DCSA Gold Standard Criteria Reference Card

July 1, 2026

Criteria	Description	Criteria Requirements	Supporting Information
NE-1	Facility promptly informed DCSA of any security violations and mitigated known vulnerabilities and administrative findings in a timely manner.	a. Security staff explained the facility's security incident procedures and the requirement to report security violations to DCSA within established timeframes listed in NE-1.c. b. Maintained documented procedures related to security incidents, including timeframes listed in NE-1.c **See Considerations.** c. If the contractor had any security incidents during the security review cycle, the facility managed those incidents using the gold standard process below: 1. Immediately isolated and safeguarded affected material. 2. Conducted a preliminary inquiry within 3 calendar days. 3. If the inquiry results in a security infraction: a) Documented the incident. b) Maintained a copy for review by DCSA upon request through the security review cycle. 4. If the inquiry could not immediately rule out loss or compromise resulting in a security violation: a) Submitted an initial report within 1 calendar day for violations involving Top Secret information and within 3 calendar days for violations involving Secret or Confidential information. b) Conducted an internal investigation to make a final determination of loss, compromise, or suspected compromise. c) Submitted a final security violation report within 30 calendar days unless an extension was requested and granted in writing by an ISR prior to the 30-day suspense. 5. When needed, because 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.** d. 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). e. Maintained documented procedures related to mitigating NISPOM non-compliances within established timelines identified in NE-1.d. f. If the contractor or DCSA identified any vulnerabilities or administrative findings during the security review cycle, the facility mitigated those non-compliances using the gold-standard process below: 1. Mitigated vulnerabilities within 15-calendar days and administrative findings within 30-calendar days, or 2. 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 be written within a standalone document or maintained within the facility's standard practice and procedures (SPP).

Criteria	Description	Criteria Requirements	Supporting Information
NE-2	Appointed security personnel fully performed their duties and responsibilities outlined in the NISPOM.	a. Ensured continuity of operations by: 1. Ensuring the Senior Management Official (SMO), Facility Security Officer (FSO), Insider Threat Program Senior Official (ITPSO), and Information Systems Security Manager (ISSM) (when applicable), where appointed throughout the security review cycle, or 2. 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. b. SMO performed required duties and responsibilities as outlined in the Appointed Personnel Duties Job Aid. **See Manual Validation.** c. FSO performed required duties and responsibilities as outlined in the Appointed Personnel Duties Job Aid. **See Manual Validation.** d. ITPSO performed required duties and responsibilities as outlined in the Appointed Personnel Duties Job Aid. e. ISSM performed required duties and responsibilities as outlined in the Appointed Personnel Duties Job Aid.	Link: Appointed Personnel Duties Job Aid **Manual Validation (NE-2b):** If MS-3c is not achieved, NE-2b is also not achieved due to the SMO's failure to perform required duties and responsibilities. **Manual Validation (NE-2c):** If NE-3a or NE-4a are not achieved, NE-2c is also not achieved due to the FSO's failure to perform required duties and responsibilities.
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.	a. Established documented security procedures to the level of the contractor's operations and involvement with classified information. **See Manual Validation.** **See Considerations.** 1. All facilities: SEAD 3 Procedures, Insider Threat Procedures 2. Additionally required for safeguarding facilities: Classified Operations Procedures (e.g., SPP). 3. Additionally required for some facilities based on operations: System Security Plan, Technology Control Plan, Electronics Control Plan, FOCI Mitigation Instruments, and others. b. 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 items. c. Security staff provided relevant personnel with a copy of the documented procedures to heighten their security awareness. d. Contractor personnel followed the processes outlined within the documented procedures.	**Manual Validation (NE-3a):** If not achieved, NE-2c is also not achieved due to the FSO's failure to perform required duties and responsibilities. **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-	a. Conducted self-inspections of the security program at least once a calendar year and at least every 12 months for classified information system components (if applicable). b. Included the following requirements as part of their self-inspection process throughout the security review cycle:	**Manual Validation (NE-4a):** If not achieved, NE-2c is also not achieved due to the FSO's failure to perform required duties and responsibilities.

