DCSA Security Review and Rating Process

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Mr. Jeremy Hargis, Senior Industrial Security Representative

DCSA Security Review Model

- DCSA's security rating model is a criteria-based system that aligns processes, terms, definitions, and minimum requirements to DoD and National-level policy.

- This compliance-first model uses a whole-company approach based on a corporate culture of security, including management support, employee awareness, and cooperation within the security community.

- The refined security review approach incorporates best practices from previous security review models to verify compliance with the NISP Operating Manual (NISPOM), while identifying risks posed throughout classified contract performance.

Objectives of the DCSA Security Review

- Evaluate NISPOM compliance

- Review internal processes throughout a classified contract product or service lifecycle

- Evaluate classified information system security controls and identify gaps in security controls

- Identify vulnerabilities and administrative findings, then monitor and track corrective actions

Objectives of the DCSA Security Review

- Identify potential approach vectors and assess countermeasures
- Provide updates and advice on how to create and maintain an effective security program
- Rate the facility's security posture and effectiveness in protecting classified information
- Classified Contract Deliverable Lifecycle (CCDL) is a part of the security review. DCSA will review at minimum one CCDL during the security review.

Classified Contract Deliverable Lifecycle

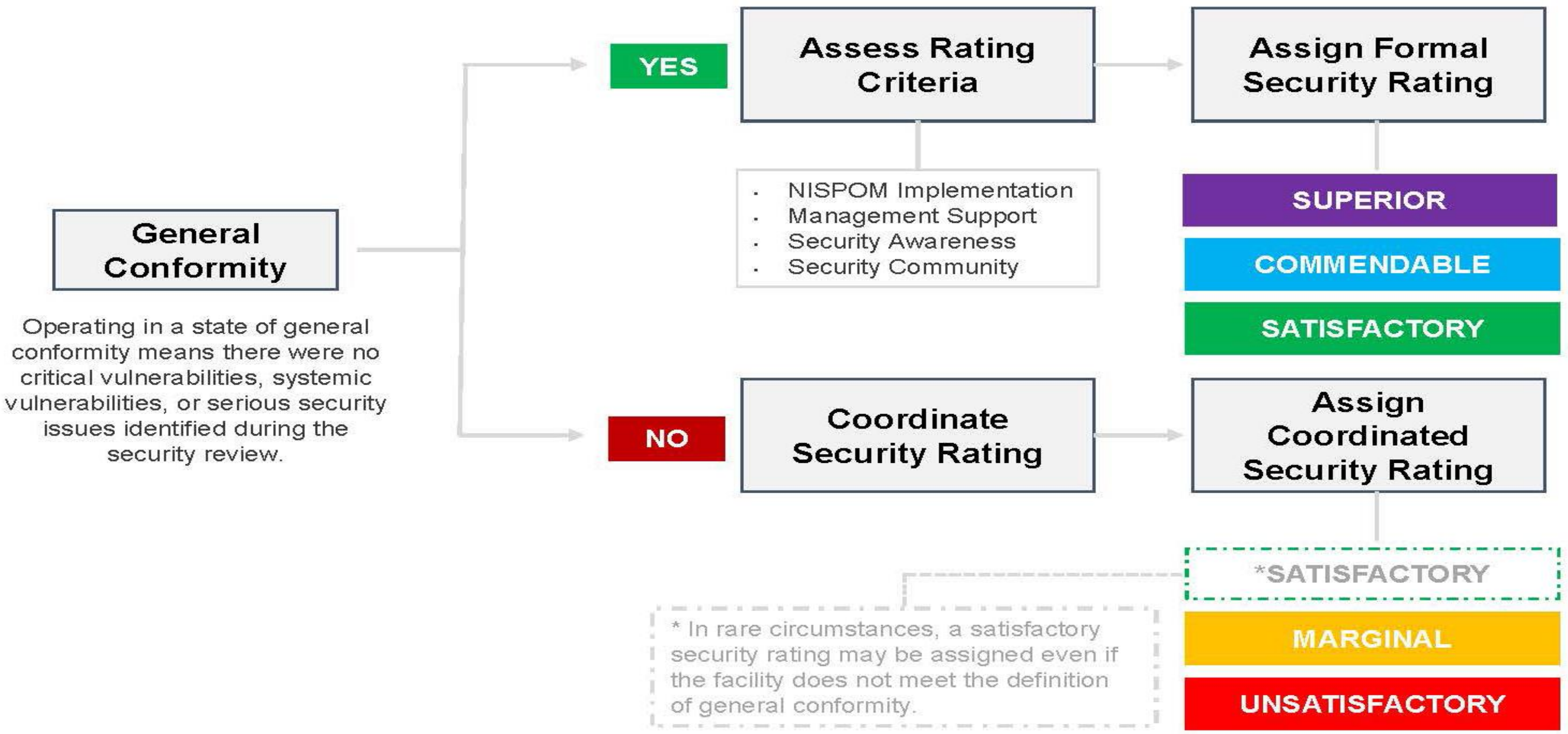
- Classified contract deliverable lifecycles (CCDL) are the collective internal processes a contractor follows from start to finish to provide products and services related to a classified contract or program to an end customer.

