

SECURITY REVIEW AND RATINGS

SECURITY RATING REFERENCE CARDS

COMMENDABLE RATING CRITERIA

NISPOM IMPLEMENTATION

Facility **fully and effectively** implements NISPOM requirements resulting in an exemplary security posture.

- 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.
- Appointed security personnel effectively perform their duties and responsibilities.
- Facility effectively implements security procedures to protect classified information and classified information systems (as applicable).
- Facility conducts formal self-inspections in accordance with risk management principles to identify gaps in security controls, determine effectiveness of implemented procedures, and to update processes accordingly.
- Facility reviews the security program on a continuing basis and implements an effective continuous monitoring program for classified information systems considering changing threats, vulnerabilities, technologies, and mission/business functions (if applicable).
- Facility 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 **strong level** of management support for the security program

- Management includes security staff in business decisions affecting the security program.
- Management provides security staff with resources to effectively oversee the security program (as needed).
- Management is fully informed of the facility's classified operations.
- Management is periodically informed of approach vectors applicable to the facility and supports 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 caused by a loss of classified information and technology.
- Senior Management Official retains accountability for the management and operations of the facility without delegation to a subordinate manager.
- Facility implements a culture of security throughout the organization.



SATISFACTORY



COMMENDABLE



SUPERIOR





DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

SECURITY RATING REFERENCE CARDS

COMMENDABLE RATING CRITERIA

SECURITY AWARENESS

Security procedures improve awareness of contractor personnel.

- Contractor personnel are aware of internal processes and security procedures, and demonstrates an understanding of the following:
- What the facility and individual protects related to classified contracts and programs, security classification guidance, and approach vectors applicable to the facility (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 customer requirements
- Reportable events, reporting procedures, and identifies reportable events at the facility and those applicable to their role

SECURITY COMMUNITY

Facility proactively cooperates with the security community.

- Facility proactively contributes the following actions:
- Cooperates with DCSA, GCA, and OGAs during official reviews, investigations, and inquiries
- Fully and timely reports required events to DCSA and OGAs as outlined in government policy and customer requirements
- Coordinates with prime contractors, GCAs, UAs, and others to gain an understanding of security classification guidance
- Participates in security community events, conferences, and webinars that positively impact the security program

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.