Criteria	Description	Criteria Requirements	Supporting Information
	inspections that addressed issues and concerns in a timely manner.	1. Reviewed classified activity, classified information, classified information systems (if applicable), conditions of the overall security program, and insider threat program. 2. Included a sampling of derivative classification actions (if applicable). 3. 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. 4. Certified to DCSA annually, 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.	**Considerations:** 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. 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.
		c. Reviewed NISPOM elements at a level commensurate with facility operations to identify NISPOM non-compliances.	
		d. Reviewed internal processes to identify gaps in security controls and determine the effectiveness of implemented procedures.	
		e. Reviewed approach vectors to determine if countermeasures were in place to mitigate potential threats.	
		f. Reviewed the FCL information in NISS and, if needed, submitted a facility profile update request or changed condition package.	
		g. Evaluated contractor personnel's knowledge and awareness of security procedures through personnel interviews, surveys, and other means.	
		h. 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 the required timeframe, implemented a plan to track and monitor mitigation, and communicated the plan and associated milestones to DCSA.	
		i. Updated documented security procedures within 30 calendar days because of the self-inspection process.	
		j. Addressed relevant issues or concerns identified during the self-inspection as part of the security refresher training. **See Considerations.**	
NE-5	Facility implemented a continuous monitoring program that facilitated ongoing awareness of threats, vulnerabilities, and changes in classified operations to	a. Monitored all elements of the industrial security program outside the formal self-inspection process.	**Manual Validation (NE-5c):** 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: (not limited to)**
		b. Adhered to the classified information systems continuous monitoring activity requirements that are part of the IS authorization (when applicable).	
		c. Explained how that facility's industrial security program facilitates ongoing awareness of threats, vulnerabilities, and changes in classified operations by: **See Manual Validation.** 1. Staying aware of potential threats that may impact the facility. **See Examples.** 2. Conducting 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.** 3. Obtained classified operation updates to include impacts to their facility clearance, new or expired classified contracts, and newly supported critical technology.	

Criteria	Description	Criteria Requirements	Supporting Information
	support organizational risk management decisions.		NE-5.c.1: Reviewed updated products such as: • Methods of Contact Methods of Operations Matrices • Targeting U.S. Technologies • Unclassified or classified threat products from relevant sources • News articles from trusted sources, as appropriate NE-5.c.2: Completed actions such as: • Reviewing DISS to ensure employee eligibility and access records are accurate • Reviewing classified documents within an open storage area or container to ensure adequate markings and need-to-know separation (when needed) • Reviewing DD Form 254s 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	a. Management included security staff in business decisions that impact the security program. **See Examples.** b. Management notified security staff prior to changes occurring that could impact the FCL to ensure prompt notification to DCSA or other government agencies (OGAs), as required. In rare cases, where notification to the security staff was not possible prior to the qualifying event, management notified security staff within 5 calendar days. **See Manual Validation.** **See Considerations.**	**Manual Validation (MS-1b):** 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.

Criteria	Description	Criteria Requirements	Supporting Information
	facility clearance.		**Considerations:** Interviewing the SMO directly is not required to award this criterion. **Examples: (not limited to)** MS-1.a: • 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.
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.	a. Management ensured authorized and cleared employees were always available to manage and implement requirements of the NISPOM. Specifically: 1. Maintained an appointed FSO, ITPSO, and ISSM (when applicable) throughout the security review cycle. 2. Maintained enough personnel to provide prompt support and successful execution of the security program. **See Considerations.** b. 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:** 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 violations • 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

Criteria	Description	Criteria Requirements	Supporting Information
			• Mitigating NISPOM non-compliances 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 and supported implementation of measures to mitigate known issues.	a. ~80% (or more) of the management interviewed were aware of the following: **See Considerations.** 1. Facility is cleared under the NISP to perform on classified contracts. 2. FCL level 3. Facility involvement with classified operations to include safeguarding, classified information systems, FOCI involvement, foreign classified operations, and others, based on their associated duties and responsibilities. b. Security staff briefed management on any necessary or lacking resources for effective implementation of the security program. c. SMO certified self-inspection results throughout the security review cycle. **See Manual Validation.** d. KMP were briefed on the results of the self-inspection throughout the security review cycle. e. Security staff notified management of relevant security vulnerabilities, systemic security problems, and issues impacting the FCL throughout the security review cycle. f. When appropriate, management provided personnel, material, or financial support to understand issues or concerns, and to implement necessary mitigation. g. Security staff briefed management on the classified IS Configuration Change Board (CCB) to manage and oversee changes to the project, scope, and budget.	**Manual Validation (MS-3c):** If not achieved, NE-2b is also not achieved due to the SMO's failure to perform required duties and responsibilities. **Considerations:** When interviewing management, the interviewer should consider 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 met the criteria. Interviewing the SMO directly is not required to award this criterion.
MS-4	Management was aware of approach vectors applicable to the facility and supported implementation of measures to counter potential threats.	a. ~80% (or more) of the management interviewed: **See Considerations.** 1. Knew the most common approach vectors applicable to cleared industry. 2. Knew the approach vectors applicable to the facility. 3. Explained how they supported measures to counter potential threats. b. When appropriate, management provided personnel material, or financial support to understand threats and implement necessary countermeasures.	**Considerations:** When interviewing management, the interviewer should consider 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 met the criteria. 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

