rating requirements and resources

DCSA SECURITY RATING PROCESS

DCSA rates the contractor's security posture at the conclusion of the security review. The security rating is a description of the contractor's effectiveness in protecting classified information.

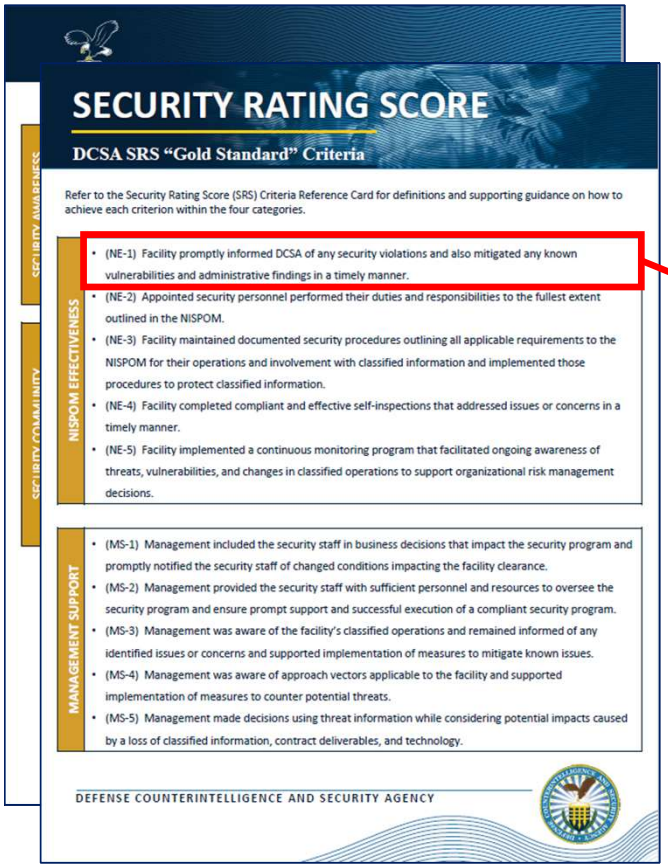
Facility Security Officer

Industrial Security Representative

SECURITY RATING PROCESS

- Minimum rating requirements for all levels are outlined in DODM 5220.32, Volume 1, Section 14.
- DCSA criteria further defines the minimum rating requirements for facilities in general conformity.
- Supporting guidance provides a common interpretation for how to achieve each criterion.
- Refer to the DCSA Security Rating Criteria Reference Card.

RELATIONSHIP BETWEEN CRITERIA AND SUPPORTING GUIDANCE



SECURITY RATING SCORE

DCSA SRS "Gold Standard" Criteria

Refer to the Security Rating Score (SRS) Criteria Reference Card for definitions and supporting guidance on how to achieve each criterion within the four categories.

