DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Security Rating "Gold Standard" Criteria Reference Card

UID	Criteria	Supporting Information
NE-1	Facility promptly informed DCSA of any security violations and also mitigated any known vulnerabilities and administrative findings in a timely manner.	**REQUIREMENT:** The contractor must meet <u>all elements</u> below to achieve this criterion (5-point value). **1. Security Incidents/Violations.** □ Security staff explained the facility's security incident procedures and the requirement to report security violations to DCSA within timeframes listed below. □ Maintained documented procedures related to security incidents, including timeframes listed below. See Considerations. Additionally, if the contractor had any security incidents during the security review cycle, the facility: □ Immediately isolated and safeguarded affected material. □ Conducted a preliminary inquiry within 3 calendar days. □ If the inquiry resulted in an infraction: - Documented the incident. - Maintained a copy for review by DCSA upon request through the security review cycle. □ If the inquiry could not immediately rule out loss or compromise resulting in a violation: - Submitted an initial report to DCSA within 1 calendar day for violations involving Top Secret information and within 3 calendar days for violations involving Secret or Confidential information. - Conducted an internal investigation to make a final determination of loss, compromise, or suspected compromise. - Submitted a final security violation report within 30 calendar days unless an extension was requested and granted in writing by the ISR prior to the 30-day suspense. □ When needed as a result of lessons learned or after-action report, updated documented procedures or provided additional training to individuals or all cleared employees to minimize the possibility of security incident recurrence. See Considerations. **2. NISPOM Non-Compliance Mitigation.** □ Security staff explained the requirement to mitigate identified NISPOM non-compliances within the established timelines (15-calendar days for vulnerabilities, 30-calendar days for administrative findings).

UID	Criteria	Supporting Information
		□ Maintained documented procedures related to mitigating NISPOM non-compliances within the established timelines identified above. Additionally, if the contractor or DCSA identified any vulnerabilities or administrative findings during the security review cycle, the facility: □ Mitigated vulnerabilities within 15-calendar days. See Exception. □ Mitigated administrative findings within 30-calendar days. See Exception. □ (Exception) Created and maintained a documented plan to track and monitor mitigation of identified non-compliances. Communicated the plan and associated milestones to DCSA. See Considerations. **CONSIDERATIONS:** □ Documented plans or procedures can written be within a standalone document or maintained within the facility’s standard practice and procedure (SPP).
NE-2	Appointed security personnel performed their duties and responsibilities to the fullest extent outlined in the NISPOM.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). **1. Continuity of Operations.** □ Contractor ensured a Senior Management Official (SMO), Facility Security Officer (FSO), Insider Threat Program Senior Official (ITPSO), and Information Systems Security Manager (ISSM), when applicable, were appointed throughout the security review cycle. See Exception. □ (Exception) If needed, established and implemented a written contingency plan to ensure there was no gap in appointed personnel to a level that impacted successful implementation of the security program. **2. Performance of Duties.** □ SMO performed required duties and responsibilities. *See Appointed Personnel Duties Job Aid.* □ FSO performed required duties and responsibilities. *See Appointed Personnel Duties Job Aid.* □ ITPSO performed required duties and responsibilities. *See Appointed Personnel Duties Job Aid.* □ ISSM, appointed when the contractor was processing information on a classified information system located at the contractor facility, performed required duties and responsibilities. *See Appointed Personnel Duties Job Aid.*

