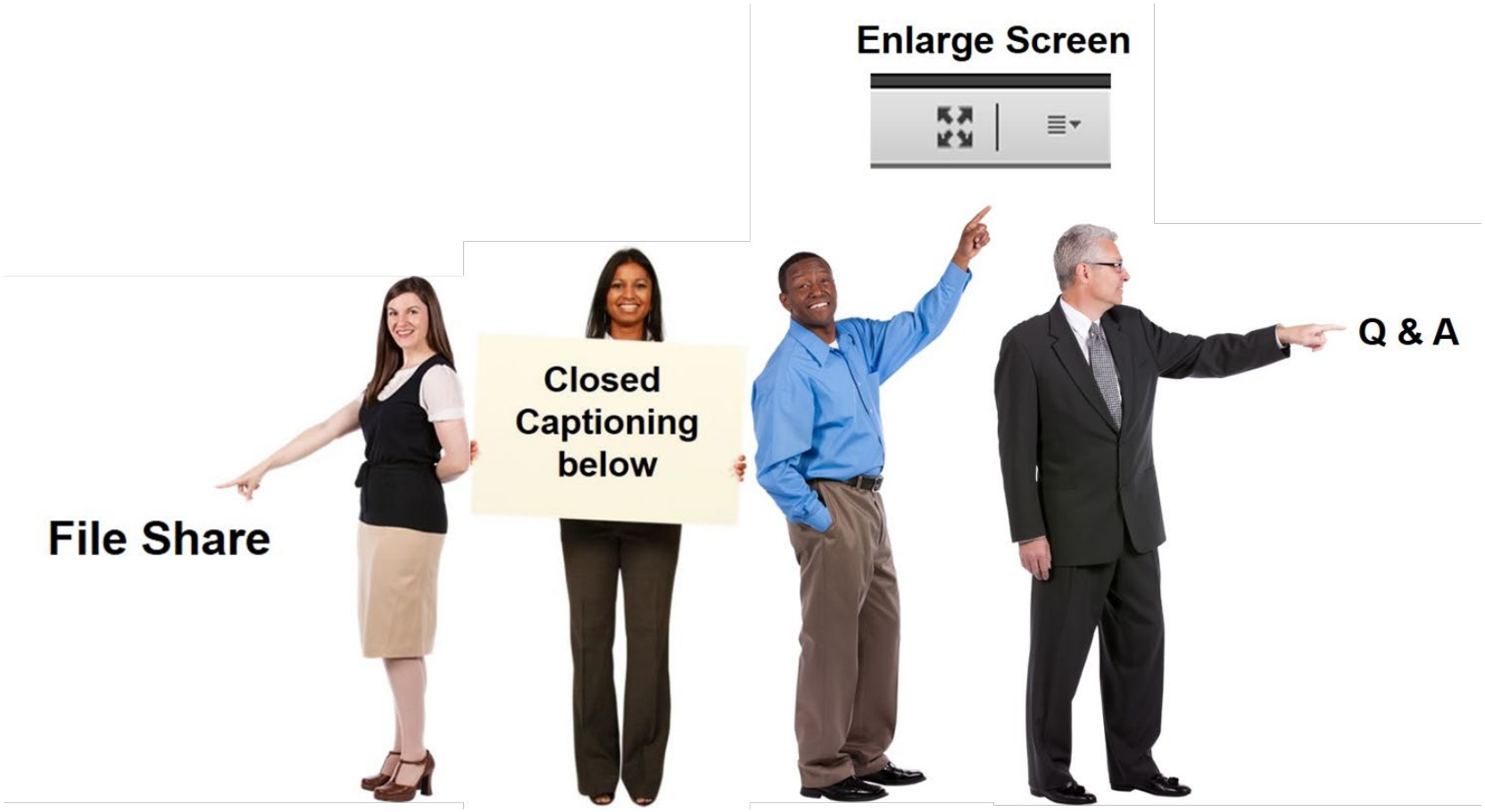
DCSA CDSE WEBINAR

SECURITY REVIEW AND RATING PROCESS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Critical Technology Protection Directorate
National Operations

Adobe Connect



Welcome

- Today's Team

  Host: Jason Steinour, CDSE Industrial Security Curriculum Manager

  Speaker: Kevin Williamson, DCSA Operations Branch Chief

  Speaker: Ryan Franklin, DCSA Operations Action Officer

  Speaker: Misty Crabtree, DCSA Senior IS Rep

  Speaker: Matthew Roche, DCSA Operations Division Chief

Agenda

- Security Review Background
- Security Review Model
- Terminology
- Security Review Objectives
- Contractor Activities
- Security Rating Model

