This briefing is unclassified in its entirety.

INTRODUCTION TO THE SECURITY RATING SCORE

IMPLEMENTATION DATE: OCTOBER 1, 2024

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NISP Mission Performance Division, Mission Branch

AGENDA

- Explain why DCSA refined the security rating process
- Explain the top 3 security rating process refinements
- Explain the process used to calculate a score and assign a security rating
- Explain where to find security rating requirements and resources

BACKGROUND: WHAT YOU NEED TO KNOW!

- May 2023: DCSA began making refinements to the security rating process in collaboration with a NISPPAC working group.
- January - March 2024: Provisional refinements were piloted using data from 40 security reviews.
- April 2024: Minor feedback was incorporated into final rating refinements.
- May 2024: DCSA leadership approved refinements for full implementation on October 1, 2024.
- June 2024: DCSA publicly announced the successful joint development of the rating process refinements.

Why this matters:

- Reflects DCSA's ongoing commitment to partnering with Industry.
- Goal: Enhance clarity, fairness, and transparency within the security framework governing the NISP.

Security is a team sport. We are all on the same team and share the same goals.

– DCSA Director Cattler

CDSE TRAINING: WHAT YOU NEED TO KNOW!

Session	Topic	Dates	Description
Session 1	Introduction to the SRS	Access recording here	Introduction to the refined security rating process which will be implemented on October 1, 2024.
Session 2	Security Rating Criteria Requirements	Access recording here	Overview of the refined security rating criteria.
Session 3	Security Rating Score Tool and Resources	August 29	Overview of security rating resources and discussion on how contractors can use the security rating score tool within their self-inspection program.

Scan the QR Code to access the CDSE Webinars website.

**Additional training is available through NCMS – The Society of Industrial Security Professionals. Members can register for NCMSLive! sessions here.*

RATING PROCESS REFINEMENTS: WHAT YOU NEED TO KNOW!

- No changes to the security review process.

- Security rating process is still policy-based, compliance-first, using a whole-of-company approach.

- Top 3 refinements include:

  1. Consolidates rating criteria into a single list known as the "gold standard" and incorporates a common interpretation on how to achieve each criterion.

  2. Added numeric component to the rating process resulting in a security rating score and eliminating the "lowest category rating" calculation.

  3. Created a new security rating tool and scorecard which provides granular level feedback on facility program effectiveness and opportunities for growth.

REFINEMENT #1: CONSOLIDATED AND CLARIFIED RATING CRITERIA

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

SECURITY REVIEW AND RATINGS

SECURITY RATING REFERENCE CARDS

COMMENDABLE RATING CRITERIA

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

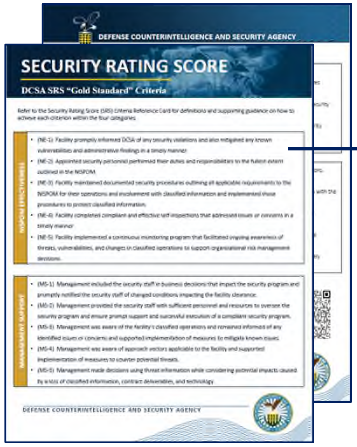
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

SECURITY REVIEW AND RATINGS

SECURITY RATING REFERENCE CARDS

SUPERIOR RATING CRITERIA

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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

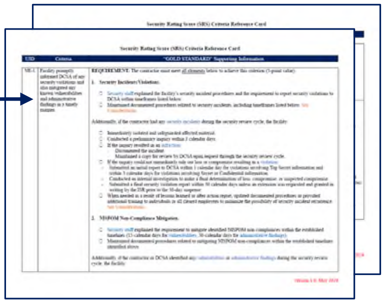
- (NE-1) Facility promptly informed DCSA of any security violations and also mitigated any known vulnerabilities and administrative findings in a timely manner.
- (NE-2) Appointed security personnel performed their duties and responsibilities to the fullest extent outlined in the NISPOM.
- (NE-3) Facility 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