NISPOM EFFECTIVENESS

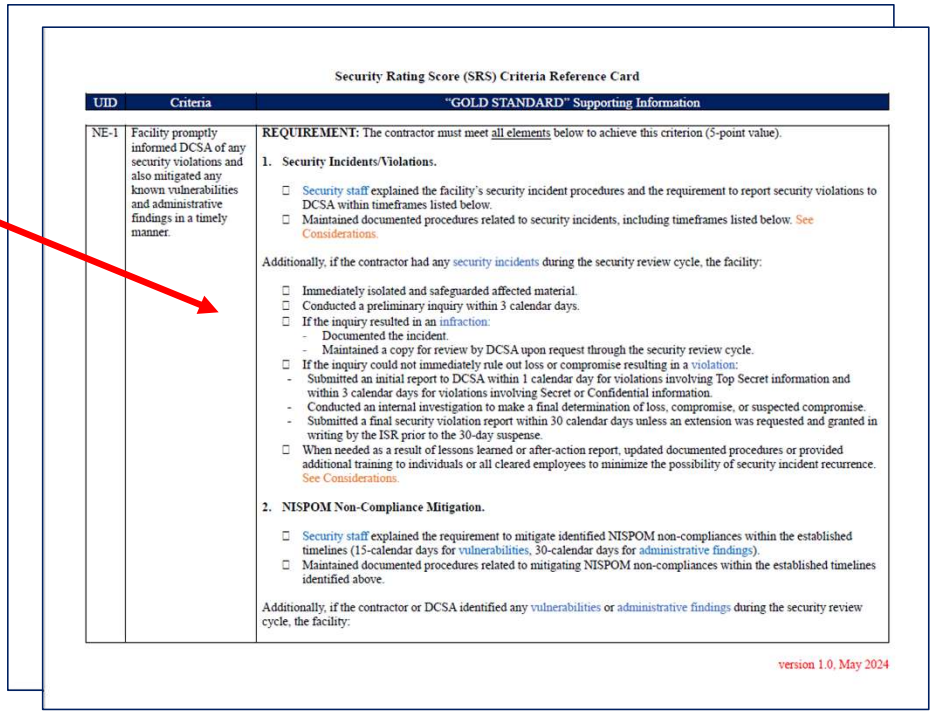
- (NE-1) Facility promptly informed DCSA of any security violations and also mitigated any known vulnerabilities and administrative findings in a timely manner.
- (NE-2) Appointed security personnel performed their duties and responsibilities to the fullest extent outlined in the NISPOM.
- (NE-3) Facility maintained documented security procedures outlining all applicable requirements to the NISPOM for their operations and involvement with classified information and implemented those procedures to protect classified information.
- (NE-4) Facility completed compliant and effective self-inspections that addressed issues or concerns in a timely manner.
- (NE-5) Facility implemented a continuous monitoring program that facilitated ongoing awareness of threats, vulnerabilities, and changes in classified operations to support organizational risk management decisions.

MANAGEMENT SUPPORT

- (MS-1) Management included the security staff in business decisions that impact the security program and promptly notified the security staff of changed conditions impacting the facility clearance.
- (MS-2) Management provided the security staff with sufficient personnel and resources to oversee the security program and ensure prompt support and successful execution of a compliant security program.
- (MS-3) Management was aware of the facility's classified operations and remained informed of any identified issues or concerns and supported implementation of measures to mitigate known issues.
- (MS-4) Management was aware of approach vectors applicable to the facility and supported implementation of measures to counter potential threats.
- (MS-5) Management made decisions using threat information while considering potential impacts caused by a loss of classified information, contract deliverables, and technology.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Gold Standard Criteria



Security Rating Score (SRS) Criteria Reference Card

UID	Criteria	"GOLD STANDARD" Supporting Information
NE-1	Facility promptly informed DCSA of any security violations and also mitigated any known vulnerabilities and administrative findings in a timely manner.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). **1. Security Incidents/Violations.** ☐ Security staff explained the facility's security incident procedures and the requirement to report security violations to DCSA within timeframes listed below. ☐ Maintained documented procedures related to security incidents, including timeframes listed below. See Considerations. Additionally, if the contractor had any security incidents during the security review cycle, the facility: ☐ Immediately isolated and safeguarded affected material. ☐ Conducted a preliminary inquiry within 3 calendar days. ☐ If the inquiry resulted in an infraction: - Documented the incident. - Maintained a copy for review by DCSA upon request through the security review cycle. ☐ If the inquiry could not immediately rule out loss or compromise resulting in a violation: - Submitted an initial report to DCSA within 1 calendar day for violations involving Top Secret information and within 3 calendar days for violations involving Secret or Confidential information. - Conducted an internal investigation to make a final determination of loss, compromise, or suspected compromise. - Submitted a final security violation report within 30 calendar days unless an extension was requested and granted in writing by the ISR prior to the 30-day suspense. ☐ When needed as a result of lessons learned or after-action report, updated documented procedures or provided additional training to individuals or all cleared employees to minimize the possibility of security incident recurrence. See Considerations. **2. NISPOM Non-Compliance Mitigation.** ☐ Security staff explained the requirement to mitigate identified NISPOM non-compliances within the established timelines (15-calendar days for vulnerabilities, 30-calendar days for administrative findings). ☐ Maintained documented procedures related to mitigating NISPOM non-compliances within the established timelines identified above. Additionally, if the contractor or DCSA identified any vulnerabilities or administrative findings during the security review cycle, the facility:

