# SECURITY REVIEW AND RATINGS

## TERMS AND DEFINITIONS

| | |
|---|---|
| ADMINISTRATIVE FINDING | Identified instance of NISPOM non-compliance in which classified information is not at risk of loss or compromise. |
| APPROACH VECTOR | Method used to connect an adversary to facility personnel, information, networks, or technology in order to execute an operation. |
| COMPLEXITY TIER | For security rating purposes, a facility's complexity tier is based on their approved safeguarding and classified information systems (IS) status. Specifically:<br>• Tier 0: No safeguarding<br>• Tier 1: Safeguarding<br>• Tier 2: Classified IS<br>The complexity tier number indicates the number of serious (isolated) vulnerabilities allowed before impacting the 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. |
| FINAL SCORE | Calculated security rating score 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. To be in general conformity, a facility can have no critical vulnerabilities, systemic vulnerabilities, or serious security issues identified during the security review. |
| INDICATOR | Criteria used to select a facility for a short-notice or no-notice Security Review. |
| 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. |
| 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 a 130. |

# DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

## TERMS AND DEFINITIONS

| | |
|---|---|
| NO-NOTICE SECURITY REVIEW | Security Review prioritized at a facility based on indicators and sufficient justification presented to the Field Office Chief in advance and giving the contractor less than 24 hours' notice. |
| OBSERVATION | Issues or concerns not related to NISPOM compliance. |
| PROVISIONAL RATING SCORE | Raw security rating score prior to consider serious (isolated) vulnerabilities and the facility's complexity tier. |
| SECURITY REVIEW | Evaluation of a contractor to determine and rate NISPOM compliance, assess actions taken to ensure adequate mitigation of vulnerabilities, and provide advice on how to achieve and maintain an effective security program. The security review considers the following:<br>• What the facility is protecting related to a classified contract or program and how the contractor protects the associated elements<br>• Approach vectors applicable to the facility and measures in place to counter a potential threat<br>• Internal processes throughout the classified contract deliverable lifecycle |
| 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. |
| SHORT-NOTICE SECURITY REVIEW | Prioritized security review conducted at a facility with 24-72 hours' notice based on indicators and sufficient justification presented to the Field Office Chief in advance. |
| 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 indicating non-compliance with the NISPOM that, based on collected evidence and supplementary controls, could be exploited to gain unauthorized access to classified information or information systems authorized to process classified information. Vulnerabilities are either categorized as critical or serious. |

For more information related to the DCSA Security Review and Rating process, visit https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/Security-Review-Rating-Process/ or scan the QR Code.

DCSA SRRP Page