SRS Gold Standard Criteria



Security Rating Score (SRS) Criteria Reference Card

"GOLD STANDARD" Supporting Information

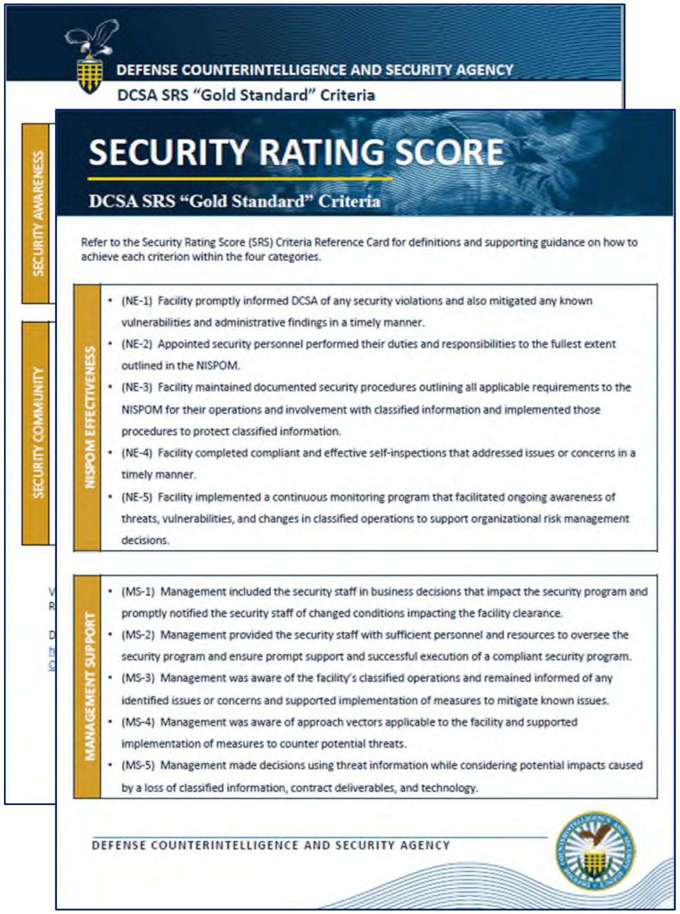
SRS Supporting Guidance

- 20 "gold standard" criteria, 5 in each of the 4 categories of:
  - NISPOM Effectiveness
  - Management Support
  - Security Awareness
  - Security Community

- Supporting guidance creates a common understanding of definitions, requirements, exceptions, considerations, and examples.

- Criteria and supporting guidance are available to all stakeholders.

RELATIONSHIP BETWEEN CATEGORIES AND CRITERIA



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DCSA SRS “Gold Standard” Criteria

SECURITY AWARENESS

SECURITY COMMUNITY

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

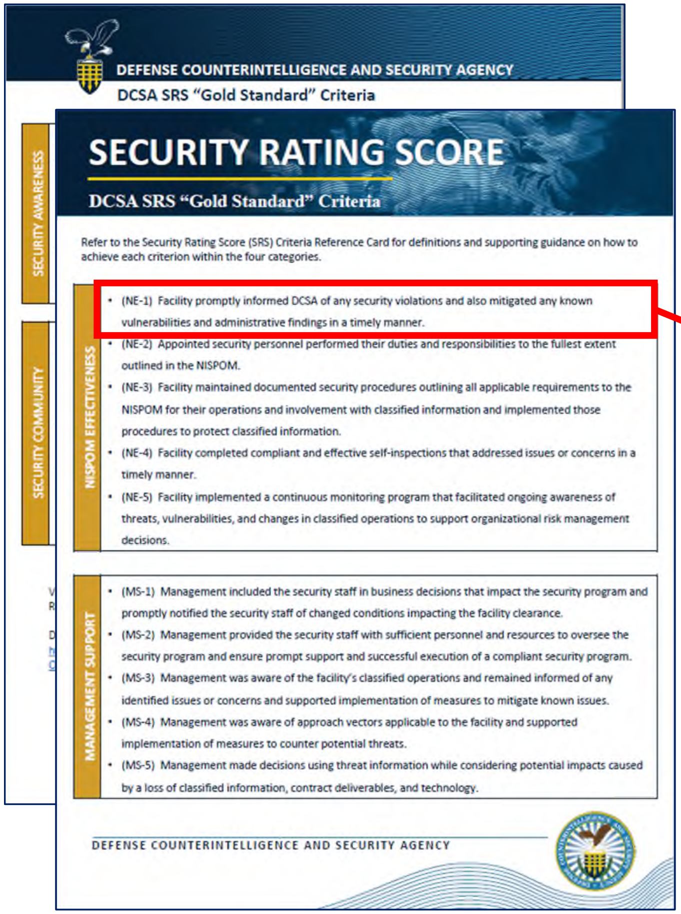
Gold Standard Criteria

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 written 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.
- (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.

Criteria within a single category

RELATIONSHIP BETWEEN CRITERIA AND SUPPORTING GUIDANCE



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DCSA SRS "Gold Standard" Criteria

SECURITY AWARENESS

SECURITY COMMUNITY

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

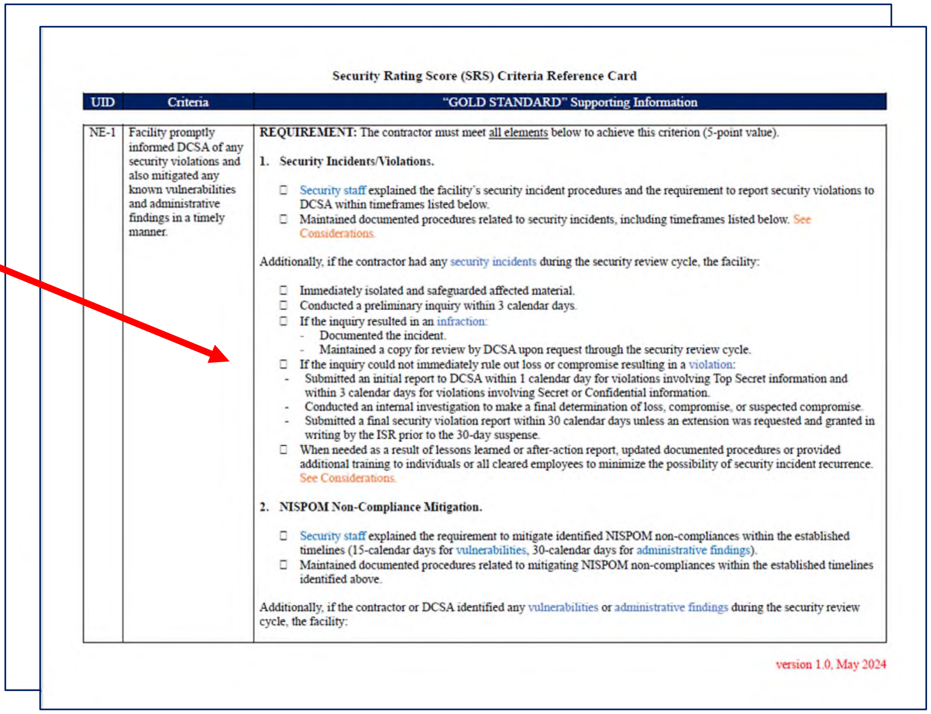
- (NE-1) Facility promptly informed DCSA of any security violations and also mitigated any known vulnerabilities and administrative findings in a timely manner.
- (NE-2) Appointed security personnel performed their duties and responsibilities to the fullest extent outlined in the NISPOM.
- (NE-3) Facility 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:

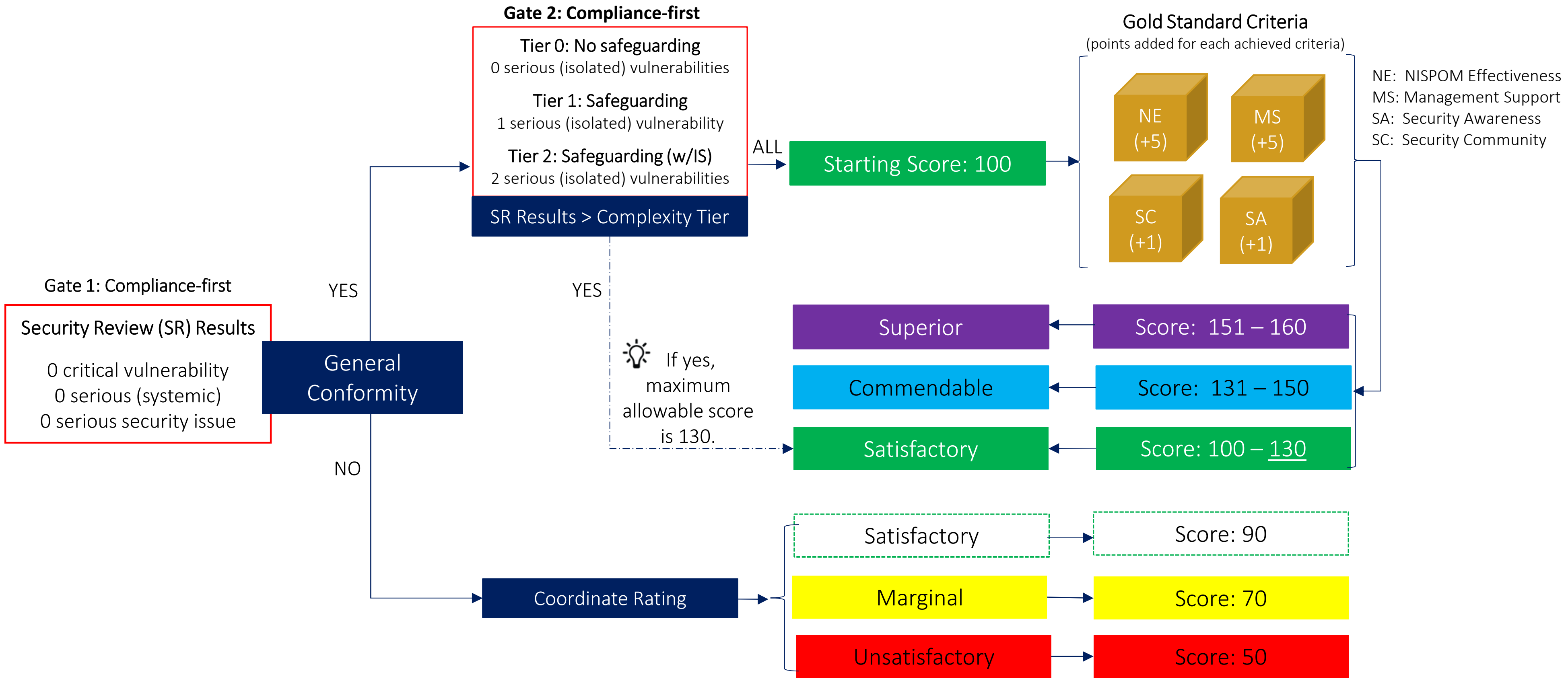
version 1.0, May 2024

Criteria Supporting Guidance

HOW TO READ 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 assists 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.

REFINEMENT #2: ADDED SCORING COMPONENT



Gate 1: Compliance-first

Security Review (SR) Results

0 critical vulnerability
0 serious (systemic)
0 serious security issue

General Conformity

YES

NO

Gate 2: Compliance-first

Tier 0: No safeguarding
0 serious (isolated) vulnerabilities

Tier 1: Safeguarding
1 serious (isolated) vulnerability

Tier 2: Safeguarding (w/IS)
2 serious (isolated) vulnerabilities

SR Results > Complexity Tier

ALL

Starting Score: 100

YES

If yes, maximum allowable score is 130.

Gold Standard Criteria
(points added for each achieved criteria)

NE (+5)

MS (+5)

SC (+1)

SA (+1)

NE: NISPOM Effectiveness
MS: Management Support
SA: Security Awareness
SC: Security Community

Superior	Score: 151 – 160
Commendable	Score: 131 – 150
Satisfactory	Score: 100 – 130

Coordinate Rating

Satisfactory	Score: 90
Marginal	Score: 70
Unsatisfactory	Score: 50

REFINEMENT #2: ADDED SCORING COMPONENT

Where do we start?

General Conformity

General conformity means your facility had no critical vulnerabilities, no systemic vulnerabilities, and no serious security issues identified during the security review.

Facility Security Officer

Industrial Security Representative

REFINEMENT #2: ADDED SCORING COMPONENT (NON-CONFORMITY)

What if my facility is not in general conformity?

Facility Security Officer

DCSA would first coordinate a policy-based rating.

Industrial Security Representative

The coordinated policy-based rating then determines the final security rating score.

Coordinated Rating		Final SRS
Satisfactory	→	Score: 90
Marginal	→	Score: 70
Unsatisfactory	→	Score: 50

REFINEMENT #2: ADDED SCORING COMPONENT (GENERAL CONFORMITY)

What if my facility is in general conformity?

Facility Security Officer

DCSA will first determine your maximum allowed score.

Industrial Security Representative

To do this we consider the following:

1. Facility's complexity tier.

2. Number of serious (isolated) vulnerabilities identified during the security review.

If your facility has more serious (isolated) vulnerabilities than your complexity tier allows, the maximum allowed score is 130. Otherwise, the maximum allowed score is 160.

REFINEMENT #2: ADDED SCORING COMPONENT (GENERAL CONFORMITY)

Facility Security Officer

Industrial Security Representative

Tier 0: No Safeguarding
0 serious (isolated) vulnerabilities allowed

Tier 1: Safeguarding (no classified IS)
1 serious (isolated) vulnerability allowed

Tier 2: Safeguarding (with classified IS)
2 serious (isolated) vulnerabilities allowed

REFINEMENT #2: ADDED SCORING COMPONENT (GENERAL CONFORMITY)

So, if my facility is access elsewhere then we are Tier O?

Facility Security Officer

Yes, this is correct.

Industrial Security Representative

As Tier 0, your facility is allowed 0 serious (isolated) vulnerabilities. This means if you have any serious (isolated) vulnerabilities, your maximum score drops from 160 to 130.

However, this will not impact your facility's general conformity status.

REFINEMENT #2: ADDED SCORING COMPONENT (GENERAL CONFORMITY)

If my maximum allowed score is 130, do you still review rating criteria?

Facility Security Officer

Industrial Security Representative

Yes, of course.

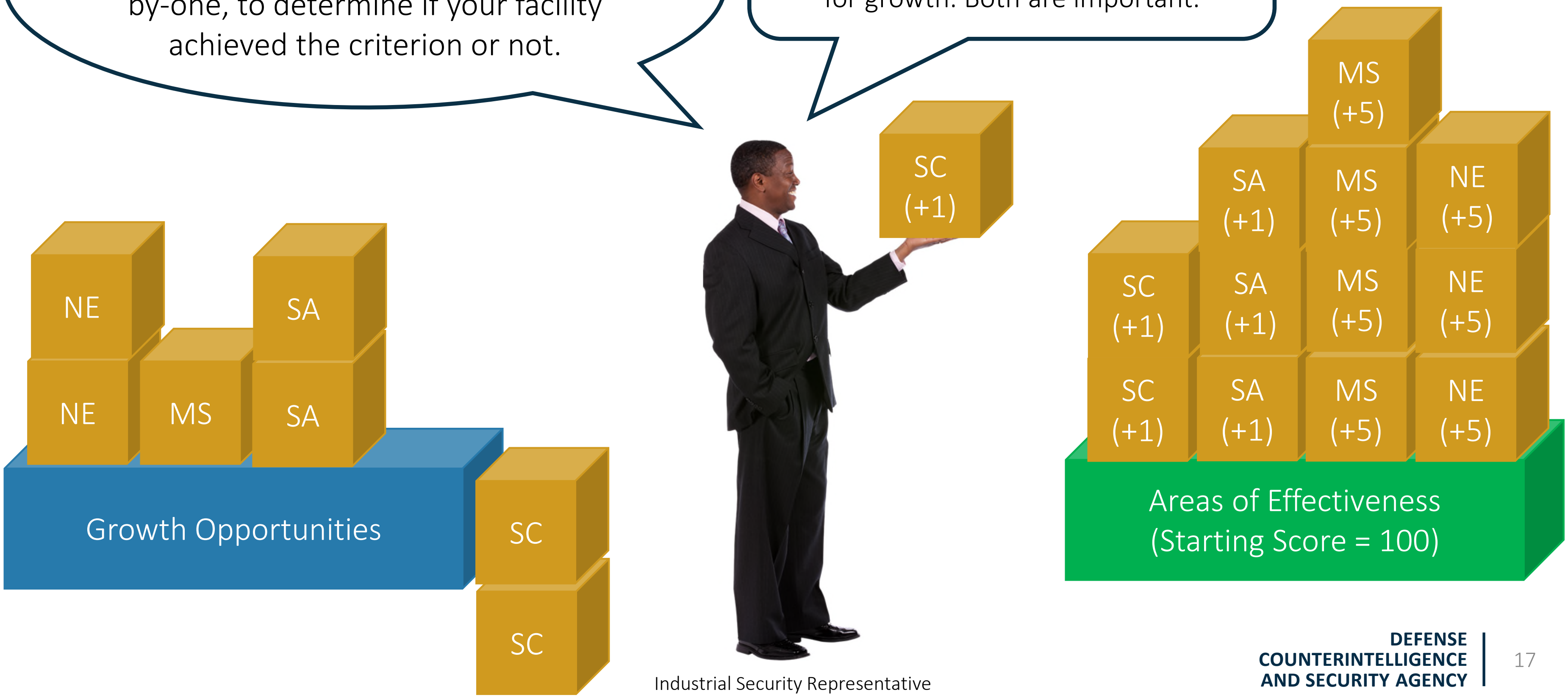
DCSA reviews rating criteria for all facilities in general conformity.

