



DCSA SECURITY REVIEW AND RATING PROCESS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

**Critical Technology Protection Directorate
National Operations**



**DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY** |

Agenda



- Security Review
 - Background
 - Model Overview
 - Objectives
- Security Rating
 - Model Overview
 - Process Flow
 - Step-by-Step Process
 - Roadmap to Commendable and Superior
- Resources

Security Review Background



- Information Security Oversight Office Letter
- Security Review Defined
- Benefits of Security Review
- Periodically refine the security review methodology to ensure processes align to national level policy
- Establish consistent, repeatable, and scalable security review procedures (by the field for the field)

Security Review Model Overview



- Aligns to minimum policy requirements outlined in DoDM 5220.22, Volume 2
- Functions within the DCSA charter of compliance while identifying risks posed throughout classified contract performance
- Incorporates best practices from previous security review models (e.g., DSS in Transition, Risk-based Industrial Security Oversight, Security Vulnerability Assessments)
- Prioritizes security reviews based on national level priorities (i.e., DoD Critical Program and Technology List) and risk management

Security Review Objectives



Review internal processes

Evaluate NISPOM compliance to identify vulnerabilities and administrative findings

Discuss approach vectors applicable to the facility and assess countermeasures

Advise the contractor on how to achieve and maintain an effective security program

Assess corrective actions taken by the contractor to mitigate previously identified vulnerabilities

Rate the facility's security posture

Evaluate classified information system plans, artifacts, and security controls

(when applicable)