UID	Criteria	Supporting Information
NE-3	Facility maintained documented security procedures outlining all applicable requirements of the NISPOM for their operations and involvement with classified information and implemented those procedures to protect classified information.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). **1. Documented Security Procedures.** □ Established documented security procedures to the level of the contractor's operations and involvement with classified information. See Considerations. - Required for all facilities: SEAD 3 and Insider Threat Procedures (e.g., SPP) - Additionally required for all safeguarding facilities: Classified Operations Procedures (e.g., SPP) - Additionally required for some facilities (based on operations): System Security Plan, Technology Control Plan, Electronic Control Plan, FOCI Mitigation Instruments, and others. □ Updated documented procedures within 30 calendar days when the following qualifying changes impacted successful implementation of the security program: self-inspection process, policy updates, changes impacting risk to classified information, and other times. **2. Implemented Documented Procedures.** □ Security staff provided relevant personnel with a copy of the documented procedures to heighten their security awareness. □ Contractor personnel followed the processes outlined within the documented procedures. **CONSIDERATIONS:** □ Independently evaluate each facility under this criterion even if there is an enterprise-wide procedure. To achieve this criterion, this may require site specific addendums or independent documentation at branch/division locations to ensure procedures are sufficient to heighten the security awareness of contractor personnel. The facility cannot achieve this criterion if they deviate from the enterprise wide SPP without approved and fully implemented site-specific procedures.
NE-4	Facility completed compliant and effective self-inspections that addressed issues or concerns in a timely manner.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). **1. Compliant Self-Inspections**. □ Conducted a self-inspection at least annually (once a calendar year) and at least every 12 months for classified information system elements, if applicable. □ Included minimum NISPOM requirements as part of the self-inspection:

UID	Criteria	Supporting Information
		- Reviewed classified activity, classified information, classified information systems, conditions of the overall security program, and insider threat program. - Included sampling of contractor's derivative classification actions, as applicable. - Prepared a formal report describing the self-inspection, its findings, and its resolution of issues discovered during the self-inspection. Retained the report until after the DCSA security review. - Annually certified to DCSA, in writing, that a self-inspection was conducted, other KMP were briefed on the results of the self-inspection, appropriate corrective actions were taken, and management fully supports the security program. **2. Effective Self-Inspections.** □ Reviewed NISPOM elements at a level commensurate with facility operations to identify NISPOM non-compliance. □ Reviewed internal processes to identify gaps in security controls and determine effectiveness of implemented procedures. □ Reviewed approach vectors to determine if countermeasures were in place to mitigate potential threat. □ Reviewed FCL information in NISS and submitted a facility profile update request, if needed. See Considerations. □ Evaluated knowledge and awareness of security procedures through personnel interviews, surveys, or other means. □ Mitigated vulnerabilities identified during the self-inspection within 15 calendar days from identification and administrative findings within 30 calendar days from identification. If unable to mitigate identified issues within required timeframe, implemented a plan to track and monitor mitigation and communicated the plan and associated milestones to DCSA. □ Updated documented security procedures within 30 calendar days as a result of the self-inspection process, policy changes, changes impacting the risk to classified information, and other times impacting successful implementation of the security program. □ Addressed relevant issues or concerns identified during the self-inspection as part of the annual refresher training. See Considerations. **CONSIDERATIONS:** □ NISS is the official system of record for facility clearances and has been approved by OMB for the collection of data. Reviewing and updating profile information is critical to assisting DCSA with prioritizing visits and preparing for security reviews.

UID	Criteria	Supporting Information
		□ Security staff can address relevant issues or concerns through a separate method or at a different time than other elements of the annual refresher training as long as all required elements are provided within the 12-month timeframe. Methods may include group briefings, interactive videos or webinars, dissemination of material, or other media and methods.
NE-5	Facility implemented a continuous monitoring program that facilitated ongoing awareness of threats, vulnerabilities, and changes in classified operations to support organizational risk management decisions.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). □ Monitored all elements of the industrial security program outside the formal self-inspection process. See Considerations. □ (For Classified IS) Adhered to the classified information systems continuous monitoring activity requirements that were part of the IS authorization. □ Explained how the facility's industrial security program facilitates ongoing awareness of threats, vulnerabilities, and changes in classified operations. Specifically: - Stayed aware of potential threats that may impact the facility. See Examples. - Conducted random spot checks of security practices outside the self-inspection process to identify NISPOM non-compliances and potential risk to classified information and classified information systems. See Examples. - Obtained classified operation updates to include impacts to their facility clearance, new or expired classified contracts, and newly supported critical technology. **CONSIDERATIONS:** □ Evidence of threats, vulnerabilities, and changes in classified operations that were not identified during the facility's continuous monitoring process or any classified information systems monitoring activities part of the IS authorization that were not completed as required disqualifies the facility from receiving this criterion. **EXAMPLES:** □ Stay Aware of Potential Threats examples include, but are not limited to: - Review updated MCMO Matrices or Targeting U.S. Technologies published by DCSA - Review unclassified or classified threat products provided by government entities or other relevant resources - Review cybersecurity or counterintelligence news articles from trusted sources.

