



DCSA Additional guidance during COVID-19

What can I expect during my Continuous Monitoring (CM) Engagement?

In lieu of implementing Enhanced Vulnerability Assessments (ESVAs) or other engagements at this time, DCSA is implementing a CM strategy intended to identify facilities that are continuing operations, offer guidance, assistance, assess the current security situation under the circumstances, and ensure classified information remains secure. CM Engagements will not result in a security rating, as they do not take the place of an ESVA, but vulnerabilities can be cited. Facilities that undergo a CM Engagement during the COVID-19 pandemic may also receive an ESVA after normal operations resume.

If your facility previously had an ESVA scheduled during this time, you will be prioritized for a CM Engagement. You will be contacted by your Industrial Security Representative (ISR) prior to the CM Engagement and may be asked to provide the following documentation via the NISS messaging function prior to the scheduled Engagement:

- Insider Threat Program (ITP) Plan
- Request for Information
- Contracts List
- Consultant Security Agreements
- Training Transcript for the Facility Security Officer (FSO) and Insider Threat Program Senior Official (ITPSO)
- Self-Inspection Senior Management Official (SMO)-Endorsed Certification
- Foreign Ownership, Control, or Influence (FOCI) documents
- Security Violation Reports
- CISA may request Suspicious Contact Reports
- Listing of Authorized Information Systems

Please inform your ISR prior to the scheduled CM engagement if you do not have access to any of the above documents that are appropriate for your facility. The CM Engagement can still occur without all of the required documents. Contractors without NISS accounts should obtain access prior to the CM Engagement.

The CM Engagement will occur telephonically and is a conversation focused on current operations/impacts during the crisis as well as the security posture of the facility. The ISR is the main DCSA representative conducting the CM Engagements, but you may also be contacted by an Information System Security Professional (ISSP) or Counterintelligence Special Agent (CISA). The length of CM Engagements varies based on facility operations, and can last anywhere from 30 minutes to 3+ hours. Following the CM Engagement, the FSO will receive a summary of cited vulnerabilities and follow-up actions. The SMO will also receive a letter summarizing the engagement.

Questions regarding CM Engagement should be sent to your assigned ISR. NISP guidance related to the COVID-19 crisis will continue to be released on www.DCSA.mil.



Additional Authorization Guidance

The Region AOs will continue to perform assess and authorize activities and manage workload appropriately.

System registrations in eMASS that have submitted completed packages (CAC1 workflow) with an ATD prior to 30 June, will be assessed and considered for extensions up to 180 days. Either the ATO or Extension workflow in eMASS will be utilized as appropriate.

For new system registrations in eMASS, the Security Control Assessment (SCA) activity will continue to occur. The onsite portion of the SCA activity may be delayed, deferred, or rescheduled. Documenting evidence of security and validation requirements remains unchanged; only the execution of onsite activity will change temporarily.

Guidance for collaboration software

DCSA understands the need to add new software or capabilities, especially in light of the current situation, and the Configuration Management (CM) plan provides the path forward for making changes or additions. Industry should follow the documentation and guidance listed in their approved System Package which defines their plan for CM and has been reviewed and authorized by DCSA. This will ensure industry ISSM's are following their CM plan and DCSA ISSP's will be able to refer to the CM plan authorized.

Questions regarding Information Systems should be sent to your assigned ISSP. NISP guidance related to the COVID-19 crisis will continue to be released on www.DCSA.mil.