2016 DSS Vulnerability Assessment Rating Matrix
Vulnerabilities and NISP Enhancement Categories

Incorporating Change 2 (published May 18, 2016)

Please note: This revision includes updates from NISPOM Change 2 and ISL 2016-02. Updates have been highlighted in red. Edits have been made based on revisions to NISPOM references, new contractor requirements for implementation of an Insider Threat Program, and changes to the requirements of a contractor self-review. You will notice omission of the example of contractors providing their self-inspection results to DSS prior to the annual SVA as a potential NISP Enhancement area. Contractors are now required to prepare a formal report describing the results of the self-inspection, and a senior management official will certify to DSS in writing on an annual basis that a self-inspection has been conducted (please refer to NISPOM 1-207 'Security Reviews' for additional information on these updates).

In addition, you will notice omission of the example of implementation of an insider threat program under Category 7a as an example of a NISP Enhancement. This is now a NISPOM requirement and all contractors must establish and maintain an insider threat program, designate an Insider Threat Program Senior Official (ITPSO), and train their cleared employees accordingly (please refer to NISPOM 1-202 for additional information).

Lastly, with the transition to the Risk Management Framework (RMF), many of the enhancements contained within Section 10 (IS) will become requirements within the 800-53 controls. The NISP Authorization Office (NAO), formerly ODAA, will provide a later update to the Rating Matrix to coincide with the transition to RMF that will include enhancements applicable to systems accredited under the Risk Management Framework.

Please submit any questions or comments to dss.quantico.dss-isfo.mbx.qao@mail.mil

Vulnerability Assessments

Overview:

The National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. nse industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. DSS administers the NISP on behalf of the Department of Defense and 31 other federal agencies. There are approximately 12,800 contractor facilities that are cleared for access to classified information.

Per National Industrial Security Program Operating Manual (NISPOM) 1-207, "Security Reviews," DSS performs vulnerability assessments of all cleared contractor facilities under its cognizance. The focus of vulnerability assessments is to ensure facilities are compliant with NISPOM requirements such that safeguards employed by contractors are adequate for the protection of classified information.

During an assessment a team comprising of one or more DSS Industrial Security Representatives, Information System Security Professionals, and Counterintelligence Special Agents will review the contractor's security program as it relates to each chapter of the NISPOM and interview personnel. Throughout the assessment DSS will identify Vulnerabilities and NISP Enhancements (detailed on the following pages).

At the end of each assessment, DSS will review the identified vulnerabilities and enhancements and, taking in to consideration the size and complexity of the facility's program, identify an assessment rating of Superior, Commendable, Satisfactory, Marginal, or Unsatisfactory.

Following each assessment DSS will provide the Facility Security Officer (FSO) a list of identified vulnerabilities, NISPOM reference, and recommended action to remedy. DSS will then continue to follow up and work with the FSO to help mitigate any outstanding issues.

In the rare case of a Marginal or Unsatisfactory rating, DSS will notify the facility's government customers for classified contracts who may discontinue or suspend contract performance. DSS will conduct a compliance assessment within 60 to 120 days to evaluate the facilities corrective actions to identified vulnerabilities. A satisfactory rating will be awarded and government customers notified at the conclusion of the compliance assessment if the vulnerabilities have been mitigated. These ratings are infrequent and it is the DSS goal to partner with industry, ensuring strong security programs are in place to protect classified information.

Vulnerabilities

Definition:

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:

- **Acute Vulnerability**: 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.
- **Critical Vulnerability**: 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 a 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. These defects in either a subset or the overall program may logically result in either a security violation or administrative inquiry if not properly mitigated.
    - Repeat - Is a repeat of a specific occurrence identified during the last DSS security assessment that has not been properly corrected (i.e. a specific document, system, personnel, etc. issue was identified and reported corrected by the contractor facility but upon the next assessment the exact same document, system, person, etc. the vulnerability still exists). 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.

For the purposes of Rating Matrix scoring, multiple instances of vulnerabilities identified under the same NISPOM reference will be counted as one item. For example, multiple documents not properly marked as required in "4-203. Overall Markings" would count as one cited vulnerability. As applicable, DSS will provide contractors a report of each occurrence of the vulnerability for appropriate mitigation action.

Clarification:

- Corrected on the spot (COS) – All vulnerabilities identified by DSS will be documented, counted, and points subtracted on the Rating Matrix form to include those 'corrected on the spot.' It is important in the DSS assessment 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.