UID	Criteria	Supporting Information
		□ Random Spot Check examples include, but are not limited to: - Review the personnel security system of record to ensure employee eligibility for access to classified information remains valid - Review documents within an open storage area to ensure adequate markings and need-to-know separation - Review DD Form 254s (or security aspect letters) to ensure classification guidance is sufficient and classification guides are available to cleared personnel.
MS-1	Management included the security staff in business decisions that impact the security program and promptly notified the security staff of changed conditions impacting the facility clearance.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). □ Management included security staff in business decisions that impact the security program. See Examples. □ Management notified security staff prior to changes occurring that could impact the FCL to ensure prompt notification to DCSA or OGAs, as required. In rare cases where notification to the security staff was not possible prior to the qualifying event, management notified the security staff within 5 calendar days. See Considerations. **CONSIDERATIONS:** □ Evidence of unreported changed conditions to the security staff during the security review cycle disqualifies the contractor from achieving this criterion. The threshold is notification to the security staff which may include the Chief Security Officer, Director of Security, FSO, or others. The intent is to ensure the security staff has a voice to raise potential issues or concerns regarding forthcoming changes that impact the FCL. □ Interviewing the SMO directly is not required to award this criterion. **EXAMPLES:** □ Included Security Staff in Business Decisions examples include, but are not limited to: - Management invited security staff to senior level meetings. - Management included security staff in written or verbal discussions. - Management provided an overview of proposed business decisions to security staff for review and feedback.

UID	Criteria	Supporting Information
MS-2	Management provided the security staff with sufficient personnel and resources to oversee the security program and ensure prompt support and successful execution of a compliant security program.	**REQUIREMENT:** The contractor must meet <u>all elements</u> below to achieve this criterion (5-point value). □ Management ensured authorized and cleared employees were available at all times to manage and implement the requirements of the NISPOM. Specifically: - Maintained an appointed FSO, ITPSO, and ISSM (when applicable) throughout the security review cycle. - Maintained a sufficient number of personnel to provide prompt support and successful execution of the security program. See Considerations. □ Management ensured the security staff had the material and financial resources available to enable them to provide prompt support and successful execution of the security program. See Considerations. **CONSIDERATIONS:** □ Evidence that prompt support and successful execution of the security program was negatively impacted due to the facility not having a sufficient number of personnel on staff disqualifies the facility from achieving this criterion. □ When determining prompt support and successful execution, considerations may include but are not limited to: - Processing security clearance applications or continuous vetting requests - Processing SEAD 3 or adverse information reports - Responding to security incidents and processing security violation - Adhering to classified IS authorization and continuous monitoring requirements including separation of duties when warranted - Providing security training and briefings as required - Conducting self-inspections - Mitigating NISPOM non-compliance. □ Interviewing the SMO directly is not required to award this criterion.
MS-3	Management was aware of the facility's classified operations and remained informed of any identified issues or concerns	**REQUIREMENT:** The contractor must meet <u>all elements</u> below to achieve this criterion (5-point value). **1. Classified Operations Awareness.** □ ~80% (or more) of interviewed management were aware of the following: See Considerations - Facility was cleared under the NISP to perform on classified contracts - Facility clearance (FCL) level

UID	Criteria	Supporting Information
	and supported implementation of measures to mitigate known issues.	- Facility’s involvement with classified operations to include safeguarding, classified IS, FOCI involvement, foreign classified operations, and others, based on their assigned duties and responsibilities. 2. **Informed of Issues or Concerns.** □ Security staff briefed management on any necessary or lacking resources for effective implementation of the security program. □ SMO certified self-inspection results throughout the security review cycle. □ KMP were briefed on the results of the self-inspection throughout the security review cycle. □ Security staff notified management of relevant security vulnerabilities, systemic security problems, and issues impacting the FCL throughout the security review cycle. □ When appropriate, management provided personnel, material, or financial support to understand issues or concerns, and to implement necessary mitigation. □ (For Classified IS) Security staff briefed management on the Configuration Change Board (CCB) to manage and oversee changes to the project, scope, and budget. **CONSIDERATIONS:** □ When interviewing management, the interviewer should take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion. □ Interviewing the SMO directly is not required to award this criterion.

