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.
CLASSIFIED CONTRACT	Any contract, license, agreement, or grant requiring access to classified information by a contractor and its employees for performance. A contract is referred to as a 'classified contract' even when the contract document and the contract provisions are not classified.
CLASSIFIED CONTRACT DELIVERABLE	Products or services generated in support of a classified contract.
CLASSIFIED CONTRACT DELIVERABLE LIFECYCLE	Internal processes a contractor follows when providing a deliverable related to a classified contract or program to an end customer.
CLASSIFIED CONTRACT PERFORMANCE	Action or process of doing what is required by a classified contract.
COMPLEX OPERATIONS	Facilities not assigned to the NAESOC or not eligible for a NAESOC assignment are considered to have complex operations. Key factors: safeguarding, classified information systems, critical technology (classified or unclassified support), home office facility of large complex multiple facility organization, and FOCI mitigation.
CRITICAL VULNERABILITY	Vulnerability that indicates classified information has already been, or is at imminent risk of being, lost or compromised. Critical vulnerabilities are further characterized as isolated or systemic.
DELIVERABLE	Products or services.
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.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

TERMS AND DEFINITIONS

INDICATOR	Criteria used to select a facility for a short-notice or no-notice Security Review.
ISOLATED CHARACTERIZATION	Characterization applied to a vulnerability that indicates risk to classified information is isolated in nature. All vulnerabilities are initially characterized as isolated.
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.
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: • What the facility is protecting related to a classified contract or program and how the contractor protects the associated elements • Approach vectors applicable to the facility and measures in place to counter a potential threat • 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 obtain or maintain a facility clearance. Serious security issues may result in an invalidation or revocation.
SERIOUS VULNERABILITY	Vulnerability that indicates classified information is in danger of loss or compromise. 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.
SIPOC	Suppliers, Inputs, Processes, Outputs, and Customers. The SIPOC methodology is an optional tool to identify the inputs and outputs of an internal process; determine the process owner, customers, suppliers; and establish clear boundaries for the process.
SYSTEMIC CHARACTERIZATION	Characterization applied to a vulnerability that indicates a systemic problem exists within the overall security program or throughout a specific NISPOM section after a review of all isolated vulnerabilities. This characterization indicates an elevated risk to classified information.
VULNERABILITY	Identified weakness in a contractor's security program indicating non-compliance with the NISPOM that could be exploited to gain unauthorized access to classified information or information systems authorized to process classified information.