Criteria	Description	Criteria Requirements	Supporting Information
			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.	a. ~80% (or more) of the management interviewed were able to explain the following: **See Considerations.** 1. How they obtained current and relevant threat information. **See Examples.** 2. 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 consider 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 met the criteria. Interviewing the SMO directly is not required to award this criterion. **Examples: (not limited to)** MS-5.a.1: • MCMO Matrices • Targeting U.S. Technologies: A Report of Threats to Cleared Industry" • "Foreign Intelligence Entities' Recruitment Plans Target Cleared Academia" • Government provided briefings • Other credible sources
SA-1	Contractor implemented a culture of security within the organization.	a. ~80% (or more) of the contractor personnel interviewed confirmed the facility successfully implemented a vulture of security within the organization through a set of shared attitudes, value, goals, and practices that characterized the organization commitment and implementation of security. **See Considerations.**	**Considerations:** When interviewing contractor personnel, the interviewer should consider the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work

Criteria	Description	Criteria Requirements	Supporting Information
			location, and security relevant job duties when determining if they sufficiently met the criterion. 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 visitor are briefed on local security practices and included in the overall security culture.
SA-2	Contractor personnel understood the security processes and documented security procedures relevant to their position.	a. ~80% (or more) of the contractor personnel interviewed correctly explained: **See Considerations.** 1. Which processes and documented procedures were relevant to their position. 2. Where to find documented security procedures for guidance. **See Manual Validation.** 3. How to perform processes and security procedures relevant to their position.	**Manual Validation (SA-2a2):** Evidence the facility does not have documented security procedures disqualifies the facility from achieving this criterion. **Considerations:** When interviewing contractor personnel, the interviewer should consider the length of time the interviewee has been employed at the facility, their involvement with classified operations, physical work

Criteria	Description	Criteria Requirements	Supporting Information
			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.	a. ~80% (or more) of the contractor personnel interviewed: **See Considerations.** 1. Explained what information, material, or technology required protection based on their position as outlined in classified contracts and security classification guides. 2. Demonstrated how to protect the information and material within their possession. **See Manual Validation.** 3. Explained which approach vectors were applicable to their position and the measures they individually take to mitigate a potential threat.	**Manual Validation (SA-3a2):** Evidence the facility does not have documented security procedures outlining how to protect classified material disqualifies the facility from achieving this criterion. **Considerations:** When interviewing contractor personnel, the interviewer should consider 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.	a. ~80% (or more) of the contractor personnel interviewed: **See Considerations.** 1. Had access to the facility's documented security procedures. **See Manual Validation.** 2. Had access to the facility's security classification guides related to their position. 3. Explained their obligation to protect classified information from loss or compromise. b. 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 Manual Validation.**	**Manual Validation (SA-4a):** Evidence the facility does not have documented security procedures disqualifies the facility from achieving this criterion. **Manual Validation (SA-4b)** Any loss, compromise, or suspected compromise of classified information during the security review cycle where the responsibility for the violation was assigned to someone at the facility disqualifies the facility from achieving this criterion. **Considerations:**

Criteria	Description	Criteria Requirements	Supporting Information
			When interviewing contractor personnel, the interviewer should consider 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.	a. ~80% (or more) of the contractor personnel interviewed explained the requirements to report the following relevant security issues to security staff when related to their position: **See Considerations.** 1. Failure to follow established security procedures. 2. Possible loss, compromise, suspected compromise of classified information. 3. Cyber incidents on classified information systems. 4. SEAD 3 and adverse information elements. 5. Suspicious contracts. b. Cleared personnel reported all security-related issues outlined above to security staff. c. Security staff explained the facility's procedures for submitting reports outlined in the NISPOM and contractual requirements to DCSA. **See Manual Validation.** d. Security staff reported security violations, SEAD 3/adverse information reports, foreign travel, cyber incidents, and suspicious contacts to DCSA as required.	**Manual Validation (SA-5c):** Evidence the facility does not have documented security procedures outlining reporting requirements disqualifies the facility from achieving this criterion. **Considerations:** When interviewing contractor personnel, the interviewer should consider 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.
SC-1	Contractor personnel cooperated with government entities during official visits and security investigations.	a. Cooperated with government entities throughout the security review cycle by taking the following actions, when applicable: 1. Provided suitable arrangements within the facility for conducting private interviews with employees during normal working hours. 2. Provided relevant employee or personnel files, security records, supervisor files, insider threat records, and any other records pertaining to an individual under investigation whether at the office or another location. 3. Submitted a NISS Facility Profile Update request or changed condition to ensure FCL documentation and contact information is current, when needed. 4. Provided information and completed follow-up actions when requested by DCSA because of an engagement, inquiry, or other request. 5. Rendered necessary assistance to support government-led investigations.	