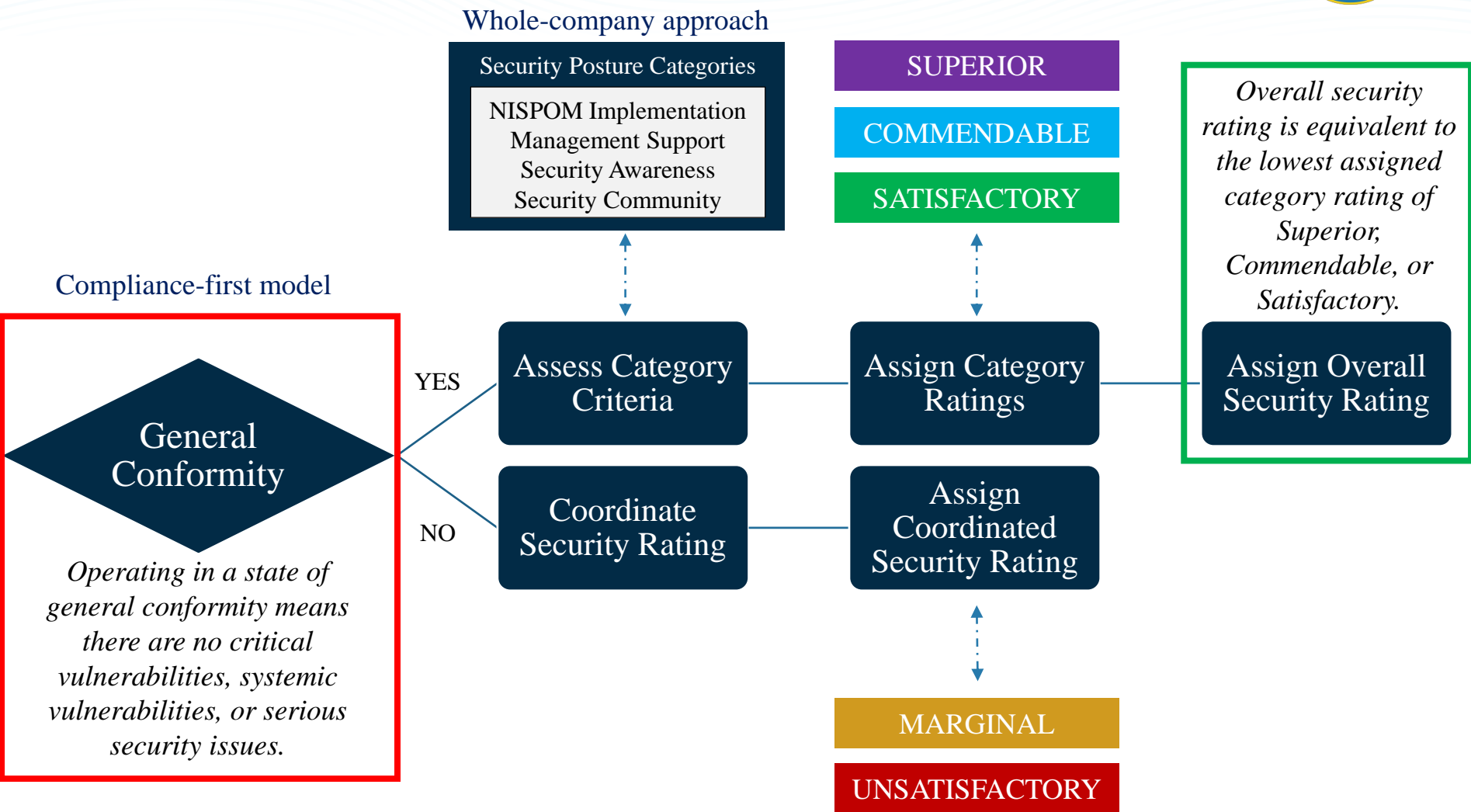
Security Rating Model Overview



- Criteria-based system that aligns processes, terms and definitions, and minimum requirements to national level and DOD policy
- Scalable, repeatable, transparent, and defensible process
- Clear standards to ensure consistency with ability for professional judgement
- Process is supported by information (evidence) collected, or knowledge obtained, during normal progression of security review
- Five-tier ratings and no enhancements (compliance-first, whole-company approach)
- Process-based rating replaces numeric score
- Designed to give all contractors the same opportunity to achieve a higher level rating



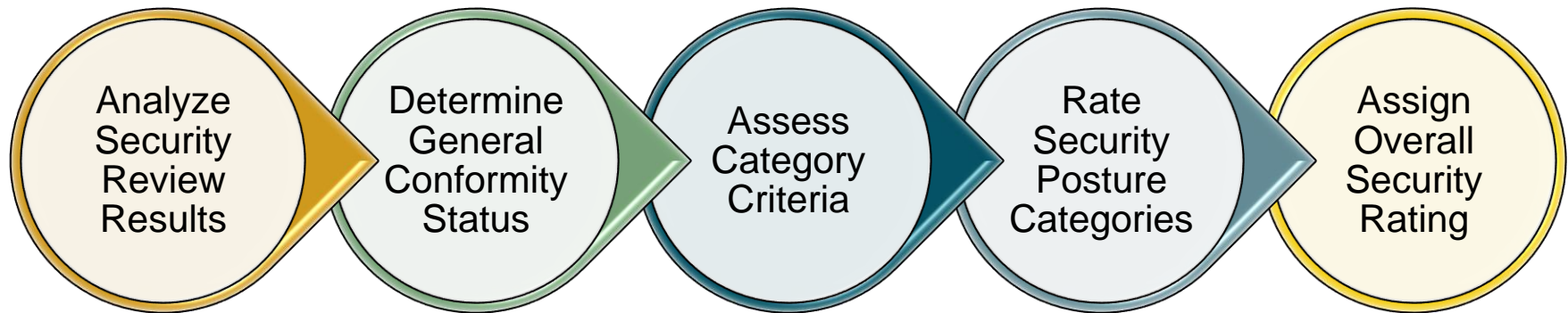
Security Rating High-Level Process Flow



Security Rating Step-by-Step Process



Using the information collected and knowledge obtained during the normal progression of the security review, DCSA personnel:



Category Reference Cards



SECURITY REVIEW AND RATINGS

CATEGORY REFERENCE CARDS

NISPOM IMPLEMENTATION

SUPERIOR

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).