NISP Enhancements

Definition:

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 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 DSS review of processes/procedures. Credit for NISP enhancements will be granted for activities beyond baseline NISPOM requirements even if required by program/contract.

In order for an enhancement to be granted the facility must meet the baseline NISPOM requirements in that area. An enhancement directly related to a NISPOM requirement cited for a vulnerability may not be granted. In essence, as the core of the DSS vulnerability assessment is to ensure compliance with NISPOM requirements and that foundation must be in place before additional activities would be recognized. If there are other effective enhancement activities in a specific category unrelated to a specific vulnerability in that category the enhancement credit may still be granted. For example, one non-acute, non-critical marking vulnerability may not eliminate opportunity for Category 9 enhancement credit where a facility implements an Information Management System reflecting history of location and disposition for material in the facility for Secret and Confidential material, i.e. 100% inventory and accountability, paralleling requirements for Top Secret.

Companies with multiple facilities which implement standardized 'corporate wide' security practices that may categorize as NISP enhancements may optionally email dss.quantico.dss-isfo.mbx.qao@mail.mil with any questions on those activities.

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.

The following pages outline each of the ten NISP enhancement categories, provides a definition and intent of the area, and examples of items considered best practices or otherwise not a NISP enhancement. These examples are not all inclusive of activities which may meet the definition and intent of an enhancement category, and DSS will continue to update the example list as appropriate.

Category 1: Company Sponsored Events

Enhancement Definition and Intent:

In addition to the annual required security refresher briefings, the cleared contractor 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. Intent of this category is to encourage cleared contractors to actively set time aside highlighting security awareness and education. This should not be a distribution of a paper or email briefing, but rather some type of interactive in person activity.

Some Examples of this Enhancement:

- 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, security webinar with company employees, etc.
- Training events conducted at off-site customer locations are acceptable for enhancement.
- Presentations at the facility provided by government employees (CISA, etc.) pertaining to its NISP involvement and security of classified information.
- There may be other situations where cleared contractors organize and have their employees attend additional security training events at customer or other contractor locations.

Items which are Best Practices or otherwise Not an Enhancement:

- CISA accompanies ISR during security vulnerability assessment and provides advice and assistance on suspicious contact reporting.

Category 2: Internal Educational Brochures/Products

Enhancement Definition and Intent:

A security education and awareness program that provides enhanced security education courses or products to employees beyond initial and annual refresher training requirements; i.e., CD/DVD, web based interactive tools, newsletters, security games/contests, international security alert system, etc. Intent of this category is to encourage cleared contractors to generate and distribute relevant security materials to employees who then incorporate the content into their activities.

Some Examples of this Enhancement:

- Content does not need to be generated by the cleared contractor. For example:
  - Home office provides branch locations with security related products whose personnel in turn incorporate the content into their activities.
  - Security staff distributes *relevant security education information* provided by government activities or security organizations and the workforce incorporates the content into their activities.
- Security staff develops security briefing products to be delivered to *uncleared* employees that specifically address the company's Facility Security Clearance and its effect on the employee; i.e., suspicious contact reports, adverse information reports, how to recognize classified material that is unprotected and the need to report such to the FSO, etc.
- Demonstration of a comprehensive and ongoing CI and/or cybersecurity Awareness program for all employees (cleared and uncleared), focused on specific threats to contractor facility's classified programs or technologies, insider threat activity, validated through a review of training material and employee interviews.

Items which are Best Practices or otherwise Not an Enhancement:

- Forwarding the monthly DSS Newsletter. The newsletter is primarily policy, knowledge required by the FSO, or training opportunities and in and of itself does not equate to an educational tool.
- Trained 100% of the cleared employees

Category 3: Security Staff Professionalization

Enhancement Definition & Intent:

Security staff training exceeds NISPOM and DSS requirements and incorporates that knowledge into NISP administration. Intent of this category is to encourage security program's key personnel to actively strive to learn more and further their professional security expertise beyond mandatory requirements.

Some Examples of this Enhancement:

- Obtaining and maintaining professional certifications such as Certified Protection Professional (CPP), SPeD Certification, Computer Information Systems Security Professional (CISSP), etc.
- Partial completion of a training program (beyond base training requirements per NISPOM 3-102 and 8-103) if accomplished security relevant courses applicable to one's duties. (i.e., final training certificate is not a requirement to receive credit).
- Additional CDSE courses, STEPP courses, NCMS "brown bag" training sessions.