Let’s discuss how that works.

REFINEMENT #2: ADDED SCORING COMPONENT (GENERAL CONFORMITY)

Using the supporting guidance, DCSA reviews each criterion, one-by-one, to determine if your facility achieved the criterion or not.

Achieved criterion is considered an area of effectiveness. Whereas criterion not achieved is considered an opportunity for growth. Both are important.



NE
NE
MS
SA
SA

Growth Opportunities

SC
SC

SC (+1)

Industrial Security Representative

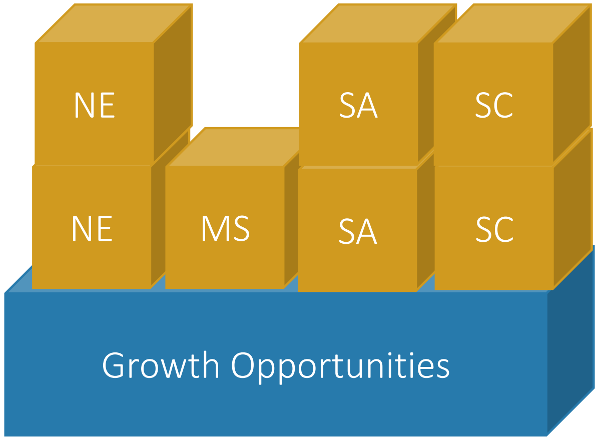
MS (+5)
SA (+1)
MS (+5)
NE (+5)
SC (+1)
SA (+1)
MS (+5)
NE (+5)
SC (+1)
SA (+1)
MS (+5)
NE (+5)

Areas of Effectiveness
(Starting Score = 100)

REFINEMENT #2: ADDED SCORING COMPONENT (GENERAL CONFORMITY)

Once all criteria decisions are made, DCSA adds your achieved points to the starting score of 100 resulting in your provisional score.

No points are added or removed for criterion not achieved.



NE NE

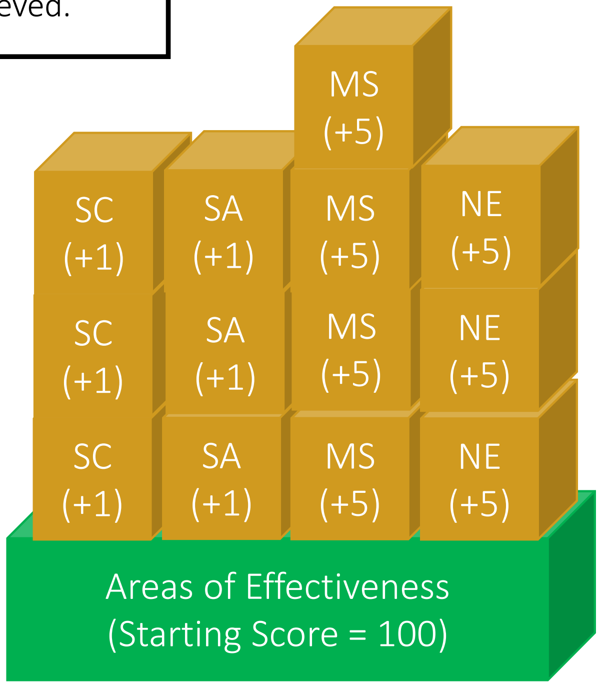
MS

SA SA

SC SC

Growth Opportunities

Industrial Security Representative



SC (+1) SC (+1) SC (+1)

SA (+1) SA (+1) SA (+1)

MS (+5) MS (+5) MS (+5) MS (+5)

NE (+5) NE (+5) NE (+5)

Areas of Effectiveness
(Starting Score = 100)

REFINEMENT #2: ADDED SCORING COMPONENT

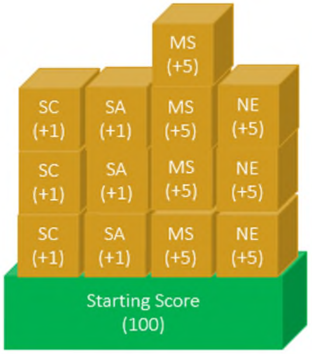
In your example, is the security rating score a 141?

