Comprehensive User Guide: DCSA Security Review Rating Score Tool 2.0

July 1, 2026

An enhanced version of the Security Review Rating Score Tool is rolling out. **Please note that the Scorecard – including all gold standard criteria and associated elements – remains unchanged.** These updates apply to the calculation tool itself, focusing on streamlining the user experience, introducing smart automation, and making minor structural layout adjustments to improve clarity and communication. The goal is to improve our industry partners' awareness of how their security rating was calculated and ensure they clearly understand their areas of success and opportunities for growth.

Implementation & Impact

The table below outlines the rollout schedule and how this update impacts post-review documentation.

Phase / Topic	Details
Soft-Launch	DCSA will begin a **soft launch of the updated calculation Tool on July 1, 2026.**
Full Implementation	Full enterprise-wide implementation is expected later in Q4, FY26.
Post-Review Artifacts	This **update will not impact standard artifacts presented to contractors after security reviews currently**. DCSA will continue to provide an official letter to management, FSO Comments Sheet, and Security Review Rating Scorecard.

Target Audience

User Group	Intended Use
DCSA ISRs & Team Members	Use this tool to calculate a contractor's security rating and score after conducting a security review.
Industry FSOs	Highly encouraged to use this tool as part of their self-inspection process to calculate their own self-assessment score and rating.

Key Highlights & System Updates

While the Scorecard criteria themselves are untouched, the calculation Tool has been updated in three main areas:

Enhancement Area	What It Means For You
Improved Clarity and Structure	Layout adjustments have been made to de-clutter the interface, such as moving guidance, terms, and job aids to their own dedicated columns and tabs.
Time-Saving Automation	The tool now automatically computes statuses and color-codes progress (Pending/No/Yes), reducing manual errors and alerting the user to disqualifying factors.
Expanded Data Capacity	Increased the available selection of findings in the Scorecard dropdowns from 15 to 45 to ensure a more accurate reflection of review results.

Tab by Tab Summary of Changes

Tab	Category	Description / Impact
Tab 1: Instructions & Tips	Clarity & Structure	New tab for instructions, criteria tool tips, and auto links. Acts as a one-stop-shop.
Tab 2: Scorecard	Clarity, Data, UI	Moved from Tab 1. Increased dropdown selections for vulnerabilities to 45. Changed default review status to double dash (--) for clear visual cues.
Tab 3: Criteria	Clarity & Structure	Moved from Tab 2. Added element letters (e.g., MS-3a). Moved "Supporting Information" to a separate column. Added an "Optional Notes" column for user comments.
	Automation	Added color-coded achieved statuses (Yellow/Pending, Green/Yes, Red/No) and automatic alert notifications based on "Yes/No/N/A" inputs.
	Automation	Added automatic logic links between dependent criteria, with notes populating when triggered.
Tab 4: Terms & Definitions	Clarity & Structure	New tab housing moved definitions to declutter the main criteria sheet.
Tab 5: Job Aid	Clarity & Structure	New tab incorporating Appointed Personnel Duties, eliminating the need for external references.

How to Use the Tool

Part 1: Initial Setup Instructions

Step	Action
1	Go to the Scorecard Tab.
2	Complete the “Facility Information” section.
3	Fill out the “Security Review Results” section.
4	Look at the “General Conformity” result to decide your next steps in Part 2.

Part 2: Determine Your Rating Path

Follow the steps below based on the “General Conformity” result received in Part 1.

Path A: For a "Yes (Calculate Rating)" Result

Step	Action
1	Select the “Criteria (General Conformity)” tab.
2	Review each criterion by marking each element as Yes, No, or N/A. *(Note: Once a "No" is identified for any element in a single criterion, a red "alert" status will show, indicating you may move to the next criterion).*
3	Once all criteria have been reviewed, return to the main Scorecard tab.
4	Check that the “Criteria Review Results” section is accurate.
5	Make sure the final Scorecard is correct.

Path B: For a "No (Coordinate Rating)" Result

Step	Action
1	Coordinate a security rating of Unsatisfactory, Marginal, or Satisfactory (rare instances).
2	Find the “Security Rating Results” section.
3	Choose the rating from the “Coordinated Security Rating (Non-Conformity)” dropdown menu.
4	Make sure the final Scorecard is correct.

How to Print Scorecard (one method)

Step	Action
1	Within the "Scorecard" tab, find the "File" tab and choose the "Print" icon.
2	Verify the Printer is set to a PDF writer (e.g., Microsoft Print to PDF, Save as PDF) and "Print Active Sheets" is selected under "Settings".
3	Choose "Print" and save the Scorecard.

Criteria Tool Tips & Automation Logic

The Criteria tab uses automated logic to calculate statuses.

Input / Scenario	System Action & Visual Indicator
If Any Criterion Element Marked "No"	• Red "Alert" Status for every element within the criterion. • Red "No" Achieved Status for the overall criterion.*(Rule: Once an element is not achieved, review of remaining elements in that criterion is discontinued).*
If All Criterion Elements Marked "Yes" or "N/A"	• Green "Alert" Status for every element within the criterion. • Green "Yes" Achieved Status for the overall criterion.
If An Auto-Link Is Triggered	• Overrides previous statuses. • Red “Yes” Alert & Red "No" Achieved Status applied to affected criterion. • Orange Highlight on the triggering "No" cell. • Auto-link Note added to "Optional Notes" section.

