Webinar Questions and Answers

Industry Rating Matrix Webinar 25 July 2013

Webinar guests submitted several questions before and during the 25 July, 2013 Industry Rating Matrix Webinar session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: The matrix is nice that it gives more points for enhancements, but it also appears to deduct more points for findings...is that correct?

Answer: The matrix update continues the same concept as the previous matrix, but the point values differ based upon your facilities complexity, the scope of your security program and level of involvement in the NISP. The overall point values granted for enhancements and deducted for vulnerabilities changed as a result of the reduction of enhancement categories from 13 to 10.

Question: Is the ISP distinction from NCMS an enhancement?

Answer: Successful completion of the ISP certification, or maintain continuing education credits for the ISP will be eligible for NISP Enhancement Category 3, Security Staff Professionalization. You may also receive credit for partial completion of a training program (beyond base training requirements per NISPOM 3-102 and 8-101b) if security relevant courses applicable to one's duties are accomplished.

Question: I will be assessed in August. How will this upcoming matrix change affect my upcoming assessment?

Answer: The Rating Matrix Phase Two will not be implemented until September 1st. If you are assessed in August, you will be assessed with the current 13 category rating matrix.

Question: Do you get credit for more than one item in each category is it not easier to get a good rating if you have 5 documents rather than 50?

Answer: The intent is to give credit to the true impact of the security enhancements, rather than to attempt to consistently break-down each individual isolated event. A company will receive full credit for a NISP Enhancement (15 or 17 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 17 points per category, regardless of how many NISP enhancements they have in a given category.

Question: If you host a CI briefing does it count for CI and Education? So can one thing cover two categories?

Answer: No, hosting a CI brief would only be applicable to Category 1, Security Education.

Hosting a CI brief does not meet the intent of the Category 7, CI integration which is to encourage cleared contractors to develop vigorous and effective CI programs that thwart foreign attempts to acquire classified and sensitive technologies. Critical elements of a vigorous and effective CI program include timely reporting, understanding the threat environment, and agile and authoritative decision making to neutralize or mitigate vulnerabilities and threats. Further examples of Category 7 are available via http://www.dss.mil/documents/facility-clearances/Vuln_Assm_Rating_Matrix_2013_Update.pdf .

Question: How can a non-possessing facility receive a superior rating under the revised matrix?

Answer: A non-possessing facility can earn a superior rating under the revised matrix by being compliant with all requirements of the NISPOM and achieving six (6) NISP Enhancements. Based on industry feedback regarding the current matrix, DSS separated out the non-possessing facilities on the matrix to ensure they are not compared to possessing facilities.

Question: Is there an appeals process for DSS Assessments?

Answer: If you disagree with your assessment rating, you can elevate your concerns to the local Field Office Chief.

Question: Why are enhancement points an "all or nothing"?

Answer: Intent is to give credit to the overall impact to the facility's security environment and the local security community, not give credit for each action that led to the overall impact of the facility's security environment.

Question: After DSS completes your Vulnerability Assessment, is the FSO supposed to receive a copy of the completed rating matrix from the assessment?

Answer: 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 assessment 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.

Question: Is there a minimum of courses that you need to take in order to get credits?

Answer: There is not a minimum of courses required to obtain credit for Category 3: Staff professionalization. However, you will need to demonstrate how taking the classes furthered your professional security expertise beyond mandatory requirements.

Question: Do webinars and/or security shorts count towards Category 3 Enhancements?

Answer: Yes, webinars and some security shorts may count if they EFFECTIVELY further the professional's security expertise beyond mandatory requirements and found effective at the time of the assessment.

Question: I am JPAS and SWFT Account Manager for 120 locations within my company. They call all the time for help, does this count?

Answer: If it is part of your job duties to support the other locations within your corporate structure then this is not an enhancement under the revised Rating Matrix. Intent of Category 5: Active Membership in Security Community is to encourage cleared contractors to actively reach out to other cleared contractors to assist those who may not have the expertise or budget and provide them with security products, services, etc.

Question: Security Professionalization...does this have to be for a certification or can we take classes in CDSE just to improve our knowledge?

Answer: This may be either obtaining and maintaining a professional certification or taking CDSE classes as long as the intent to further the professional's security expertise beyond mandatory requirements is met and found effective at the time of the assessment.

Question: What sources are available for creating internal education brochures/products?

Answer: There are many great resources provided by the Center for Development of Security Excellence (CDSE) www.cdse.edu and your local ISACs or NCMS chapters.