Poll Question #1 and #2

- How many DCSA security reviews have you participated in?
  - 0
  - 1
  - 2
  - 3 or more

- How knowledgeable are you on the current DCSA security rating and review process (1 low - 5 high)?
  - 1
  - 2
  - 3
  - 4
  - 5

Security Review Background

- Provide GCAs with assurance their contractors are eligible for access to classified information and maintain foundational security practices
- Conduct security reviews (and other engagements) to help DCSA understand a cleared contractor's internal security processes associated with their classified contract performance
- 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 and risk management

Security Review Terminology

Vulnerability	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. (Severity: Critical or Serious)
Serious Security Issue	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.
Administrative Finding	Identified instance of NISPOM non-compliance that does not put classified information at risk. Administrative findings may be elevated to a vulnerability as situationally relevant.
General Conformity	Facility is in general compliance with the basic terms of the NISPOM and have no critical vulnerabilities, systemic vulnerabilities, or serious security issues identified during the security review.
Approach Vector	Method used to connect an adversary to facility personnel, information, networks, or technology in order to execute an operation.

Poll Question #3

- How long ago was your facility's last security review?
  - I don't know
  - 1 year
  - 2 years
  - 3 or more years

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)

High-Level Contractor Activities

Before

- Coordinate and confirm security review date
- Submit updates to NISS facility profile
- Discuss what the facility is protecting related to classified contracts and programs

During

- Coordinate and participate in entrance briefing
- Discuss classified contract deliverable lifecycles and approach vectors applicable to the facility
- Discuss internal processes, countermeasures, and security controls
- Begin mitigating vulnerabilities and administrative findings
- Coordinate and participate in exit briefing