Automated Dependency Links (Auto-Links)

Triggering Criterion Marked "No"	Trigger Reason	Automatically Restricts & Results in Red Alert
MS-3c *(SMO self-inspection certification)*	SMO failed to annually certify self-inspections.	NE-2 *(via element NE-2b: SMO Duties and Responsibilities)*
NE-3a *(Documented procedures)*	FSO failed to ensure written procedures were documented.	NE-2 *(via element NE-2c: FSO Duties and Responsibilities)*
NE-4a *(Annual self-inspections)*	FSO failed to ensure formal self-inspections were conducted.	NE-2 *(via element NE-2c: FSO Duties and Responsibilities)*

Visual Legend: Criteria Tab Word Highlights

Item	Color-Code	Description
Terms	**Blue**	Terms defined within the "Terms and Definitions" tab to assist with consistent implementation.
Considerations	**Orange**	Additional context or clarifying information to consider when determining if a contractor achieved the criterion elements.
Examples	**Purple**	Examples of how a contractor may achieve a criterion element. These are not the only ways to achieve this element, and the listed examples may change based on available programs. DCSA will always consider the intent of the element when awarding the criterion.
Manual Validation	**Dark Red**	Additional review of the criterion element or a subsequent criterion element is needed using the supporting information provided.
Auto Links	**Red**	Smart automation embedded into the Tool to streamline the user experience and foster consistency by automatically updating dependent statuses.

Terms and Definitions Reference

Term	Definition
Administrative Finding	Identified weakness in a contractor's security program indicating non-compliance with the NISPOM that, based on collected evidence and implemented supplementary controls, could not be exploited to gain unauthorized access to classified information.
Approach Vector	Methods of contact used by an adversary to execute an operation and are identified within the DCSA MCMO Matrix and Targeting U.S. Technologies report. Recommended countermeasures for each contact method are located at: https://securityawareness.usalearning.gov/cdse/matrix/index.html.
Complexity Tier	For security rating purposes, a facility's complexity tier is based on their approved safeguarding and classified information systems (IS) status. Specifically: • Tier 0: No Safeguarding • Tier 1: Safeguarding • Tier 2: Classified IS

	The complexity tier number indicates the number of serious (isolated) vulnerabilities allowed before impacting a facility's maximum allowed score.
Critical Vulnerability	Vulnerability that indicates classified information has already been, or is at imminent risk of being lost or compromised after considering evidence and supplementary controls. Critical vulnerabilities are further characterized as isolated or systemic.
Contractor Personnel	Includes cleared and uncleared employees, on-site subcontractors, on-site government personnel, and visitors (as appropriate).
Final Security Rating Score	Calculated security rating after considering the facility's maximum allowed score.
General Conformity	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.
Government Entities	Includes DCSA, Government Contractor Activities (GCA), Department of Defense Inspector General (DOD IG), and other government agencies.
Isolated (Characterization)	All vulnerabilities are initially characterized as isolated. Three or more related isolated vulnerabilities may indicate a systemic problem exists throughout the security program or within a specific NISPOM area resulting in a systemic characterization.
Management	Includes the SMO, KMP, program managers, and other management throughout the chain of command involved in classified operations.
Maximum Allowed Score	Highest security rating score allowed for a general conformity facility after considering the complexity tier and number of serious (isolated) vulnerabilities. All facilities begin with a maximum score of 160. If the facility has more serious (isolated) vulnerabilities than their complexity tier permits, the maximum allowed score drops to 130.
Provisional Security Rating Score	Raw security rating score prior to considering serious (isolated) vulnerabilities and the facility’s complexity tier.
Security Community	Includes industrial security personnel, other cleared contractors, DCSA, GCAs, or other government entities.

Security Incident	Indicates actual or potential risk to classified information and is further categorized as an infraction or violation. Security incidents typically involve a security procedure that was not in place or was not followed properly (e.g., unsecured classified documents, improper receipt of classified material, data spills).
Security Infraction	Security incident that does not result in loss, compromise or suspected compromise.
Security Staff	Includes the Chief Security Officer, Director of Security, Security Manager, FSO, ITPSO, ISSM, and others as appropriate.
Security Violation	Security incidents that result in loss, compromise, or suspected compromise.
Serious Security Issue	Vulnerability that requires immediate mitigation due to its impact on the facility's ability to maintain a facility clearance (FCL). Serious security issues may result in an FCL invalidation or revocation.
Serious Vulnerability	Vulnerability that indicates classified information is in danger of loss or compromise after considering evidence and supplementary controls. Serious vulnerabilities are further characterized as isolated and systemic.
Suspicious Contacts	Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, as well as all contacts with suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.
Systemic (Characterization)	Characterization applied to a vulnerability that indicates a systemic problem exists within the overall security program or throughout a specific NISPOM area represented by three or more related isolated vulnerabilities.
Vulnerability	Identified weakness in a contractor's security program that indicates non-compliance with the NISPOM that, based on collected evidence and implemented supplementary controls, could be exploited to gain unauthorized access to classified information. Vulnerabilities are either categorized as critical or serious.

Resources & Reference Links

Access the updated tools and reference materials by visiting the DCSA Security Review and Rating Process page (Resources tab):

- DCSA Security Review Rating Score Tool 2.0
- DCSA Security Rating Gold Standard Criteria Reference Card 2.0

For questions related to this User Guide, please contact the DCSA NISP Operations Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.