Facility Security Officer

Yes, great job! 141 is the provisional score.

Industrial Security Representative

100	Starting Score
+ 41	Achieved Points
141	Provisional Score



REFINEMENT #2: ADDED SCORING COMPONENT

Facility Security Officer

Industrial Security Representative

The provisional score is the final score if the maximum allowed score is 160. For example:

Provisional score = 141
Maximum allowed score = 160
Final score = 141

However, if the maximum allowed score is 130, the final score will be 130 or less. For example:

Provisional score = 141
Maximum allowed score = 130
Final score = 130

REFINEMENT #2: ADDED SCORING COMPONENT

If the final security rating score is 141, what is the rating?

Easy. Check the security rating score range.

Facility Security Officer

Industrial Security Representative

Security Rating Score Range

Superior	Score: 151 – 160
Commendable	Score: 131 – 150
Satisfactory	Score: 100 – 130

A final security rating score of 141 corresponds to a Commendable rating. Also, the DCSA security rating score tool calculates the security rating score and final rating to foster consistency.

REFINEMENT #2: ADDED SCORING COMPONENT

Can I use the tool to calculate my facility’s score and rating?
Yes, absolutely.

Facility Security Officer

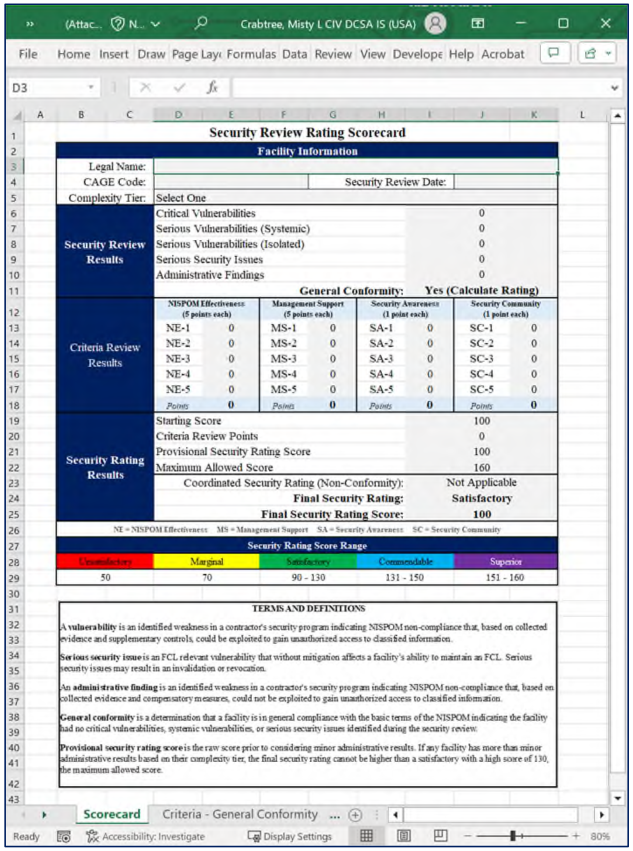
Industrial Security Representative

DCSA encourages you to use the Security Rating Score tool to calculate an unofficial score and rating as part of your self-inspection process. The tool and all resources are located on the DCSA security review and rating process website.

REFINEMENT #3: CREATED TOOL AND SCORECARD

Security Rating Score Tool is a **fully automated** excel workbook consisting of two tabs:

- Tab 1: Used for all security reviews (scorecard).
- Tab 2: Used for facilities in general conformity.



(Attac... N... Crabtree, Misty L CIV DCSA IS (USA)
File Home Insert Draw Page Lay Formulas Data Review View Develope Help Acrobat
D3
Scorecard
Criteria - General Conformity
Ready Accessibility: Investigate Display Settings 80%

Security Review Rating Scorecard

Facility Information			
Legal Name:			
CAGE Code:		Security Review Date:	
Complexity Tier:	Select One		
Security Review Results	Critical Vulnerabilities		0
	Serious Vulnerabilities (Systemic)		0
	Serious Vulnerabilities (Isolated)		0
	Serious Security Issues		0
	Administrative Findings		0
		General Conformity:	**Yes (Calculate Rating)**

Criteria Review Results	NISPOM Effectiveness (5 points each)		Management Support (5 points each)		Security Awareness (1 point each)		Security Community (1 point each)	
	NE-1	0	MS-1	0	SA-1	0	SC-1	0
	NE-2	0	MS-2	0	SA-2	0	SC-2	0
	NE-3	0	MS-3	0	SA-3	0	SC-3	0
	NE-4	0	MS-4	0	SA-4	0	SC-4	0
	NE-5	0	MS-5	0	SA-5	0	SC-5	0
	Points	**0**	*Points*	**0**	*Points*	**0**	*Points*	**0**

Security Rating Results	Starting Score	100
	Criteria Review Points	0
	Provisional Security Rating Score	100
	Maximum Allowed Score	160
	Coordinated Security Rating (Non-Conformity):	Not Applicable
	Final Security Rating:	**Satisfactory**
	Final Security Rating Score:	**100**

NE = NISPOM Effectiveness MS = Management Support SA = Security Awareness SC = Security Community

Security Rating Score Range

Unsatisfactory	Marginal	Satisfactory	Commendable	Superior
50	70	90 - 130	131 - 150	151 - 160

TERMS AND DEFINITIONS

A **vulnerability** is an identified weakness in a contractor's security program indicating NISPOM non-compliance that, based on collected evidence and supplementary controls, could be exploited to gain unauthorized access to classified information.