Criteria	Description	Criteria Requirements	Supporting Information
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.	a. Reported relevant events outlined in NISPOM 117.8 and contractual requirements to DCSA and other government agencies. **See Considerations.** b. Shared relevant threat information within the security community. **See Considerations. See Examples.**	**Considerations:** Contractor security staff can share potential threat information from the corporate level within a Multiple Facility Organization. If 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: (not limited to)** SC-2.b: • Shared relevant information through DIBNet or DIBNet • Shared relevant information that might otherwise be unavailable • Provided DCSA with cyber network logs
SC-3	Contractor coordinated with relevant stakeholders to obtain accurate and sufficient security classification guidance.	a. Security staff reviewed all aspects of the security classification guidance, including embedded security contract clauses, to ensure all requirements were identified and implemented. b. 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. If a remedy was not provided to the initial challenge, security staff submitted a formal written challenge to the GCA (or prime contractor). If needed, the contractor requested assistance from DCSA. c. As the prime contractor, responded to the subcontractor security classification guidance challenges and coordinated with the GCA for a remedy. d. Coordinated with the customer for a Risk Acknowledgment Letter, when appropriate, for classified information systems.	
SC-4	Contractor provided support to the security community that positively	a. Provided support to the security community in a way that positively impacted the NISP. **See Examples.**	**Examples: (not limited to)** • Provided information to the security community through weekly emails that were used by junior and senior security

Criteria	Description	Criteria Requirements	Supporting Information
	impacted the national industrial security program.		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 to grow as security professionals. • Served as an officer in a professional security organization which impacted the security professionalization of hundreds of FSOs within xx chapter.
SC-5	Contractor security staff participated in security community events, conferences, or webinars that positively impacted their security program.	a. FSO participated in a minimum of two security community events/training per calendar year which positively impacted the facility's security program. **See Examples.** b. ITPSO participated in a minimum of two security community events/training per calendar year which positively impacted the facility's security program. **See Examples.** c. ISSM, if applicable, participated in a minimum of two security community events/training per calendar year which positively impacted the facility's security program. **See Examples.**	**Examples: (not limited to)** • Participated in a virtual industrial security conference and used the knowledge to mentor/training others within the facility's security program. • Attended a DCSA hosted SVTC and implemented countermeasures at the facility based on newly discovered threat information. • Completed a CDSE training course and use the knowledge gained to update internal training for cleared personnel. • Attended a local workplace violence seminar and used to the

Criteria	Description	Criteria Requirements	Supporting Information
			knowledge gained to update internal security procedures. • Participated in an NCMSLive! webinar and used the knowledge to send updated communications to cleared 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.
- Contractor Personnel: Includes cleared and uncleared employees, on-site subcontractors, on-site government personnel, and visitors (as appropriate).
- Government Entities: Includes DCSA, Government Contractor Activities (GCA), Department of Defense Inspector General (DOD IG), and other government agencies.
- Management: Includes the SMO, KMP, program managers, and other management throughout the chain of command involved in classified operations.
- Security Community: Includes industrial security personnel, other cleared contractors, DCSA, OGAs, or other government entities.
- 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: Includes the Chief Security Officer, Director of Security, Security Manager, FSO, ITPSO, ISSM, and others as appropriate.
- Security Violation: Security incident that results in loss, compromise, or suspected compromise.
- 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.
- 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 be exploited to gain unauthorized access to classified information.

VISUAL LEGEND

Blue	Terms defined within the "Terms and Definitions" section above used to assist with consistent implementation.
Orange	Considerations which add context or clarifying information to consider when determining if a contractor achieved the criterion elements.
Purple	Examples of how a contractor may achieve a criterion element. Note that these are not the only ways to achieve an element, and the listed examples may change based on available programs. DCSA will always consider the intent of the element when awarding the criterion.
Dark Red	Manual Validation of the criterion element or a subsequent criterion is needed using the supporting information provided.