Items which are Best Practices or otherwise Not an Enhancement:

- Currently possess a certification but has not taken any training or ongoing certification maintenance within the assessment cycle; i.e., received certification in 2008 and has not done anything since then.
- Taking additional security courses *but* has not completed required training to date (i.e. if an FSO has not yet completed required FSO training this category would not receive credit for additional training).

Category 4: Information & Product Sharing within Security Community

Enhancement Definition and Intent:

Facility Security Officer (FSO) provides peer training support within the security community and/or shares security products/services with other cleared contractors outside their corporate family. Intent of this category 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.

Some Examples of this Enhancement:

- Sharing classified destruction equipment to the local security community. Classified should be properly handled, i.e. per NISPOM requirements.
- Cleared contractor serves as a source for fingerprinting employees from other cleared contractors.
- Cleared contractor actively participates in DSS pilot programs and other services and products.
- Cleared contractor shares examples of effective self-review methods.
- Cleared contractor provides training and support for new facilities. For example: Electronic Facility Clearance (eFCL), JPAS, Electronic Questionnaire for Investigations Processing (eQIP), etc.
- Cleared contractor assists other cleared contractors with international activities such as writing of Technology Control Plans (TCP), Transportation Plans (TP), etc.
- Information Systems Security Manager (ISSM) or Facility Security Officer mentors ISSMs/FSOs at other cleared contractors.

Items which are Best Practices or otherwise Not an Enhancement:

- Sharing or providing products/services to companies or agencies that are not participating in the National Industrial Security Program.

Further Clarification:

- These activities should not be related to or in conjunction with security organizations such as Industrial Security Awareness Council (ISAC), National Classification Management Society (NCMS), American Society for Industrial Security (ASIS), etc. Items relating to these types of groups would fall under Category 5.

Category 5: Active Membership in Security Community

Enhancement Definition and Intent:

Security personnel are members and actively participate with NISP/security-related professional organizations. Intent of this category is to encourage security programs to actively collaborate with their local security community to identify best practices to implement within their own NISP security programs.

Some Examples of this Enhancement:

- Examples of these types of organizations include security/NISP-related activities.
- Cleared contractor hosts security events on behalf of security/NISP-related professional organizations.
- Cleared contractor security staff is a guest speaker at a security event provided by a security-related professional organization.
- Members of the facility's security staff are elected on security community boards (i.e. President or Committee/Board Member).

Items which are Best Practices or otherwise Not an Enhancement:

- Any security groups or events not directly related to the National Industrial Security Program (NISP). For example, a President of a cleared facility speaks at an event hosted by a university, but the audience is not familiar with or part of the NISP.

Further Clarification:

- Verification of enhancement should be aimed at asking what were the take-aways from events, how do they apply to the facility's security program and how is the security staff implementing any take-away information.
- Security personnel unable to attend meetings on a regular basis can collaborate virtually via the organization's websites, email etc.

Category 6: Contractor Self-Review

Enhancement Definition and Intent:

Contractors sustain multiple reviews of their security posture that are thorough and impactful. 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.

Some Examples of this Enhancement:

- Multiple documented self-reviews providing an on-going, continuous evaluation of the security program.
- Establishment of 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).

Items which are Best Practices or otherwise Not an Enhancement:

- Uses CDSE Self-Inspection Handbook for Contractors.
- Only develops corrective action plan for vulnerabilities and does not follow-up to mitigate those vulnerabilities.
- Conducting parts of a self-review over an extended period of time, however only completing the one required formal self-review, preparing a formal report describing the self-inspection (issues and resolution), and SMO certifying to DSS in writing that a self-inspection has been conducted.

Further Clarification:

- If there are numerous vulnerabilities identified in their self- review which can be mitigated in a reasonable timeframe that are not corrected prior to the DSS assessment, then credit should not be given
- Taking in to account the size and complexity of the facility, if vulnerabilities were identified during the self-review and documented as mitigated in the formal report prepared for DSS review, then during the DSS assessment vulnerabilities were found in these areas, the mitigating process put in place was not effective and this enhancement should not be granted.

Category 7a: Threat Identification and Management

Enhancement Definition and Intent:

The foreign intelligence threat to cleared contractors is constant and pervasive. The intent of this enhancement is to encourage cleared contractors to build a counterintelligence (CI) focused culture, implementing strategies and processes within their security program to detect, deter, and expeditiously report suspicious contacts (SCR) to DSS.

By way of this enhancement, DSS encourages cleared contractors to develop programs, policies, and processes that identify and proactively thwart foreign attempts across known threat vectors (purchase solicitation, foreign visit and foreign travel, suspicious network activity, academic solicitation, etc.) to acquire classified and sensitive technologies.

Effective threat management and mitigation includes timely identification and reporting of suspicious activities, an understanding of the threat environment, agile and authoritative decision making to neutralize or mitigate vulnerabilities and threats, and proactive action to prevent any reoccurrence of a reported suspicious activity, as demonstrated through immediate response to a suspicious or illegal acts.

Some Examples of this Enhancement:

- Systematic and effective foreign travel /contact pre-briefings and de-briefings conducted in-person or telephonically designed to identify contacts or activities displaying potential espionage indicators.
- Systematic notification process advising DSS of incoming and outgoing foreign visitors prior to occurrence and implementation of briefing and debriefing program for persons hosting foreign visitors.
- Effective identification, collection, and coordination of threat information (pertaining to CI, cybersecurity, force protection, etc.) tailored to the facility's classified programs or technologies, and application of related defensive measures.

Items which are Best Practices or otherwise Not an Enhancement:

- Contractor developed a foreign travel briefing, but no OCONUS travel occurred during the rated assessment cycle.
- Contractor educates employees on incoming foreign visitor procedures but did not host incoming foreign visitors during the rated assessment cycle.
- Contractor provides sterile travel laptops with full disk encryption for employees travelling OCONUS.
- Contractor provides pre/post domestic conference briefings.
- Contractor utilizes a centralized mailbox to collect potential SCR notifications.
- Effective awareness program that ensures all employees (cleared and uncleared) are cognizant of individual reporting responsibilities.
- Use of general classified threat products to assess threats, implement focused security countermeasures (i.e. dissemination and incorporation of the DSS Technology Trends document).
- Demonstration of an effective and timely reporting process for suspicious contact reporting to DSS.

Category 7b: Threat Mitigation

Enhancement Definition and Intent:

As a result of the successful execution of Category 7a, *Threat Identification and Management*, cleared contractors (CC) who have validated vigorous and effective CI programs are more likely to identify foreign intelligence targeting of their technology. By way of this enhancement, DSS encourages CCs to directly engage with thwarting illegal attempts to acquire classified and sensitive technologies and support law enforcement and intelligence efforts to neutralize the threat. For this enhancement credit, the CC must have provided suspicious contact reporting to DSS resulting in the:

- Initiation of investigations or activities by Other Government Agencies within the evaluation period.
- Cleared facility must be awarded Category 7a enhancement, *Threat Identification and Management*, during the same assessment to qualify for this enhancement.

Some Examples of this Enhancement:

- An effective CI program that includes a federal law enforcement case opening linked to SCR reporting validated by DSS CI (Note: The date the OGA advises DSS of the investigation will be used as the validation date and falls within the assessment cycle).
- An effective CI program that includes an intelligence community investigation linked to SCR reporting validated by DSS CI. (Note: The date the IC OGA advises DSS of the investigation will be used as the validation date and falls within the assessment cycle).
- An effective CI program that includes essential and critical cooperation provided to federal law enforcement or intelligence community agencies pursuing the neutralization of illegal penetrators validated by the investigative agency.
- An effective CI program that includes an intelligence or federal law enforcement case opening linked to contractor facility's identification of suspicious network activity, anomalies or intrusions of CC systems to DSS.

Category 8: FOCI / International

Enhancement Definition and Intent:

Cleared contractor implements additional effective procedures to mitigate risk to export controlled items and/or FOCI. Intent of this category is to encourage cleared contractors to implement an enhanced export control program increasing the effectiveness. For FOCI mitigated facilities, intent is to encourage activities above mitigation instrument requirements to further minimize foreign influence at the facility.

Some Examples of this Enhancement:

Note - Items which are requirements of the mitigation instrument may not be counted as enhancements.

- Cleared contractor performs 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 voluntarily conducts, or has outside experts conduct, ongoing export compliance audit and shares the results with interested U.S. Government Agencies.
- Facility maintains an enhanced ongoing export control self-inspection program.
- Effective briefing and debriefing program for persons hosting foreign visitors.
- Enhanced TCP processes would include cleared contractors developing a Foreign Visitor management system to include foreign national visitors being approved by export control and security before arrival. Security briefs for all FN visitors on the TCP and guards are required to have a foreign visitor request approval number before the FN can enter the facility (being escorted by an appropriately briefed individual).
- 100% or a risk-prioritized review of electronic communications with documented action-driving analysis with a documented follow-on audit/interview program, including enterprise-wide analysis for anomalies.
- Outside Directors, Proxy Holders, or Trustees interacts directly with the cleared contractor site employees (training program, vulnerability assessment, compliance visits, etc.) with effective impacts.
- Requiring that all electronic communications to the parent or affiliates obtain advance approval.
- Implements and maintains system for automatic designation of emails to/from foreign parent/affiliates.
- Appointment of additional Outside Directors, Proxy Holders, or Trustees. The facility must demonstrate the benefit in additional FOCI oversight these persons add (i.e. OD is assigned specifically to monitor and report on X).