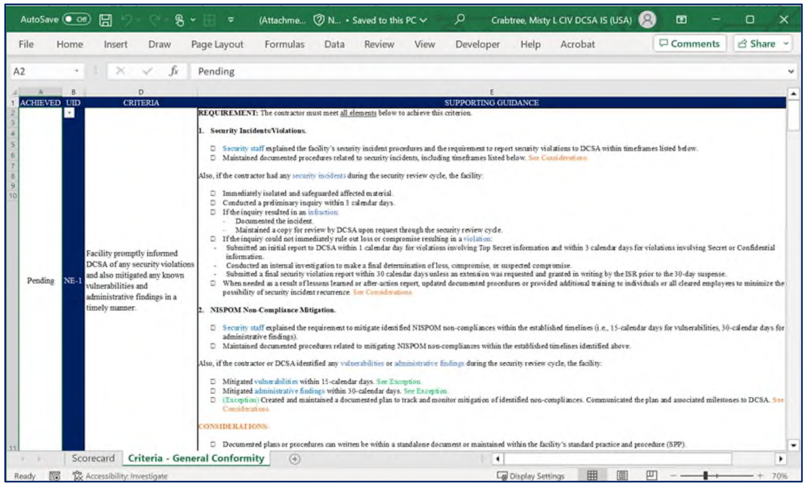
Serious security issue is an FCL relevant vulnerability that without mitigation affects a facility's ability to maintain an FCL. Serious security issues may result in an invalidation or revocation.

An **administrative finding** is an identified weakness in a contractor's security program indicating NISPOM non-compliance that, based on collected evidence and compensatory measures, could not be exploited to gain unauthorized access to classified information.

General conformity is a determination that a facility is in general compliance with the basic terms of the NISPOM indicating the facility had no critical vulnerabilities, systemic vulnerabilities, or serious security issues identified during the security review.

Provisional security rating score is the raw score prior to considering minor administrative results. If any facility has more than minor administrative results based on their complexity tier, the final security rating cannot be higher than a satisfactory with a high score of 130, the maximum allowed score.

Tab 1: Security Rating Scorecard

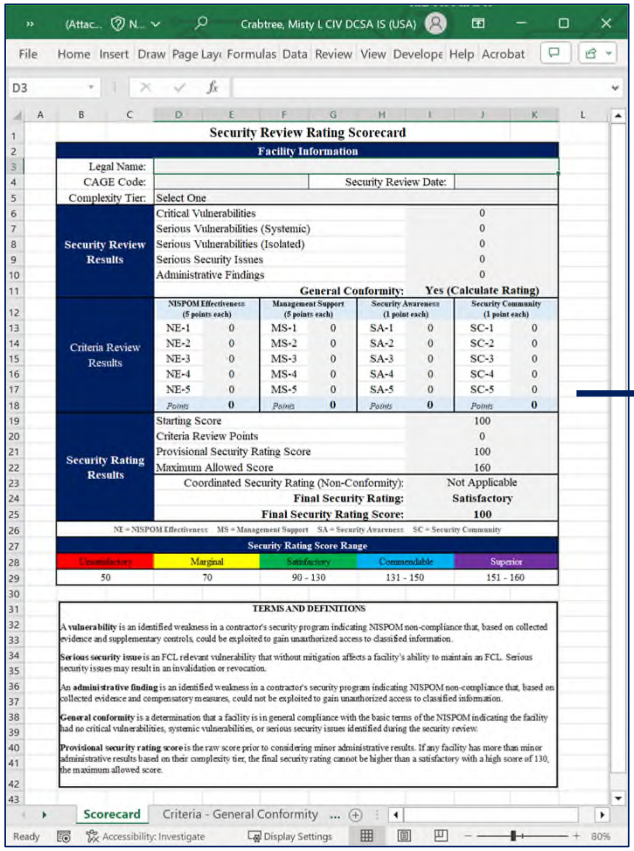


AutoSave Off (Attachme... N... • Saved to this PC Crabtree, Misty L CIV DCSA IS (USA)
File Home Insert Draw Page Layout Formulas Data Review View Developer Help Acrobat Comments Share
A2 Pending
Scorecard
Criteria - General Conformity
Ready Accessibility: Investigate Display Settings 70%

ACHIEVED	UID	CRITERIA	SUPPORTING GUIDANCE
Pending	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. 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. Also, 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 (i.e., 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. Also, if the contractor or DCSA identified any vulnerabilities or administrative findings during the security review cycle, the facility: □ Mitigated vulnerabilities within 15-calendar days. See Exception. □ Mitigated administrative findings within 30-calendar days. See Exception. □ (Exception) Created and maintained a documented plan to track and monitor mitigation of identified non-compliances. Communicated the plan and associated milestones to DCSA. See Considerations. CONSIDERATIONS: □ Documented plans or procedures can written be within a standalone document or maintained within the facility's standard practice and procedure (SPP).