version 1.0, May 2024

Criteria Supporting Guidance

UNDERSTANDING THE SUPPORTING GUIDANCE SECTION

Item	Color Code	Description
Requirements	Black	Required elements a contractor must achieve to be awarded the criterion points.
Exceptions	Green	Clearly defined exceptions to the baseline requirement (only a few instances).
Definitions	Blue	Clearly defined words or phrases that assist with consistency.
Considerations	Orange	Additional context to add clarity, disqualifications, and other items to consider when determining if the contractor achieved the criteria.
Examples	Purple	Examples of how a contractor may achieve a criterion element. These are not the only ways to achieve the criterion and the listed examples may change based on available programs. DCSA will consider the intent of the element when awarding the criterion.

DISCLAIMER

- The following slides include a high-level overview of the DCSA criteria and supporting guidance effective 1 Oct 2024.

- To view a complete list of all criteria requirements and considerations, refer to the DCSA Security Rating Criteria Reference Card located on the DCSA SRRP Website.

Scan here to visit the
DCSA SRRP Website

NEW TERMS AND DEFINITIONS

Contractor Personnel	Includes cleared and uncleared employees, on-site subcontractors, on-site Government personnel, and visitors (as appropriate).
Government Entities	Includes DCSA, GCAs, DOD IG, and other Government agencies.
Management	Includes, but is not limited to, the SMO, KMP, program managers, and other management throughout the chain of command involved in classified operations.
Security Community	Includes industrial security personnel, other cleared contractors, DCSA, GCAs, and other Government agencies.
Security Staff	Includes, but is not limited to, the Chief Security Officer, Director of Security, Security Manager, FSO, ITPSO, ISSM, and others (as appropriate).

NISPOM EFFECTIVENESS (NE-1)

Facility promptly informed DCSA of any security violations and mitigated any known vulnerabilities and administrative findings in a timely manner.

- Maintain documented procedures related to security incidents and NISPOM non-compliance mitigation (including timelines).
- Explain the facility's security incident procedures and the requirement to mitigate NISPOM non-compliances identified throughout the security review cycle (including timelines).
- Process security incidents as outlined in the security incident job aid.
- Mitigate known vulnerabilities and administrative findings within established timelines.

NISPOM EFFECTIVENESS (NE-2)

Appointed security personnel performed their duties and responsibilities to the fullest extend outlined in the NISPOM.

- Appoint a SMO, FSO, ITPSO, and ISSM (when appropriate) throughout the security review cycle.
- Perform all applicable duties and responsibilities outlined in the NISPOM. Refer to the Appointed Personnel Duties Job Aid for a complete list.

NISPOM EFFECTIVENESS (NE-3)

Facility maintained documented security procedures outlining all applicable requirements of the NISPOM for their operations and involvement with classified information and implemented those procedures to protect classified information.

- Establish documented security procedures to the level of operations and involvement with classified information.
- Update documented procedures when a qualifying change impacts successful implementation of the security program.
- Provide relevant contractor personnel a copy of documented procedures.
- Implement the processes outlined in the documented procedures.

NISPOM EFFECTIVENESS (NE-4)

Facility completed compliant and effective self-inspections that addressed issues or concerns in a timely manner.

- Conduct a formal self-inspection at least annually that adheres to all NISPOM requirements.
- Additionally, include the following components in the formal self-inspection:
  - Review internal processes and approach vectors.
  - Review and update NISS facility profile if needed.
  - Evaluate employee knowledge of security practices.
  - Fully mitigate known non-compliances and issues.
  - Update documented security procedures if needed.
  - Address relevant issues or concerns in annual refresher training.