Items which are Best Practices or otherwise Not an Enhancement:

- Facility maintains a list of export controlled items the facility works and it is shared with relevant employees to ensure awareness across the workforce.
- FOCI mitigation instruments are effectively deployed prior to the formal requirements being communicated.
- Corporate Secretary periodically reviews 328 for accuracy.

Category 9: Classified Material Controls/Physical Security

Enhancement Definition and Intent:

Facility has deployed an enhanced process for managing classified information and/or has implemented additional Physical Security measures, with built-in features to identify anomalies. Intent of this category is to encourage security programs to maximize the protection and accountability of classified material on-site by implementing effective processes, regardless of quantity of classified holdings.

Some Examples of this Enhancement:

- Information Management System (electronic or physical) reflects history of location and disposition for material in the facility for Secret and Confidential material (100% inventory and accountability, paralleling requirements for Top Secret).
- Working papers are fully marked and automatically brought into IMS regardless of date of creation.
- Safe custodian performs 100% check-in/check-out of materials, reviews material for appropriate markings and classification.
- Monitored and recorded CCTV, card access readers, biometric equipment strategically positioned around controlled areas with on-going analysis of data.
- In addition to supplemental control requirements, facility has written procedures outlining guard personnel responsibilities to include verifying safes, closed areas, etc. are properly secured and/or verifying working areas are free of classified information and maintain documentation of performance.

Items which are Best Practices or otherwise Not an Enhancement:

- Added video monitors of high theft areas.
- Establishment of documented tracking system for inspections of areas above and below false ceilings/floors in Closed Areas.
- Combination changes more frequently than required.
- FSO has pre-coordinated with DSS in building out new facilities re Closed Areas, Classified Network Controls.
- FSO has proactively obtained Security Classification Guidance (SCG) for classified programs.
- FSO coordinates proactively with the GCA regarding SCG's for derivative classification.
- 100% inventory conducted during self-inspection does not count towards enhancement.

Further Clarification:

- Enhanced supplemental controls that do not have an impact on protection of classified information are not counted as enhancement.

Category 10: Information Systems

Enhancement Definition and Intent:

Incorporating process enhancements and leveraging tools to expand the overall security posture of accredited information systems. Intent of this category is to encourage security programs to maximize protection of classified information on IS.

Some Examples of this Enhancement:

- Development and use of a formalized SOP and a comprehensive checklist to augment a detailed weekly audit review process which describes what is performed during the review of large, complex IS (LANs/WANs) with multiple Operating Systems.
- Additional IS oversight processes put in place to enhance security of classified information residing on IS.
- Develop, implement, and utilize significant and effective (LAN/WAN based) Information System audit trail reduction/collection or analysis tools/scripts. These tools help focus on real security relevant events while minimizing the amount of non-security relevant data extracted within the audits.
- Use of a file or scripts that tracks downloaded files and/or compares generation records for unauthorized classified downloads and review/auditing of report outputs.
- Use of a file or scripts that tracks and/or block unauthorized USB connections and review/auditing of report outputs.
- Utilize scripts to maintain compliance to the SSP and ODAA's baseline. The scripts validate Security Relevant Object (SRO) settings and report back if discrepancies are found. ISSM reviews and acts on report findings.