Question: Are there procedures for having the self-inspections reported to DSS?

Answer: No, there are no standardized procedures for reporting self-inspections to DSS.

Question: I was told by my last rep that we must send two signed self-audits per year in order to receive credit on the matrix. Is this true?

Answer: This may have been a recommendation by your ISR to help you achieve this enhancement. The intent of this category is to encourage cleared contractors to maintain an

effective, on-going self-review program to analyze and identify any threats or vulnerabilities within their program and coordinate with DSS to address those issues prior to the annual assessment.

Examples of this enhancement include:

- Providing DSS a detailed report of their self-review to include identified threats or vulnerabilities, analysis, and countermeasures to mitigate vulnerabilities, and collaborates with DSS to correct prior to the annual assessment.
- Multiple documented self-reviews providing an on-going, continuous evaluation of the security program.
- Establish an internal corporate review program conducted by another facility within the organizational/corporate structure in addition to the required self-review.
- Self-review conducted by a cleared contractor outside of the corporate structure, i.e. prime contractor assisting a subcontractor or a consultant with an applicable need-to-know (DD254).

Question: With security events that focus specifically on CI, which category would that count toward? Are there any single events/instances that count for more than one category?

Answer: Depending on the event, it would count toward the appropriate security education enhancement. For example, if you have a guest speaker come present a CI briefing, then that would be a Category 1 enhancement. Single instances typically count for one category.

Question: I was told during my last review that having an Export Control audit from an outside agency would count as an enhancement. Would that still be true for Category 8 enhancements?

Answer: Yes, facilities that voluntarily conduct, or has outside experts conduct, ongoing export compliance audit and shares the results with interested U.S. Government Agencies are eligible for a Category 8 enhancement. Additional examples of the Category 8 enhancement include:

- Facilities that perform significant trend analysis of internal governance processes and interactions with the foreign parent company and affiliates. Contractor uses this trend analysis and follow-on audit programs to proactively identify and report attempts of undue influence to DSS, to identify weaknesses and best practices.
- Facility maintains an enhanced ongoing export control self-inspection program**.**

Questions: Is it still best practice to retain the least amount of holdings as possible?

Answer: This is not considered an enhancement. Per NISPOM 5-700b: "Contractors shall establish procedures for review of their classified holdings on a recurring basis to reduce these classified inventories to the minimum necessary."

Questions: Regarding Category 9, we are non-possessing facility. If we have a policy for handling and managing controlled unclassified information as an addition to the TCP, can this be considered here or would it apply to Category 8 here?

Answer: No. Non-possessing facilities are not eligible to receive enhancement credits for areas that are not assessed during a DSS assessment (i.e. classified material controls) as these are areas where the facilities are not assessed and do not receive cited vulnerabilities.

Questions: Is there a website that's just for rating information?

Answer: Updates posted on the DSS website. Current update may be found at http://www.dss.mil/about_dss/news/20130627.html

Questions: Is there a list of associations recommended to join?

Answer: There is no DSS-endorsed list of associations but some security organizations you may consider would include your local Industrial Security Awareness Council (ISAC), local National Classification Management Society (NCMS) chapter, and American Society for Industrial Security (ASIS). Your DSS ISR may also have knowledge of the local security organizations.

Question: How does Cat 8 relate to facilities w/out FOCI? It seems to be a disadvantage to those facilities.

Answer: With the matrix update, the previous FOCI and International enhancement categories of were combined so now cleared contractors that are either under a FOCI mitigation instrument or export controlled items are eligible to receive credit for Category 8. The matrix calculations were formulated so that facilities without FOCI or export controlled items are not at a disadvantage and may still be eligible to receive a superior rating.

Question: Can we get more examples of non-acute vulnerabilities vs. acute & critical?

Answer: Acute vulnerabilities are those vulnerabilities that put classified information at imminent risk of loss or compromise, or that have already resulted in the compromise of classified information. An example would be posting classified information on the internet. Critical vulnerabilities are 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. An example may be systemic non-compliance to perform weekly audits on accredited information systems. Non-acute/non-critical vulnerabilities are all instances of non-compliance with the NISPOM that are not acute or critical vulnerabilities. An example would be failure to provide your employees with the DoD hotline information.

Question: For professionalization is there a number of classes or activities DSS will look for?

Answer: There is no specific number of classes required as long as the intent of this category which is to encourage security program's key personnel to actively strive to learn more and further their professional security expertise beyond mandatory requirements are met.