Defense Security Service

Facility Security Rating Matrix
Frequently Asked Questions

February 2012

1. Why is the Defense Security Service (DSS) introducing the Security Rating Calculation tool?

The new security rating calculation tool is intended to standardize and improve consistency in the rating process. The matrix tool is numerically based, quantifiable, and accounts for all aspects of a facility’s involvement in the National Industrial Security Program (NISP).

2. How is DSS ensuring consistent application of the tool throughout the country?

DSS has created detailed guidance to DSS field offices on the application and use of the tool. DSS is also taking proactive steps to ensure all DSS industrial security personnel are fully trained prior to implementation of this tool. Additionally, DSS will internally share experiences and feedback on the tool in order to validate and assess the effectiveness of the tool. DSS is also reaching out to industry through a variety of forums to ensure that cleared contractors understand the process and intent of the tool.

3. How does DSS define “Vulnerabilities”?

If a contractor is not in compliance with the requirements of the NISPOM, DSS will identify the issue as either an “Acute Vulnerability”, a “Critical Vulnerability” or a “Vulnerability”.

The following further defines each category:

<u>Acute Vulnerability:</u> Those vulnerabilities that put classified information at imminent risk of loss or compromise, or that have already resulted in the compromise of classified information. Acute vulnerabilities require immediate corrective action.

<u>Critical Vulnerability:</u> Those instances of NISPOM non-compliance vulnerabilities that are serious, or that may foreseeably place classified information at risk or in danger of loss or compromise.

Once a vulnerability is determined to be Acute or Critical, it shall be further categorized as “Isolated”, “Systemic”, or “Repeat”.

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

Systemic-Deficiency or deficiencies that demonstrate defects in an entire specific subset of the contractor's industrial security program (e.g., security education and awareness, AIS security) or in the contractor's overall industrial security program. A systemic critical vulnerability could be the result of the contractor not having a required or necessary program in place, the result of an existing process not adequately designed to make the program compliant with NISP requirements, or due to a failure of contractor personnel to comply with an existing and adequate contractor policy.

Repeat- Is a repeat of a specific occurrence identified during the last DSS security assessment 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.

Vulnerability: All instances of non-compliance with the NISPOM that are not acute or critical vulnerabilities.

4. Are vulnerabilities which are corrected on the spot counted on the Security Rating Matrix tool?

Yes. DSS will document and count each corrected on the spot (COS) vulnerability and points will be subtracted on the matrix form. It is important in the DSS review of contractor NISP programs that the steps taken to correct vulnerabilities and the measures implemented to prevent recurrence of those vulnerabilities are fully documented. Additionally, if the vulnerabilities prove to be 'repeat' at subsequent DSS assessments, they are categorized as critical and additional point reductions will occur. DSS encourages contractors to correct all vulnerabilities expeditiously. DSS will appropriately note those items as COS in the security assessment report and a written response to DSS on corrective actions will not be required.

6. What is a National Industrial Security Program (NISP) "enhancement"?

An enhancement directly relates to and enhances the protection of classified information beyond baseline NISPOM standards. Point credits are given for these procedures and factored into the overall assigned rating. Items to be documented as "NISP enhancements" must relate directly to the NISP, and do not include other commonplace security measures or best practices. NISP enhancements (also commonly referred to as "exceeding" or "above and beyond") must be validated during the security assessment as having an effective impact on the overall NISP program in place at the company. This validation is usually accomplished through employee interviews and review of processes/procedures by DSS.

There are often positive areas or best practices of a security program that DSS identifies as noted improvements, but which are not necessarily related to a company's involvement with the NISP. Often these positive areas, or best practices, are enhanced processes implemented in order to adequately manage a security program due to the size or complexity of a facility. DSS will ***not*** be counting these items toward point calculation on the rating matrix worksheet as "NISP enhancements." However, DSS will recognize these improvements, efforts, and other notable best practices during the exit briefing with senior management and the FSO.

7. What are the definitions of each NISP Enhancement Category?

DSS has established 13 NISP Enhancement categories. A breakdown of categories and examples are provided below. The examples provided in each category are not all-inclusive list and are being provided to provide clarity on category definitions.