UID	Criteria	Supporting Information
MS-4	Management was aware of approach vectors applicable to the facility and supported implementation of measures to counter potential threats.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). □ ~80% (or more) of interviewed management: See Considerations - Knew the most common approach vectors applicable to cleared Industry. See Considerations - Knew the approach vectors applicable to their facility. - Explained how they supported measures to counter potential threats. □ When appropriate, management provided personnel, material, or financial support to understand threats and implement necessary countermeasures. **CONSIDERATIONS:** □ When interviewing management, the interviewer should take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion. □ Contractor security staff can use the MCMO Matrix, “Targeting U.S. Technologies: A Report of Threats to Cleared Industry” (formerly known as “Trends”), CDSE training, and other resources to gain awareness of approach vectors. □ Interviewing the SMO directly is not required to award this criterion.
MS-5	Management made decisions using threat information while considering potential impacts caused by a loss of classified information, contract deliverables, and technology.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (5-point value). □ ~80% (or more) of interviewed management: See Considerations - Explained how they obtained current and relevant threat information. See Considerations - Explained how they used threat information to make business, operational, and mission decisions considering potential impacts caused by a loss of classified information, contract deliverables, and technology. **CONSIDERATIONS:** □ When interviewing management, the interviewer should take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion. □ Contractor security staff can use the MCMO Matrix, “Targeting U.S. Technologies: A Report of Threats to Cleared Industry” (formerly known as “Trends”), “Foreign Intelligence Entities’ Recruitment Plans

UID	Criteria	Supporting Information
		Target Cleared Academia", government provided briefings, and other credible sources to obtain current and relevant threat information. □ Interviewing the SMO directly is not required to award this criterion.
SA-1	Contractor implemented a culture of security within the organization.	**REQUIREMENT:** The contractor must meet <u>all elements</u> below to achieve this criterion (1-point value). □ ~80% (or more) of interviewed contractor personnel confirmed the facility successfully implemented a culture of security within the organization through a set of shared attitudes, values, goals, and practices that characterizes the organization commitment and implementation of security. See Considerations **CONSIDERATIONS:** □ When determining if the organization implemented a culture of security, considerations may include but are not limited to: - Security is everyone's responsibility. - Security is practiced from the top down. - Strategies are in place to mitigate historical weaknesses. - Facility has a comprehensive security awareness training program. - Successful security practices are encouraged and recognized. - On-site government personnel, subcontractors, and long-term visitors are briefed on local security practices and included in the overall security culture. □ When interviewing contractor personnel, the interviewer should take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion.
SA-2	Contractor personnel understood the security processes and documented security procedures relevant to their position.	**REQUIREMENT:** The contractor must meet <u>all elements</u> below to achieve this criterion (1-point value). □ ~80% (or more) of interviewed contractor personnel correctly explained: See Considerations - Which processes and documented security procedures were relevant to their position. - Where to find documented security procedures for guidance. - How to perform processes and security procedures relevant to their position. **CONSIDERATIONS:**

UID	Criteria	Supporting Information
		□ Evidence the facility does not have documented security procedures disqualifies the facility from achieving this criterion. □ When interviewing contractor personnel, the interviewer should take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion.
SA-3	Contractor personnel understood what required protection related to classified contracts, security classification guidance, and approach vectors applicable to their position.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (1-point value). □ ~80% (or more) of interviewed contractor personnel: See Considerations □ Explained what information, material, or technology required protection based on their position as outlined in classified contracts and security classified guides. □ Demonstrated how to protect the information and material within their possession. □ Explained which approach vectors were applicable to their position and the measures they individually take to mitigate a potential threat. **CONSIDERATIONS:** □ Evidence the facility does not have documented security procedures outlining how to protect classified material disqualifies the facility from achieving this criterion. □ When interviewing contractor personnel, the interviewer should take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion.
SA-4	Contractor personnel protected classified information in accordance with documented security procedures, NISPOM standards, and contractual requirements.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (1-point value). □ ~80% (or more) of interviewed contractor personnel: See Considerations. - Had access to the facility's documented security procedures. - Had access to the facility's security classification guides related to their position. - Explained their obligation to protect classified information from loss or compromise. □ Cleared personnel protected classified information from loss or compromise throughout the security review cycle both at the contractor facility or to which they had access. See Considerations **CONSIDERATIONS:**