Items which are Best Practices or otherwise Not an Enhancement:

- ISSM or ISSO is certified – note, this would fall under Category 3.
- Employing a color coded labeling system for *components* for both classified and unclassified networks (switches, routers, network jacks) when co-located in the same secure area to further identify and deter unauthorized or inadvertent system connections.
- Cleared contractors provide additional user training, briefings, etc. to people who are going to hold the privileged user position (the NISPOM only requires User training and annual refresher training). So not only do they get the same annual training as the general user they have to agree in writing to the additional responsibilities of being a privileged user and they then have to undergo further training and refresher every year.
- Developed reports to give ample notification on when a system is due for re-accreditation. This is done to provide enough time for the submission to work through the ODAA process.
- Developed reports to give ISSM notification of systems that are in the ODAA process. These notifications are day triggered based on the submission of paperwork to ODAA. After 30 days a notice is made to the ISSM to follow-up, and every 15 days after that follow-up till either an IATO or ATO is received.
- Utilize a daily report that shows when audits should be performed on accredited systems. This report helps show future audits and if they land on non-work days so the ISSM can adjust the audit schedule as needed. It also provides notice to other security staff in case the audit individual is out so others can cover.
- Developed a method to patch and maintain air gapped systems. This method utilizes different approaches from an offline WSUS, using Microsoft's patch catalog and ISO DVD, and internal application repositories.
- Utilize scripts to maintain time on air gapped systems. Since air gapped systems are not always able to connect to a time server, systems do experience time drift. By checking the time and time zone during audits we are able to minimize time drift to keep audit records compliant.
- Utilize scripts to apply and maintain antivirus definition updates. This standardizes the process to make sure they are applied properly.
- Utilize a method to track SID numbers. This method helps correlate uses back to an audit event if the user has been removed from the system.

Rating Matrix 2016 - Calculation Worksheet

Rating Calculation *(Complete areas in grey)*

**Note: For rating calculation purposes, treat multiple occurrences under the same NISPOM reference as one finding*

	CAT AA, A, B		CAT C, D		CAT E	
	Starting Score →	700	Starting Score →	700	Starting Score →	700
Non-Acute/Critical Vulnerabilities by Reference*	(x 2)	-	(x 3)	-	(x 4)	-
Acute or Critical Vulnerabilities Reference*	(x 14)	-	(x 17)	-	(x 20)	-
Total (Subtractions)	=		=		=	
NISP Enhancements by Category						
1 Company Sponsored Events	(15)	+	(15)	+	(17)	+
2 Internal Educational Brochures/Products	(15)	+	(15)	+	(17)	+
3 Security Staff Professionalization	(15)	+	(15)	+	(17)	+
4 Information/Product Sharing w/in Community	(15)	+	(15)	+	(17)	+
5 Active Membership in Security Community	(15)	+	(15)	+	(17)	+
6 Contractor Self-Review	(15)	+	(15)	+	(17)	+
7a Threat Identification and Management	(15)	+	(15)	+	(17)	+
7b Threat Mitigation	(15)	+	(15)	+	(17)	+
8 FOCI/International	(15)	+	(15)	+	(17)	+
9 Classified Material Controls/Physical Security	(15)	+	(15)	+	n/a	n/a
10 Information Systems	(15)	+	(15)	+	n/a	n/a
Total (Additions)	=		=		=	
FINAL SCORE	=		=		=	

Red Flag Items ***(Contact FOC if any of the below conditions exist)***
Unmitigated or unreported FOCI.
Intentional disregard of NISPOM regulations.
Failure to report a KMP change that involves the addition or removal of one or more essential KMP.
Essential KMP not cleared to the level of the facility's FCL
Uncleared persons in essential KMP positions.
Lack of senior management support to comply with PCL investigation requirements (Essential KMP PRs)
Evidence of self-adjudication of, or failure to report known adverse information
Evidence that the FSO is unable or unwilling to effectively supervise and direct security measures.
Inability to accurately annotate and maintain employee's access records in JPAS (systemic inaccuracy of records).
Acute or Critical vulnerabilities that could lead to the loss of, compromise, or suspected compromise of classified information.
Substantial vulnerabilities indicative of a substandard security program.
Any additional items which may result in invalidation of the FCL.
Processing on an unaccredited IS.
Failure to promptly report any information concerning actual, probable or possible espionage, sabotage, terrorism or subversive activities
Failure to promptly report the unauthorized disclosure, theft, loss, or compromise of classified information or defense related information prohibited from foreign disclosure to an unauthorized entity (uncleared person, foreign entity, or agent of a foreign power).

Providing false or misleading information regarding the potential compromise of classified or defense related information
Systemic non-compliance with FOCI Mitigation Instrument (i.e. ECP, TCP).
Matrix score leading to marginal or unsatisfactory rating.

CAGE Code	
Company	
Assm. Date	
Team Assm	**Yes / No**

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

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
x2	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
x3	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45
x4	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
x14	14	28	42	56	70	84	98	112	126	140	154	168	182	196	210
x15	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225
x17	17	34	51	68	85	102	119	136	153	170	187	204	221	238	255
x20	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300