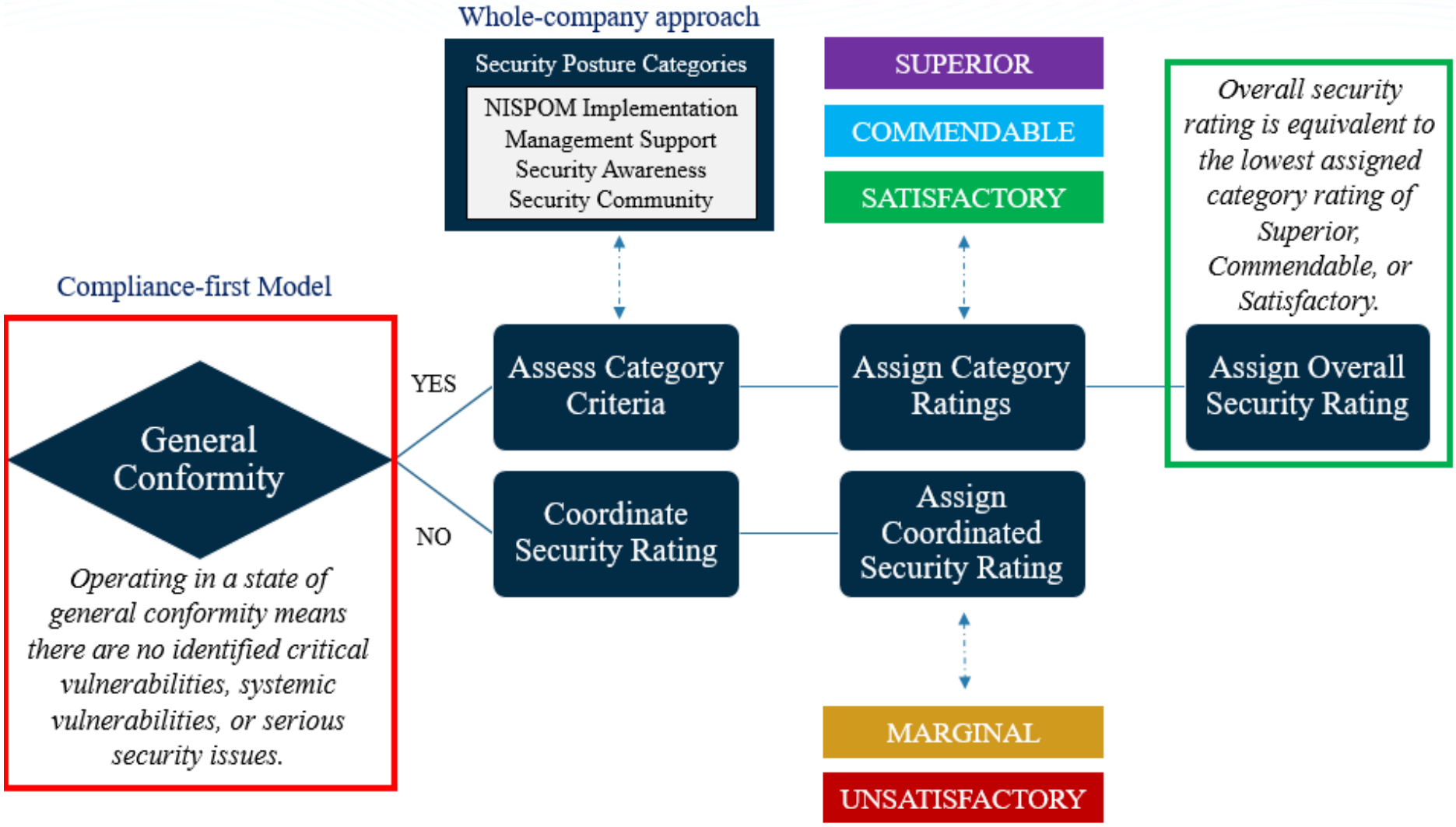
After

- Provide a written response of corrective actions
  - *Vulnerabilities = 15 calendar days from the exit briefing*
  - *Administrative findings = 30 calendar days from the exit briefing*

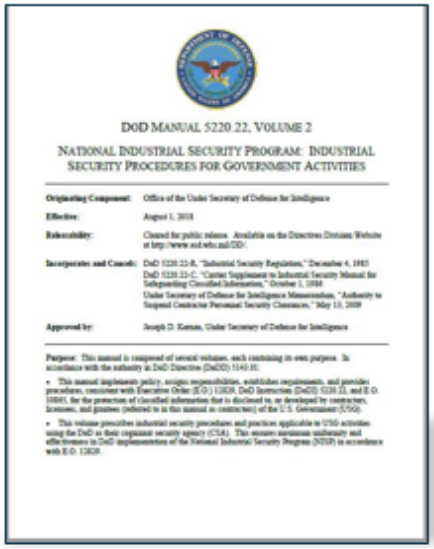
Security Rating Overview

- Criteria-based system that aligns processes, terms and definitions, and minimum requirements to national level policy
- Scalable, repeatable, transparent, and defendable process
- Designed to give all contractors the same opportunity to achieve a superior rating
- 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

Security Rating High-Level Process Flow



Security Rating Policy Requirements



DoD MANUAL 5220.22, VOLUME 2

NATIONAL INDUSTRIAL SECURITY PROGRAM: INDUSTRIAL SECURITY PROCEDURES FOR GOVERNMENT ACTIVITIES

DODM 5220.22, Volume 2
"National Industrial Security Program: Industrial Security Procedures for Government Activities"

Superior Security Rating

- Reserved for contractors that have consistently, fully, and effectively implemented the requirements of the NISPOM
- Requires sustained high level of management support of the security program
- Must have documented and implemented procedures that heighten the security awareness of contractor employees
- Must foster a spirit of cooperation within the security community
- Cannot be assigned if any serious security issues or systemic vulnerabilities are identified during the security review
- At most, can only have minor administrative results with complex operations

Using Policy to Develop Rating Categories

Superior Policy Requirements	Security Posture Categories
Consistent, full, and effective NISPOM implementation	NISPOM Implementation
Sustained high level of management support for the security program	Management Support
Documented and implemented procedures that heighten security awareness	Security Awareness
Spirit of cooperation within the security community	Security Community

Also contains Superior "must not haves" which include critical vulnerabilities, systemic vulnerabilities, or serious security issues.

* As outlined in DODM 5220.22, Volume 2

Using Category Ratings to Calculate Overall Rating

1 Criteria used to assign category ratings

Superior	Commendable	Satisfactory
Sustained High Level	Strong Level	Basic Level

All criteria must be met at, or above, the rating level to be assigned the category rating.

2 Category ratings used to assign overall rating

	Category Rating	Overall Rating
NISPOM Implementation	Satisfactory	Satisfactory
Management Support	Commendable	
Security Awareness	Superior	
Security Community	Commendable	

Security Rating Calculation Example

Calculated as the lowest category rating

All criteria must be met at, or above, the rating level to be assigned the overall rating.

Category ratings are provided for transparency and process improvement purposes.

Poll Question #4

- Do you have a better understanding of the new DCSA security review and rating process?
  - Yes
  - No
  - Unsure

Questions

Thank you for your participation.