COMMENDABLE

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).

SATISFACTORY

Facility is in **general conformity** with the basic terms of the NISPOM resulting in an acceptable security posture.

- DCSA identifies no critical vulnerabilities, systemic vulnerabilities, or serious security issues during the security review.
- At most, DCSA identifies isolated serious vulnerabilities in one or more security elements of the overall security program.
- Appointed security personnel adequately perform their duties and responsibilities.
- Facility implements a system of security controls to protect classified information and classified information systems
- Facility has self-inspection and continuous monitoring programs (as applicable).
- Facility has a risk-based set of management, operational, and technical controls to protect the confidentiality, integrity, and availability of classified systems (if applicable).

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY



Security Posture Category

Superior Level Criteria

Commendable Level Criteria

Satisfactory Level Criteria



Roadmap to a Superior Rating

General
Conformity

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

2 MANAGEMENT SUPPORT
Facility maintains a sustained high level of management support for the security program.

3 SECURITY AWARENESS
Documented and implemented procedures heighten security awareness of contractor personnel.

4 SECURITY COMMUNITY
Facility fosters a spirit of cooperation within the security community.

**SUPERIOR
SECURITY RATING**

All facilities have an opportunity to achieve a superior level rating.

Refer to the Category Reference Cards and Roadmap to a Superior Rating document located on the DCSA Security Review and Rating page.

<https://www.dcsa.mil/mc/ctp/srrp/>

Security Rating Sheet



Security Rating Sheet

Facility Name: **Lily, LLC** Date: **9/7/21**
 CAGE Code: **12XX1** Category: **D** Complex¹: **Yes**

Security Review Results Overview	
Critical Vulnerabilities ²	0
Serious Vulnerabilities ³ (Systemic)	0
Serious Vulnerabilities (Isolated)	1
Serious Security Issues ⁴	0
Administrative Findings ⁵	2
General Conformity ⁶	Yes
Security Posture Rating Overview	
NISPOM Implementation Category	Satisfactory
Management Support Category	Commendable
Security Awareness Category	Commendable
Security Community Category	Superior
Overall Security Rating⁷	Satisfactory

¹Complex operations indicates a facility is not assigned to, or eligible for an assignment to, the National Access Elsewhere Security Oversight Center (NAESOC).

²Critical vulnerability indicates classified information has already been, or is at imminent risk of being, lost or compromised.

³Serious vulnerability indicates classified information is in danger of loss or compromise.

⁴Serious security issue is an FCL relevant vulnerability that without mitigation would affect a facility's ability to obtain and maintain a FCL. Serious security issues may result in an invalidation or revocation.

⁵Administrative finding is an identified instance of NISPOM non-compliance that does not put classified information at risk of loss or compromise.

⁶General conformity is a determination that a facility is in general compliance with the basic terms of the NISPOM and the facility had no critical vulnerabilities, systemic vulnerabilities, or serious security issues identified during the security review.

⁷Facility is assigned one security rating. All criteria must be met at, or above, the rating level to be assigned the rating. To support process improvement efforts and transparency purposes, category ratings are provided; however, the overall rating cannot exceed the lowest category rating.

Note: This rating summary is based on activities and findings of the associated security review. Refer to additional security review artifacts for more information.

Facility Information

Security Review Results

Category Ratings and Overall Security Rating

Terms and Definitions



Additional information related to the security review and rating process, including the below webinars, are available at

<https://www.dcsa.mil/mc/ctp/srrp/>

- CDSE “Understanding the DCSA Security Review and Security Rating Process” webinar recorded on June 24, 2021
- DCSA “Security Rating Process” webinar recorded on September 16, 2021



Thank you for your participation.

For more information visit the
DCSA Security Review and Rating page at
<https://www.dcsa.mil/mc/ctp/srrp/>.