Category 1-4: Security Education: Training conducted 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, webinar with 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 uncleared employees) (i.e., CD/DVD, 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 and DSS requirements to include obtaining on-going professional certifications and incorporating the knowledge through the program. (Certified Protection Professional (CPP), SPeD Certification-additional CDSE courses, Computer Information Systems Security Professional (CISSP), etc.).

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

Category 5: Contractor Self Review- Effective documented self reviews designed to provide an on-going, continuous evaluation of the security program, and promptly sharing the contractor self review results with DSS, which encourages open dialogue of identified issues and possible resolutions prior to the DSS scheduled assessment.

Category 6: Classified Material Controls/Physical Security- Facility has deployed an enhanced process for managing classified information which has built in countermeasures to identify significant anomalies. Examples include 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: Counterintelligence 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 training on suspicious contact reporting (SCR), and employee knowledge (e.g., setting up appropriate exercises to validate employee knowledge/situational awareness of SCR reporting process)

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

Category 9: FOCI- Security programs that perform significant trend analysis of internal 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, on-going 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 or other security organizations such as Industrial Security Awareness Councils, professional societies and associations for security professionals, 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 Chapter, committee/board member of ISAC, etc.).

Category 13: Personnel Security- Implementation of a corporate wide call center or centralized process established to support employee questions and issues related to Cognizant Security Agency (CSA) designated databases (JPAS, EQIP, etc.).

8. Why were NISP enhancements further broken down by Category?
NISP enhancements were broken down into Categories, based on practical areas, to simplify and enable consistency of application of this tool by DSS personnel. 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. The intent is for a company to receive full credit for a NISP Enhancement (15 or 12 points depending on facility complexity) if a facility completes any action/item in a given category. The facility will only receive a total of 15 or 12 points per category, regardless of how many NISP enhancements they have in a given category.

9. Will DSS provide a copy of the Security Rating matrix worksheet and scoring at the completion of the assessment?

Yes. DSS will release the populated worksheet attached to the assessment results letter given to the FSO. Full transparency on how DSS arrived at a rating, (e.g. break-down in vulnerabilities and positive NISP enhancements identified) will be provided. The security rating of record will be discussed with the FSO and senior management official during the exit briefing. The exit briefing discussion will focus on identifying the security vulnerabilities and required corrective actions, NISP enhancements, and on providing suggested improvements where possible.

10. Will DSS provide a complete listing of what is considered a NISP Enhancement?

No. Although an all-inclusive master list of NISP Enhancement items cannot be created, DSS will periodically provide cleared industry notices with identified trends analysis of both NISP enhancements and security vulnerabilities. Additionally, a sample of the rating matrix calculation tool is available, with examples for each category.

11. Are there any variables that would impact the final security rating outside of the security rating calculation worksheet?

Yes. There are a number of items to be considered as "red flags" which, if identified, may have a significant impact on the final security rating and possibly the status of the facility clearance. Therefore if such vulnerabilities are identified, the rating matrix score may not be applicable. The assigned Industrial Security Representative (ISR) will review with his or her DSS supervisor the final rating of record to be issued, before it is issued to the cleared company "Red flag" items include, but are not limited to, unreported/unmitigated FOCI, appointment of a senior management official without required eligibility for access to classified information, deliberate disregard for security requirements, acute and critical systemic vulnerabilities that lead to the potential or actual loss or compromise of classified information and any additional items that may result in the invalidation of the FCL.

12. What does category level on the rating calculation worksheet mean?

DSS assigns category levels to facilities based on a variety of considerations, most of which relate to the complexity of a facility and its level of involvement in the NISP. Facilities which possess classified material on-site are ranked from category "AA" (the largest and most complex industrial facilities) and descend by size/complexity through categories "A," "B," and "C" to category "D" (the lowest category ranking for a facility which possesses classified material on-site.) Facilities which do not possess classified material are category "E." A facility category level will be indicated on the rating calculation worksheet provided with assessment results letter.

13. If vulnerabilities are identified at my company during a security assessment, what is the next step?

DSS will request that the company provide a written response outlining procedures or policies put in place to correct any identified vulnerabilities. If an acute or critical vulnerability is identified, immediate corrective actions must be taken. DSS may also schedule a follow-up visit to the company to validate the effectiveness of the corrective actions taken.