NISPOM EFFECTIVENESS (NE-5)

Facility implemented a continuous monitoring program that facilitated ongoing awareness of threats, vulnerabilities, and changes in classified operations to support organizational risk management decisions.

- Monitor the industrial security program throughout the security review cycle.
- Complete all classified IS continuous monitoring activity requirements as part of the authorization if applicable.
- Explain how the facility facilitates ongoing awareness of threats, vulnerabilities, and changes in classified operations throughout the security review cycle.

MANAGEMENT SUPPORT (MS-1)

Management included the security staff in business decisions that impact the security program and promptly notified the security staff of changed conditions impacting the facility clearance.

- Include security staff in business decisions impacting the security program.
- Notify security staff prior to changed conditions impacting the facility clearance (or no later than five calendar days after the change).

MANAGEMENT SUPPORT (MS-2)

Management provided the security staff with sufficient personnel and resources to oversee the security program and ensure prompt support and successful execution of a compliant security program.

- Maintain an appointed FSO, ITPSO, and ISSM (when appropriate) throughout the security review cycle.
- Maintain enough personnel to provide prompt support and successful execution of the security program.
- Provide enough material and financial resources to enable prompt support and successful execution of the security program.

MANAGEMENT SUPPORT (MS-3)

Management was aware of the facility's classified operations and remained informed of any identified issues or concerns and supported implementation of measures to mitigate known issues.

- Provide personnel, material, or financial support to understand issues or concerns and to implement necessary mitigation (when appropriate).
- Receive briefings from the security staff on any necessary or lacking resources, and classified IS project updates through the configuration change board (when appropriate).
- Receive notifications from the security staff of relevant security vulnerabilities, systemic security problems, and issues impacting the FCL.
- Understand the facility's involvement with classified operations based on assigned duties and responsibilities.
- (SMO) Certify results of the self-inspection and brief KMP on the results throughout the security review cycle.

MANAGEMENT SUPPORT (MS-4)

Management was aware of approach vectors applicable to the facility and supported implementation of measures to counter potential threats.

- Provide personnel, material, or financial support to understand threats and to implement necessary countermeasures (when appropriate).
- Understand the most common approach vectors applicable to cleared industry as outlined in the MCMO Matrix.
- Understand the approach vectors applicable to the facility.
- Explain how they support measures to counter potential threats.

MANAGEMENT SUPPORT (MS-5)

Management made decisions using threat information while considering potential impacts caused by a loss of classified information, contract deliverables, and technology.

- Explain how they obtain current and relevant threat information.
- Explain how they use threat information to make business, operational, and mission decisions considering potential impacts caused by a loss of classified information, contract deliverables, and technology.

SECURITY AWARENESS (SA-1)

Contractor implemented a culture of security within the organization.

- Explain how the facility successfully implements a culture of security within the organization.

SECURITY AWARENESS (SA-2)

Contractor personnel understood the security processes and documented security procedures relevant to their position.

- Maintain documented security procedures to the level of operations and involvement with classified information.
- Explain which procedures are relevant to their position and where to find those procedures.
- Explain how to perform processes relevant to their position.

SECURITY AWARENESS (SA-3)

Contractor personnel understood what required protection related to classified contracts, security classification guidance, and approach vectors applicable to their position.

- Maintain documented security procedures to the level of operations and involvement with classified information.
- Explain what information, material, or technology requires protection based on their position as outlined in classified contracts and security classification guides.
- Explain which approach vectors are applicable to their position and the measures they take to mitigate a potential threat.
- Explain how to protect the information and material within their possession.

SECURITY AWARENESS (SA-4)

Contractor personnel protected classified information in accordance with documented security procedures, NISPOM standards, and contractual requirements.