- The primary purpose of the CCDL review is to:

  - Assess the facility's NISPOM compliance/general conformity.

  - Identify possible approach vectors and determine if measures are in place to counter a potential threat.

DCSA Security Rating Process Flow



General Conformity

Operating in a state of general conformity means there were no critical vulnerabilities, systemic vulnerabilities, or serious security issues identified during the security review.

YES

Assess Rating Criteria

- NISPOM Implementation
- Management Support
- Security Awareness
- Security Community

Assign Formal Security Rating

SUPERIOR

COMMENDABLE

SATISFACTORY

NO

Coordinate Security Rating

Assign Coordinated Security Rating

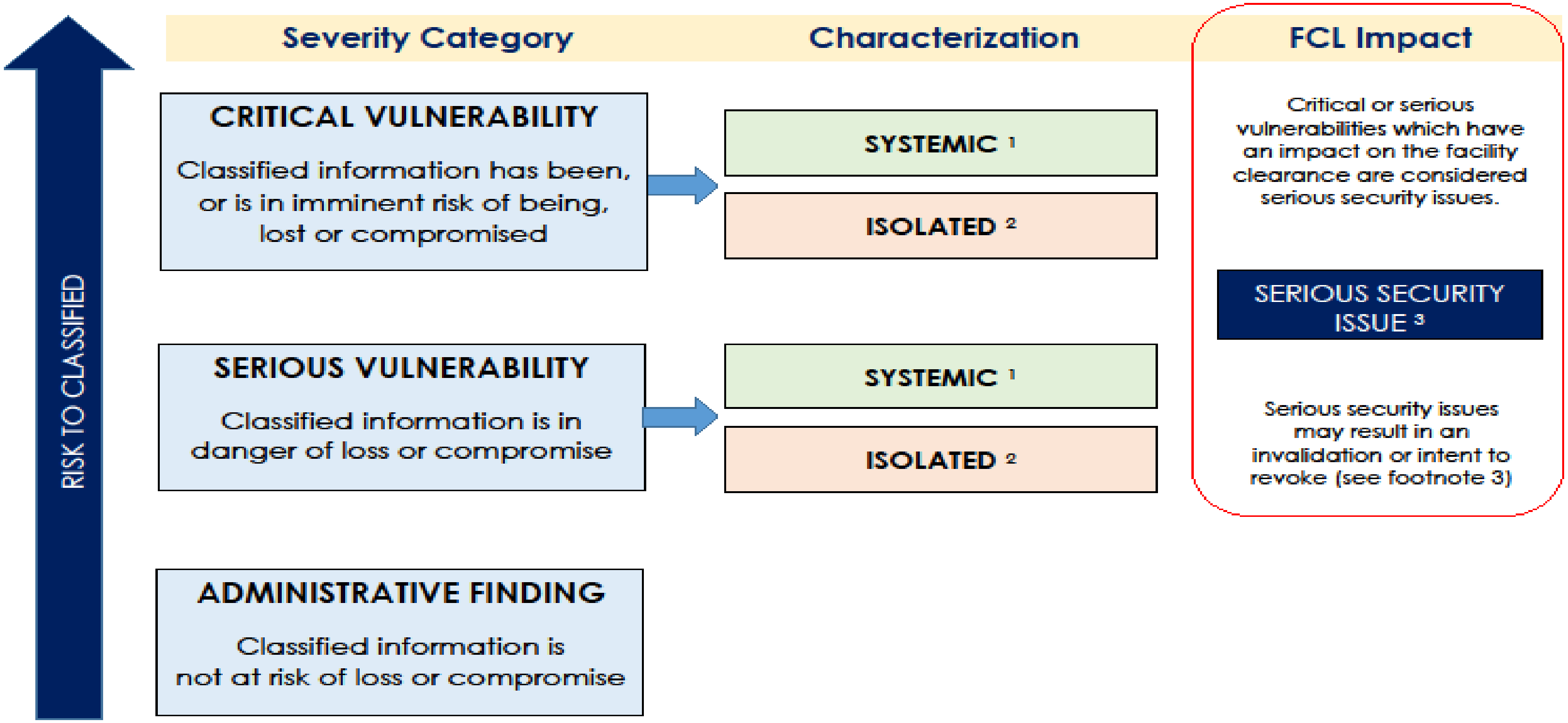
*SATISFACTORY

MARGINAL

UNSATISFACTORY

* In rare circumstances, a satisfactory security rating may be assigned even if the facility does not meet the definition of general conformity.

Identifying Vulnerabilities, Administrative Findings, and Serious Security Issues



RISK TO CLASSIFIED

Severity Category

Characterization

FCL Impact

CRITICAL VULNERABILITY

Classified information has been, or is in imminent risk of being, lost or compromised

SYSTEMIC [1]

ISOLATED [2]

SERIOUS VULNERABILITY

Classified information is in danger of loss or compromise

SYSTEMIC [1]

ISOLATED [2]

ADMINISTRATIVE FINDING

Classified information is not at risk of loss or compromise

Critical or serious vulnerabilities which have an impact on the facility clearance are considered serious security issues.

SERIOUS SECURITY ISSUE [3]

Serious security issues may result in an invalidation or intent to revoke (see footnote 3)

1. Systemic is a 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.
