

Industrial Security Webinar Series



Defense Security Service Security Rating Matrix



Security Rating Matrix

Security Rating Process Overview

It was recognized by all levels within DSS and Industry that we needed a standardized, less subjective rating process. The new security rating calculation tool is intended to standardize and improve consistency in our rating process.

We are committed to your success and the success of the National Industrial Security Program (NISP)—this is a transparent process. Full transparency on how DSS has arrived at a rating (e.g., breakdown in vulnerabilities and positive NISP enhancements identified) will be provided and discussed.

The matrix tool is numerically based, quantifiable, and accounts for all aspects of a facility's involvement in the NISP.

How Does The Matrix Work?

The Rating Matrix uses a numerical based rating system.

All facilities start with the same score (700).

Points are added for identified NISP enhancements by Category.

Points are subtracted for vulnerabilities by NISPOM reference.

Acute/Critical and Non-Acute/Non-Critical vulnerabilities are weighed separately.

Note: Points are subtracted by NISPOM reference, not by number of occurrences.

The Scoring Key

The rating calculation worksheet accounts for size and complexity in scoring values. “One size does not fit all.” A larger company receives slightly less amount of credit for NISP enhancements and vulnerabilities, whereas a smaller company receives a slightly higher amount of credit for NISP enhancements and vulnerabilities.



Security Rating Matrix

The Scoring Range

The scoring range is as follows: 599 & Below = Unsatisfactory.

An acute vulnerability is defined as non-compliance with a NISPOM requirement that puts classified information at imminent risk of loss or compromise. Acute vulnerabilities require immediate corrective action. **A critical vulnerability** is defined as non-compliance with a NISPOM requirement that places classified information in danger of loss or compromise. Once a finding is determined to be acute or critical, it is further categorized as either “Isolated”, “Systemic”, or “Repeat.”

Isolated – Single occurrence that resulted in or could logically lead to the loss or compromise of classified information.

Systemic – Specific requirement is 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. For instance, if a security program was one-third deficient in a specific area across the program, it would be considered systemic.

Repeat – Is a repeat of a specific occurrence identified during the last review that has not been properly corrected. Note: Although some repeat vulnerabilities may be administrative in nature and not directly place classified information at risk to loss or compromise, it is documented as critical as it demonstrates non-compliance.

All other Vulnerabilities are defined as non-compliance with a NISPOM requirement that does not place classified information in danger of loss or compromise.

NISP Enhancement Definition

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

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 process/procedures.

Security Rating Matrix

We have established 13 NISP enhancement Categories, based on practical areas, to simplify and ensure field consistency. (The goal is to have a well rounded security program.)

The result is to give credit to the true impact of the security enhancements, rather than attempt to consistently break-down each isolated event.

A company will receive full credit (15 or 12 points depending on facility complexity) if any action/item is implemented in a given category.

The facility will only receive a total of 15/12 points per category, regardless of how many NISP enhancements are implemented in a given category.

NISP Enhancements

As you are aware, NISP enhancements were broken down into Categories, based on practical areas, to simplify and ensure field consistency. (The goal is to have a well rounded security program.) The result is to give credit to the true impact of the security enhancements, rather than to attempt to consistently break-down each individual isolated event.

Provide a brief description of each Category:

National Industrial Security Program Enhancements are as follows:

Category 1-4: Security Education: In addition to the annual required security refresher briefings.

Category 1: Security Education (Company Sponsored Events) - The facility holds company sponsored events such as "security fairs, interactive designated security focused weeks, security lunch events, hosting guest speakers on security related topics, webinars with the security community, etc."

Category 2: Security Education: Internal Educational Brochures/Products - A security education and awareness program that provides enhanced security education courses or products to the entire employee population (may include unclassified employees) (i.e., CD/ DVDs, web-based interactive tools, newsletters, security games/contests, international security alert system, etc.).

Category 3: Security Education: Security Staff Professionalization - Security staff training exceeds NISPOM/DSS requirements, to include obtaining ongoing professional certifications and incorporating the knowledge throughout the program. (Certified Protection Professional (CPP), SPeD Certification, additional CDSE courses, Computer Information Systems Security Professional (CISSP), etc.).

Security Rating Matrix

Category 4: Security Education: Information/Product Sharing within Community - The FSO provides peer training support within the security community and/or shares security products/services with other organizations both within and outside their corporate family.

Category 5: Self Inspection - Effective documented self inspections are designed to provide an ongoing, continuous evaluation of the security program. Promptly sharing the self inspection results with DSS encourages open dialogue of identified issues and possible resolutions prior to the DSS scheduled assessment.

Category 6: Classified Material Controls/Physical Security - The facility has deployed an enhanced process for managing classified information with built-in countermeasures to identify significant anomalies, such as 100% inventory on random basis or Information Management System (IMS) indefinitely reflects history of location and disposition for material in facility of all classification (100% accountability).

Category 7: CI Integration/Cyber Security - Foreign travel pre-briefings and debriefings conducted (when not a contractual requirement) or implementation of quality assurance efforts to check and verify SCR training, reporting directions and employee knowledge (e.g., setting up appropriate simulated exercises to validate employee knowledge/situational awareness of SCR reporting process).

Category 8: Information Systems - Developing and implementing significant and effective (LAN/WAN based) IS audit trail reduction/collection or analysis tools/scripts internally and sharing across the corporation or NISP community at large.

Category 9: FOCI - Security programs that perform significant trend analysis of governance processes and interactions with the foreign parent company. (Companies that utilize trend analysis and follow-on audit programs to proactively identify and report attempts of undue influence, identify weaknesses, best practices, and areas for improvement.)

Category 10: International - Facility voluntarily conducts, or has outside experts conduct, ongoing export compliance audit and shares the results with interested U.S. Government Agencies.

Category 11: Membership/Attendance in Security Community Events - Security staff are members of and attend meetings of professional NISP organizations, such as ISAC, NISPPAC, NCMS, AIA, NDIA, ISWG, FOCI working groups, etc.

Category 12: Active Participation in the Security Community - The FSO or other key security personnel or key management personnel actively participates in and contributes to security-related professional organizations beyond merely being a member of the organizations, such as being elected on security community boards (i.e., President of ISAC/NCMS Chapter, committee/board member of ISAC/NCMS, etc.).

Security Rating Matrix

Category 13: Personnel Security - Implementation of a corporate wide call center or centralized process established to support employee questions and issues related to CSA designated databases (JPAS, e-QIP, etc.). (If asked for an example of how a smaller company can achieve credit in Category 13, provide the following: Enhanced ongoing security, personnel, and adverse information record checks when submitting e-QIP packages to verify accuracy and completeness that go beyond typical open source records checks.

Red Flag Items

DSS considers some items, if identified during the assessment, as a “red flag area,” and the rating Matrix score may not be applicable. If certain items are identified, the field representative will not assign the security rating at the conclusion of the assessment and internal coordination will take place. As you can see, these items may demonstrate a significant lack of compliance and may have an impact on the overall facility security clearance status.

Security Rating Updates

We post updates to the FAQs and security rating matrix calculation worksheet on the DSS website for industry awareness. Recently the rating calculation worksheet was updated with the new security vulnerability terminology.

We regularly gather quality trend data to ensure consistency and lessons learned for future rating matrix improvements.

Recently we instituted a NISP enhancement advisory committee to review NISP enhancement consistency and to formulate ideas for improvements. The goal is to continually improve our rating process while ensuring consistency and transparency.