- Maintain documented security procedures to the level of operations and involvement with classified information.
- Provide contractor personnel with a copy of security procedures relevant to their position.
- Provide contractor personnel with a copy of classification guides relevant to their position.
- Explain how to protect the information and material within their possession.
- Protect classified information resulting in no loss, compromise, or suspected compromise.

SECURITY AWARENESS (SA-5)

Contractor personnel understood reporting requirements and reported relevant events.

- Maintain documented security procedures to the level of operations and involvement with classified information.
- Explain the requirement to report all relevant security-related issues.
- Report all relevant security-related issues.

SECURITY COMMUNITY (SC-1)

Contractor cooperated with Government entities during official visits and security investigations.

- Provide suitable arrangements within the facility for conducting private interviews with employees.
- Provide relevant files and records pertaining to an individual under investigation.
- Review the facility's NISS facility and submit an update when needed.
- Provide information and complete follow-up actions when requested by DCSA.
- Render necessary assistance to support Government-led investigations.

SECURITY COMMUNITY (SC-2)

Contractor reported events to DCSA and OGAs in accordance with NISPOM and contractual requirements and supported the interest of national security by sharing relevant threat information within the security community.

- Report relevant security events to DCSA and OGAs outlined in NISPOM 117.8 and contractual requirements.
- Share relevant threat information with the security community.

SECURITY COMMUNITY (SC-3)

Contractor coordinated with relevant stakeholders to obtain accurate and sufficient security classification guidance.

- Review all aspects of the security classification guidance, including embedded security contract clauses.
- Submit a request for remedy to the GCA or prime contractor, as appropriate, and follow-up as needed when information is classified improperly or unnecessary, or when security classification guidance is inadequate, improper, or not provided.
- Respond to subcontractor requests for remedy, if applicable.
- Coordinate with the customer for classified IS Risk Acknowledgement Letters, when appropriate.

SECURITY COMMUNITY (SC-4)

Contractor provided support to the security community that positively impacted the national industrial security program.

- Provide support to the security community.
- Explain how the support positively impacts the National Industrial Security Program.

SECURITY COMMUNITY (SC-5)

Contractor participated in security community events, conferences, or webinars that positively impacted their security program.

- Participate in at least two security community events/training per calendar year (i.e., FSO, ITPSO, and ISSM).
- Explain how the participation positively impacts the facility's security program.

RESOURCES

- DCSA Security Review and Rating Process (SRRP) Website
  - Security Rating Process Slick Sheet
  - Gold Standard Criteria
  - Security Rating Reference Card
  - Appointed Personnel Duties Job Aid
  - Security Rating Score Tool
- For questions related to these resources, contact your assigned DCSA Industrial Security Representative.

Scan here to visit the DCSA SRRP Website

CDSE EVENTS

Upcoming CDSE Webinars

Security Rating Score Tool and Resources
August 29, 2024 (1:00 PM to 2:30 PM ET)

Past CDSE Webinars

Introduction to the Security Rating Score
Recorded on June 25, 2024

Categories and Criteria Requirements
Recorded on July 30, 2024

Scan here for more information on
CDSE Webinars and Conferences

NCMS LIVE! EVENTS

Upcoming NCMS Live! SRS Sessions

Security Rating Criteria Requirements
August 7, 2024 (3:00 PM to 4:00 PM ET)

Security Rating Score Tool
September 4, 2024 (3:00 PM to 4:00 PM ET)

Security Rating Resources and Q&A
October 2, 2024 (3:00 PM to 4:00 PM ET)

Past NCMS Live! SRS Sessions

Introduction to the Security Rating Score
July 11, 2024

Scan here for more information on
NCMS Events

These sessions are restricted to members of NCMS – The Society of Industrial Security Professionals.

REVIEW

- Understand the security rating definition and where to find security rating requirements
- Understand refinements related to security rating criteria
- Understand the purpose of the supporting guidance section
- Understand the requirements to achieve each criterion
- Understand where to find security rating resources

QUESTIONS

Thank you for your participation.
Questions will be consolidated and posted to the CDSE website with a copy of the recording and slides.