

Industrial Security Webinar Series

Learn @ Lunch



**Defense Security Service
Security Rating Matrix**

Learn @ Lunch

CDSE

Security Rating Process Overview

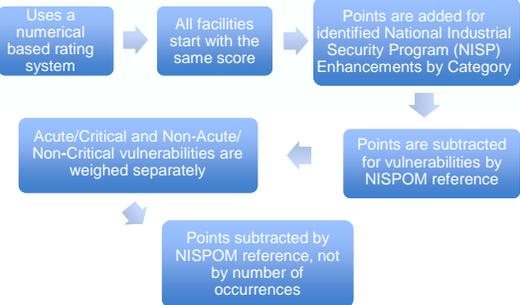
- New security rating process implemented November 2011
- More standardized and less subjective rating process
- Numerically based, quantifiable, and accounts for all aspects of a facility's involvement in the National Industrial Security Program (NISP)



Learn @ Lunch

CDSE

How Does the Matrix Work?



```
graph TD; A[Uses a numerical based rating system] --> B[All facilities start with the same score]; B --> C[Points are added for identified National Industrial Security Program (NISP) Enhancements by Category]; C --> D[Points are subtracted for vulnerabilities by NISPOM reference]; D --> E[Points subtracted by NISPOM reference, not by number of occurrences]; E --> F[Acute/Critical and Non-Acute/Non-Critical vulnerabilities are weighed separately];
```

Learn @ Lunch CDSE

How Does the Matrix Work?

Each ratings matrix comes with a “scoring key” that is based on the facility category

Learn @ Lunch CDSE

Scoring

	CAT AA, A, B, C			CAT D, E		
	Starting Score →		700	Starting Score →		700
Items Exceeding Baseline NISPOM Requirements		X 12	+		X 15	+
Non-Acute/Critical Vulnerability by Reference*		X 2	-		X 4	-
Acute/Critical Vulnerability by Reference*		X 12	-		X 20	-
	FINAL SCORE →			FINAL SCORE →		

599 & Below = Unsatisfactory
 600 - 649 = Marginal
 650 - 749 = Satisfactory
 750 - 799 = Commendable
 800 & Above = Superior

Learn @ Lunch CDSE

Security Rating Process Terminology

Acute Vulnerability



- Non-compliance with a NISPOM requirement that puts classified information at imminent risk of loss or compromise.
- Acute vulnerabilities require immediate corrective action.

Learn @ Lunch CDSE

Security Rating Process Terminology

Critical Vulnerability

- Non-compliance with a NISPOM requirement that places classified information in danger of loss or compromise.



Learn @ Lunch CDSE

Acute/Critical Vulnerabilities

- 1) Acute
- 2) Critical
 - a. Isolated
 - b. Systemic
 - c. Repeat

- Once a vulnerability is determined to be acute or critical, it is further categorized as either "Isolated", "Systemic", or "Repeat".

Learn @ Lunch CDSE

Security Rating Process Terminology

Acute/Critical Vulnerability

Isolated

- Single occurrence
- Resulted in or could logically lead to the loss or compromise of classified information



Learn @ Lunch CDSE

Security Rating Process Terminology

Acute/Critical Vulnerability

Systemic

- Deficient in multiple areas as a result of there not being a process in place, or an existing process is not adequately designed to comply.



Learn @ Lunch CDSE

Security Rating Process Terminology

Acute/Critical Vulnerability

Repeat

- Is a repeat of a specific occurrence identified during the last review that has not been properly corrected.
- Note: Documented as critical, as it demonstrates non-compliance.



Learn @ Lunch CDSE

Security Rating Process Terminology

All Other Vulnerabilities

Non-compliance with a NISPOM requirement that does not place classified information in danger of loss or compromise



Learn @ Lunch CDSE

NISP Enhancement Definition

A **NISP enhancement** relates to and enhances the protection of classified information beyond baseline NISPOM standards.

Learn @ Lunch CDSE

NISP Enhancement Definition

- NISP enhancements will be validated during the assessment as having an **effective impact** on the overall security program, which is usually accomplished through employee interviews and review of processes/procedures.

Learn @ Lunch CDSE

NISP Enhancement Definition

- DSS established 13 NISP Enhancement Categories, based on practical areas, to simplify and ensure field consistency.

Learn @ Lunch CDSE

NISP Enhancement Definition

- Full credit for a NISP Enhancement (15 or 12 points depending on facility complexity) will be given if a facility completes any action/item in a given category.
- The facility will only receive a total of 15/12 points per category, regardless of how many NISP Enhancements they have in a given category.

Learn @ Lunch CDSE

NISP Enhancement Categories

1: Security Education (Company Sponsored Events)	7: CI Integration/Cyber Security
2: Security Education: Internal Educational Brochures/Products	8: Information Systems
3: Security Education: Security Staff Professionalization	9: FOCI
4: Security Education: Information/Product Sharing within Community	10: International
5: Self Inspection	11: Membership/Attendance in Security Community Events
6: Classified Material Controls/Physical Security	12: Active Participation in the Security Community
	13: Personnel Security

Learn @ Lunch CDSE

Red Flag Items

▪ DSS considers some factors as “red flag areas” and the rating calculation score may not be applicable.



Learn @ Lunch CDSE

Red Flag Items

- For example:
 - Unmitigated or unreported FOCI
 - Uncleared persons in KMP positions requiring clearance
 - Intentional disregard of NISPOM regulations
 - Acute or Critical systemic vulnerabilities w/potential loss/compromise
 - Any additional items which may result in invalidation of the FCL
 - Matrix score leading to marginal or unsatisfactory rating

Learn @ Lunch CDSE

Security Rating Updates

- Updates published on DSS internet
- Security Matrix FAQ on DSS internet
 - http://www.dss.mil/isp/fac_clear/security-rating-matrix.html
- New Security Matrix Calculation Worksheet
 - New security vulnerability terminology
- Gathering lessons learned and quality trend data for future rating matrix revisions
 - NISP Enhancement Advisory Committee
 - Goal is to continually improve our rating process while ensuring consistency and transparency

Learn @ Lunch CDSE

Feedback Link

industrialsecurity.training@dss.mil

Learn @ Lunch 

Thank You for Joining Us

Future Webinar Topics and Dates:
<http://www.dss.mil/cdse/catalog/webinars/index.html>
