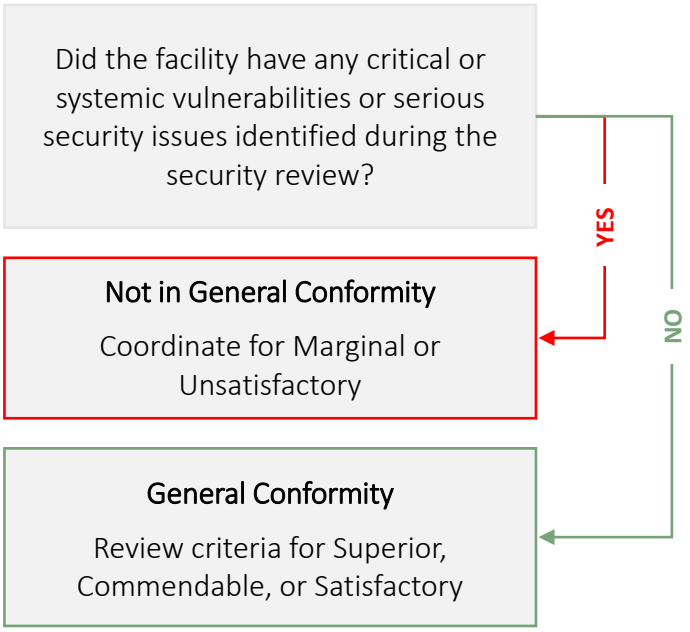
SECURITY REVIEW AND RATINGS

DCSA SECURITY RATING MODEL

DCSA's security rating model is a criteria-based system that aligns processes, terms, definitions, and minimum policy requirements. This compliance-first model eliminates the use of enhancements and uses a whole company approach based on a corporate culture of security to include management support, employee awareness, and cooperation within the security community. A formal security rating of superior, commendable, satisfactory, marginal, or unsatisfactory is provided during the security review exit briefing.

SECURITY RATING MODEL



TIPS TO ACHIEVE A SUPERIOR SECURITY RATING
BE COMPLIANT WITH 32 CFR PART 117, NISPOM RULE
MITIGATE AND DISCLOSE IDENTIFIED VULNERABILITIES
PERFORM SECURITY DUTIES AND RESPONSIBILITIES
DOCUMENT AND IMPLEMENT INTERNAL PROCEDURES
PERFORM CUSTOMIZED SELF-INSPECTIONS
IMPLEMENT CLASSIFIED INFORMATION SYSTEMS PROGRAM
EMBED A CULTURE OF SECURITY THROUGHOUT THE FACILITY
BUILD A SPIRIT OF COOPERATION WITHIN THE COMMUNITY

KEY TERMS

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

Administrative finding is an identified instance of NISPOM non-compliance that does not put classified information at risk of loss or compromise.

Serious vulnerability indicates classified information is in danger of loss or compromise.

Critical vulnerability indicates classified information has already been, or is at imminent risk of being, lost or compromised.

Isolated characterization indicates a single occurrence.

Systemic characterization indicates a widespread issue spread throughout the security program.

Serious security issue is a vulnerability that without mitigation would affect a facility's ability to obtain and maintain a facility clearance.

Complex operations is indicated by those facilities not assigned too not eligible for a National Access Elsewhere Oversight Center (NAESOC) assignment.

Refer to the Category Reference Cards for a complete list of requirements to achieve a superior, commendable, or satisfactory security rating.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DCSA SECURITY RATING MODEL

BE COMPLIANT WITH 32 CFR PART 117, NISPOM RULE

The security rating process is a compliance-first model. Critical vulnerabilities, systemic vulnerabilities, and serious security issues identified during the security review will disqualify the facility from being considered for a superior (or commendable) rating. A single 'isolated' serious vulnerability identified during the security review will disqualify a facility that does not have complex operations from being considered for a superior rating.

MITIGATE AND DISCLOSE IDENTIFIED VULNERABILITIES DURING THE SECURITY REVIEW CYCLE

Critical or serious vulnerabilities identified at the facility since the last security review must be proactively mitigated and promptly disclosed to DCSA to be considered for a superior rating. Identified vulnerabilities during the security review which were previously noted during the security review cycle but not proactively mitigated will disqualify the facility from being considered for a superior rating.

PERFORM SECURITY DUTIES AND RESPONSIBILITIES AS REQUIRED

Appointed personnel must fully and effectively perform their security duties and responsibilities outlined in 32 CFR Part 117. This includes the Senior Management Official, Insider Threat Program Senior Official, Facility Security Officer, Information Systems Security Manager (as applicable), and other employees performing security duties.

DOCUMENT AND IMPLEMENT INTERNAL PROCESSES AND SECURITY PROCEDURES

Internal security procedures must be documented in writing and effectively implemented at the facility to protect classified information and classified information systems. Contractor personnel must have a full understanding of these processes and procedures which will be validated through interviews. Contractor personnel must have a full understanding of what requires protection related to classified contracts, security classification guidance, and approach vectors applicable to them and the facility. Additionally, contractor personnel must fully understand their responsibility to protect classified information and how to identify and report events.

CONDUCT CUSTOMIZED SELF-INSPECTIONS

Formal self-inspections must be customized to facility operations and conducted using a similar process as DCSA security reviews. Self-inspections will identify gaps in security controls, determine effectiveness of implemented internal security procedures, and update processes as needed. As stated previously, vulnerabilities must be mitigated and promptly disclosed to DCSA.

IMPLEMENT CLASSIFIED INFORMATION SYSTEMS MANAGEMENT PROGRAM

Facilities with classified information systems (IS) must consistently and effectively implement a risk-based set of security controls to protect the confidentiality, integrity, and availability of classified IS, including external systems. Failing a classified IS inspection (e.g., Command Cyber Readiness Inspection) is an indication of an ineffective program and will disqualify the facility from being considered for a superior security rating. Facility must also consistently implement an effective continuous monitoring program which considers changing threats, vulnerabilities, technologies, and mission/business operations.

EMBED A CULTURE OF SECURITY THROUGHOUT THE ORGANIZATION

Building a culture of security starts with management and flows into all aspects of the facility. Management must be consistently and fully informed of approach vectors, threat information, and classified operations, and must use this information to make decisions within the facility. Management must provide security staff with appropriate resources to oversee the security program and include them in senior level meetings and when business decisions are made affecting the security program. As previously mentioned, contractor personnel must have a sustained high level of awareness regarding the security.

BUILD A SPIRIT OF COOPERATION WITHIN THE SECURITY COMMUNITY

Building a spirit of cooperation with the security community begins internally and flows into community involvement. Cooperating during official engagements or inquiries, reporting required events and those in the best interest of national security, and coordinating with stakeholders to fully understand security requirements are all required to qualify for a superior security rating. Externally, the facility must lend support to the security community and participate in security related events or training that positively impacts the security program.