UID	Criteria	Supporting Information
		□ Evidence the facility does not have documented security procedures or any loss, compromise, or suspected compromise of classified information during the security review cycle where the culpability was assigned to someone at the facility disqualifies the facility from achieving this criterion. □ When interviewing contractor personnel, take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion.
SA-5	Contractor personnel understood reporting requirements and reported relevant events.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (1-point value). □ ~80% (or more) of interviewed contractor personnel explained the requirement to report the following relevant security related issues to security staff when related to their position: See Considerations. - Failure to follow established security procedures. - Possible loss, compromise, or suspected compromise of classified information. - Cyber incidents on classified covered information systems. - SEAD 3 and adverse information elements. - Suspicious Contacts. □ Cleared personnel reported all security related issues outlined above to the security staff. See Considerations. □ Security Staff explained the facility's procedures for submitting reports outlined in the NISPOM and contractual requirements to DCSA. □ Security staff reported security violations, SEAD 3/adverse information reports, foreign travel, cyber incidents, and suspicious contacts to DCSA as required. See Considerations **CONSIDERATIONS:** □ Evidence the facility does not have documented security procedures outlining reporting requirements disqualifies the facility from achieving this criterion. □ Evidence of contractor personnel not reporting relevant security related issues to security staff automatically disqualifies the facility from achieving this criterion. □ Evidence of security staff not reporting relevant events to DCSA automatically disqualifies the facility from achieving this criterion. □ When interviewing contractor personnel, take into account the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work location, and security relevant job duties when determining if they sufficiently met the criterion.

UID	Criteria	Supporting Information
SC-1	Contractor cooperated with government entities during official visits and security investigations.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (1-point value). □ Cooperate with government entities throughout the security review cycle by taking all the below actions when requested: See Considerations. - Provide suitable arrangements within the facility for conducting private interviews with employees during normal working hours. - Provide relevant employee or personnel files, security records, supervisory files, records pertaining to insider threat, and any other records pertaining to an individual under investigation whether located in the office or at another location. - Submit a NISS Facility Profile Update request to ensure FCL documentation and contact information is current. - Provide information and complete follow-up actions when requested by DCSA as a result of an engagement, inquiry, or other request. - Render necessary assistance to support government-led investigations. **CONSIDERATIONS:** □ Evidence of not cooperating with government entities as outlined above throughout the security review cycle disqualifies the contractor from achieving this criterion.
SC-2	Contractor reported events to DCSA and OGAs in accordance with NISPOM and contractual requirements and supported the interest of national security by sharing relevant threat information with the security community.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (1-point value). □ Reported relevant events to DCSA, and other government agencies outlined in NISPOM 117.8 and contractual requirements. See Considerations □ Shared relevant threat information with the security community. See Examples. See Considerations. **CONSIDERATIONS:** □ Evidence of not reporting relevant events disqualifies the facility from achieving this criterion. □ Contractor security staff can share potential threat information from the corporate level within a Multiple Facility Organization. As long as there is no evidence that a branch/division failed to report relevant events, then sharing threat information at the corporate level does not preclude award of this criterion. **EXAMPLES:**

UID	Criteria	Supporting Information
		□ Sharing Threat Information: Examples include, but are not limited to: - Shared relevant information through DIBNet or DIBNet-S - Shared threat information within the security community that might otherwise be unavailable - Participated in the DCSA Joint Cyber Intelligence Tool Suite (JCITS) - Provided DCSA with cyber network logs
SC-3	Contractor coordinated with relevant stakeholders to obtain accurate and sufficient security classification guidance.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (1-point value). □ Security staff reviewed all aspects of the security classification guidance, including embedded security contract clauses, to ensure all requirements were identified and implemented. □ Security staff submitted a request for remedy to the GCA (or prime contractor) when information was classified improperly or unnecessarily, **or** security classification guidance (including the DD Form 254) was not provided, was improper, or was inadequate. Security staff submitted a formal written challenge to the GCA (or prime contractor) if a remedy was not provided to an initial challenge and, as needed, requested assistance from DCSA. □ (Prime Contractors) Responded to subcontractor security classification guidance challenges and coordinated with the GCA for a remedy. □ (For Classified IS) Coordinated with the customer for a Risk Acknowledgement Letter, when appropriate. **CONSIDERATIONS:** □ Evidence of security staff not being aware of security contract requirements or failure to coordinate with the GCA (or prime contractor) to obtain contract clarification when appropriate will disqualify the contractor from achieving this criterion.
SC-4	Contractor provided support to the security community that positively impacted the national industrial security program.	**REQUIREMENT:** The contractor must meet all elements below to achieve this criterion (1-point value). □ Provided support to the security community in a way that positively impacted the NISP. See Examples. **CONSIDERATIONS:** □ Do not award this criterion if the support provided by the facility did not have a positive impact to the NISP security community. **EXAMPLES:** □ Support to the Security Community with Positive Impact: Examples include, but are not limited to:

UID	Criteria	Supporting Information
		- Provided information to the security community through weekly emails that was used by junior and senior security personnel to further their knowledge on XX topic. - Provided conference briefing on managing personnel security clearance which was attended by 40 FSO's who used the knowledge within their security programs. - Mentored junior security personnel on NISP related topics, directly helping two security personnel develop their security programs and grow as security professionals. - Mentored another cleared entity with limited resources which saved the cleared entity (and ultimately the federal government) money and other resources without impacting program quality. - Served as an officer in a professional security organization which impacted the security professionalization of hundreds of FSOs within the XX chapter.
SC-5	Contractor participated in security community events, conferences, or webinars that positively impacted their security program.	**REQUIREMENT:** The contractor must meet <u>all elements</u> below to achieve this criterion (1-point value). □ FSO, ITPSO, and ISSM (if applicable), participated in a minimum of two security community events/training per calendar year each. See Examples. □ Security community events/training positively impacted the facility's security program. **CONSIDERATIONS:** □ Do not award this criterion if the security community event/training did not have a positive impact on the facility's security program. **EXAMPLES:** □ Examples of community events/training examples includes but are not limited to in person or virtual meetings, conferences, webinars, webcasts, and training courses. □ Examples of positive impact includes, but is not limited to: - Mentor/train others based on information - Establish or update processes/procedures - Implement countermeasures based on newly discovered risks - Develop or update training - Send new or updated communicates or notifications to contractor personnel.

TERMS AND DEFINITIONS:

□ Administrative Finding: Identified weakness in a contractor’s security program indicating non-compliance with the NISPOM that, based on collected evidence and implemented supplementary controls, could not be exploited to gain unauthorized access to classified information.

□ Approach Vector: Methods of contact used by an adversary to execute an operation and are identified within the DCSA MCMO Matrix and Targeting U.S. Technologies report. Recommended countermeasures for each contact method are located at https://securityawareness.usalearning.gov/cdse/matrix/index.html.

□ Government Entities: Includes DCSA, Government Contractor Activities (GCA), Department of Defense Inspector General (DOD IG), and other government agencies.

□ Management: Contractor management may include, but is not limited to, the SMO, KMP, program managers, and other management throughout the chain of command involved in classified operations.

□ Security Incident: Indicates actual or potential risk to classified information and is further categorized as an infraction or violation. Security incidents typically involve a security procedure that was not in place or was not followed properly (e.g., unsecured classified documents, improper receipt of classified material, data spills).

□ Security Infraction: Security incident that does not result in loss, compromise or suspected compromise.

□ Security Staff: Contractor security staff may include, but is not limited to, the Chief Security Officer, Director of Security, Security Manager, FSO, ITPSO, ISSM, and others as appropriate.

□ Security Community: Includes industrial security personnel, other cleared contractors, DCSA, OGAs, or other government entities.

□ Suspicious Contact: Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information, or efforts by any individual, regardless of nationality, to elicit information from an employee determined eligible for access to classified information, and any contact which suggests the employee may be the target of an attempted exploitation by an intelligence service of another country.

□ Security Violation: Security incident that results in loss, compromise, or suspected compromise.

□ Vulnerabilities: Identified weakness in a contractor’s security program that indicates non-compliance with the NISPOM that, based on collected evidence and implemented supplementary controls, could not be exploited to gain unauthorized access to classified information.