Tab 2: Security Rating Criteria (General Conformity)

REFINEMENT #3: CREATED TOOL AND SCORECARD



Security Review Rating Scorecard

Facility Information			
Legal Name:			
CAGE Code:		Security Review Date:	
Complexity Tier:	Select One		

Security Review Results	Critical Vulnerabilities	0
	Serious Vulnerabilities (Systemic)	0
	Serious Vulnerabilities (Isolated)	0
	Serious Security Issues	0
	Administrative Findings	0
	General Conformity:	**Yes (Calculate Rating)**

	NISPOM Effectiveness (5 points each)		Management Support (5 points each)		Security Awareness (1 point each)		Security Community (1 point each)	
Criteria Review Results	NE-1	0	MS-1	0	SA-1	0	SC-1	0
	NE-2	0	MS-2	0	SA-2	0	SC-2	0
	NE-3	0	MS-3	0	SA-3	0	SC-3	0
	NE-4	0	MS-4	0	SA-4	0	SC-4	0
	NE-5	0	MS-5	0	SA-5	0	SC-5	0
	Points	**0**	*Points*	**0**	*Points*	**0**	*Points*	**0**

Security Rating Results	Starting Score	100
	Criteria Review Points	0
	Provisional Security Rating Score	100
	Maximum Allowed Score	160
	Coordinated Security Rating (Non-Conformity):	Not Applicable
	Final Security Rating:	**Satisfactory**
	Final Security Rating Score:	**100**

NE = NISPOM Effectiveness   MS = Management Support   SA = Security Awareness   SC = Security Community

Security Rating Score Range				
Unsatisfactory	Marginal	Satisfactory	Commendable	Superior
50	70	90 - 130	131 - 150	151 - 160

TERMS AND DEFINITIONS

A **vulnerability** is an identified weakness in a contractor's security program indicating NISPOM non-compliance that, based on collected evidence and supplementary controls, could be exploited to gain unauthorized access to classified information.

Serious security issue is an FCL relevant vulnerability that without mitigation affects a facility's ability to maintain an FCL. Serious security issues may result in an invalidation or revocation.

An **administrative finding** is an identified weakness in a contractor's security program indicating NISPOM non-compliance that, based on collected evidence and compensatory measures, could not be exploited to gain unauthorized access to classified information.

General conformity is a determination that a facility is in general compliance with the basic terms of the NISPOM indicating the facility had no critical vulnerabilities, systemic vulnerabilities, or serious security issues identified during the security review.

Provisional security rating score is the raw score prior to considering minor administrative results. If any facility has more than minor administrative results based on their complexity tier, the final security rating cannot be higher than a satisfactory with a high score of 130, the maximum allowed score.

Tab 1: Security Rating Scorecard

- Tool automatically calculates general conformity and the maximum allowed score based on information entered in the facility and security review results sections.
- Criteria Review Results section displays which criterion was and was not achieved, increasing transparency in how DCSA calculated the security rating score.
- Security Rating Score Tool is available to download on the DCSA SRRP website.

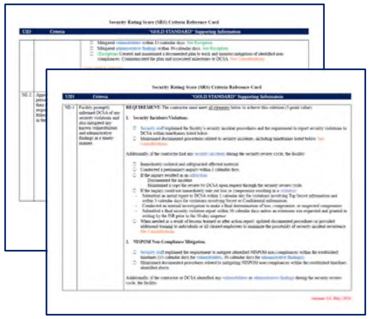
RESOURCES: WHERE TO FIND SECURITY RATING REQUIREMENTS

- 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.

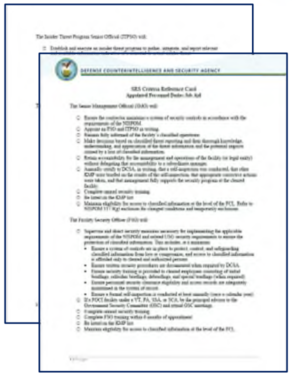
RESOURCES: WHAT YOU NEED TO KNOW!

Security Rating Process Slick Sheet

Security Rating Gold Standard Criteria



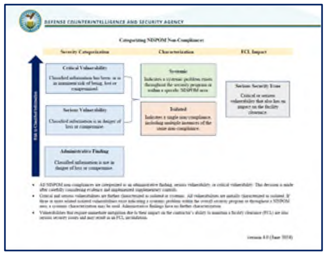
Security Rating Criteria Reference Card



Appointed Personnel Duties Job Aid

Terms and Definitions Job Aid

Security Rating Score Tool



Categorizing NISPOM Non-Compliances Job Aid

DCSA SRRP Website

REVIEW

- Understand why DCSA refined the security rating process
- Understand the top 3 security rating process refinements
- Understand the process used to calculate a score and assign a security rating
- Understand where to find security rating requirements and resources

QUESTIONS

Thank you for your participation.
Please direct additional questions to your assigned DCSA Industrial Security Representative.