2. Isolated is a characterization applied to a vulnerability that indicates risk to classified information is isolated in nature. All vulnerabilities are initially be characterized as isolated.
3. Serious security issue is a 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.

Version 3.0 (November 2022)

Preparing for a DCSA Security Review

- Engage with your ISR prior to the review to discuss focus areas, logistics, questions etc.

- Update your NISS profile with current and accurate information and focus on program information/DD 254, at a minimum of a week prior to the date of the review.

- Ensure your most recent self-inspection SMO certification is available in NISS.

- If DCSA requests information prior to the review, provide the information promptly which will assist the ISR with conducting an efficient and effective review.

Most Common Instances of Non-Compliance

- **117.10(a)(3)** – Determination of Eligibility for Access to Classified Information for Contractor Employees – DISS Management
- **117.7(h)(2)** – Procedures: Security Reviews – Contractor Reviews
- **117.8(c)** – Reporting Requirements: Reports to Be Submitted to the CSA
- **117.18(b)** – Information System Security: IS Security Program
- **117.12(g)** – Security Training and Briefings: Insider Threat Training
- **117.7(b)** – Procedures Contractor Security Officials
- **117.19(g)(7)** – International Security Requirements: NATO Information Security Requirements
- **117.12(k)** – Security Training and Briefings: Refresher Training
- **117.7(d)** – Procedures: Insider Threat Program
- **117.10(b)(5)** – Determination of Eligibility for Access to Classified Information for Contractor Employees - Reinvestigation and Continuous Eval

Questions ?

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY