SECURITY REVIEW AND RATINGS

SECURITY RATING REFERENCE CARDS

SUPERIOR RATING CRITERIA

NISPOM IMPLEMENTATION

Facility consistently, fully, and effectively implements NISPOM requirements resulting in the highest caliber of security posture.

- Facility proactively mitigates and promptly discloses to DCSA any identified vulnerability since the last security review.
- DCSA identifies no critical vulnerabilities, systemic vulnerabilities, or serious security issues during the security review.
- At most, DCSA identifies a single isolated serious vulnerability during the security review at facilities with complex operations (no vulnerabilities at facilities without complex operations).
- Appointed security personnel fully and effectively perform their duties and responsibilities.
- Facility effectively documents and implements security procedures to protect classified information and classified information systems (as applicable).
- Facility customizes formal self-inspections to facility operations and conducts them in a security review-like fashion to identify gaps in security controls, determine effectiveness in implemented procedures, and to update processes accordingly.
- Facility reviews the security program on a continuing basis and consistently implements an effective continuous monitoring program for classified information systems considering changing threats, vulnerabilities, technologies, and mission/business operations (as applicable).
- Facility consistently and effectively implements a risk-based set of management, operational, and technical controls to protect the confidentiality, integrity, and availability of classified information systems (if applicable).

MANAGEMENT SUPPORT

Facility has a sustained high level of management support for the security program.

- Management includes security staff in senior level meetings and business decisions affecting the security program.
- Management provides security staff with resources to consistently and effectively oversee the security program (as needed).
- Management is consistently and fully informed of the facility's classified operations.
- Management is consistently and routinely informed of approach vectors applicable to the facility and supports implementation of measures to counter potential threats.
- Management makes decisions based on threat reporting (classified and unclassified) and their thorough knowledge, understanding, and appreciation of threat information and potential impacts causes by a loss of classified information, classified contract deliverables, and technology.
- Senior Management Official retains accountability for the management and operations of the facility without delegation to a subordinate manager.
- Facility embeds a culture of security throughout the organization.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

SECURITY RATING REFERENCE CARDS

SUPERIOR RATING CRITERIA

SECURITY AWARENESS

Security procedures heighten awareness of contractor personnel.

Contractor personnel are aware of internal processes and security procedures and effectively demonstrates a full understanding of the following:

- What the facility and individual protects related to classified contracts and programs, security classification guidance, and approach vectors applicable to both the facility and individual (as relevant)
- Facility and individual responsibility to protect and safeguard classified information in their possession and to which they have access in accordance with government policy and contractual requirements
- Reportable events, reporting procedures, and identifies reportable events at the facility and those applicable to their role

SECURITY COMMUNITY

Facility fosters a spirit of cooperation within the security community.

- Facility consistently and proactively contributes the following actions:
- Cooperates with DCSA, Government Contracting Activities (GCA), and other government agencies (OGA) during official reviews, investigations, and inquiries
- Fully and timely reports required events to DCSA and OGAs, and engages to support the interest of the national security community beyond policy and contractual requirements
- Coordinates with prime contractors, GCAs, User Agencies (UA), and others to gain a full understanding of security classification guidance
- Lends support to the security community to maintain the viability and effectiveness of industrial security program
- Participates in security community events, conferences, and webinars that positively impact the security program
- Aims to achieve and maintain cooperation within the security community beyond contractual requirements

---

A **vulnerability** is an identified weakness in a contractor's security program that indicates non-compliance with the NISPOM that could be exploited to gain unauthorized access to classified information or information systems authorized to process classified information. This is not referring to administrative findings which are instances of NISPOM non-compliance that do not put classified information at risk.

A **critical vulnerability** is a 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.

A **systemic** characterization is assigned to a critical or serious vulnerability that is part of a systemic issue spread throughout the security program.

A **serious security issue** is a vulnerability that without mitigation would affect a facility's ability to obtain and maintain a facility clearance. Serious security issues may result in an invalidation or revocation.

A **serious vulnerability** is a vulnerability that indicates classified information is in danger of loss or compromise. Serious vulnerabilities are further characterized as isolated or systemic.

Facilities are determined to have **complex operations** if they are not assigned to the National Access Elsewhere Security Oversight Center (NAESOC) or are otherwise not eligible for a NAESOC assignment.

An **approach vector** is a method used to connect an adversary to facility personnel, information, networks, or technology in order to execute an operation.