SEPTEMBER 2026

Newsletter

Our services are centered around proven policies, procedures and training that deliver compliance with government security requirements.

www.FSO-Services.com **@fso-services-llc**

Complete Your Annual Self-Inspection Before Year-End

Year-end is the right time to confirm your industrial security program is current, documented, and ready for DCSA oversight.
NISPOM requires cleared contractors to conduct a self-inspection at least annually. This review is an opportunity to identify gaps, address corrective actions, and ensure required records, training, personnel actions, and procedures are up to date.

Once your self-inspection is complete, remember to update your NISS profile with:
The date of the completed self-inspection and a signed certification letter from your Senior Management Official.

DCSA will certainly review this in your next audit.

FSO Services can help you plan and conduct a thorough self-inspection, document findings, develop corrective-action plans, and ensure your NISS profile is updated correctly. Our team supports cleared contractors, so internal teams can stay focused on their core business.



Key Dates To Know

September 2026: IEP self-reporting is expected to deploy

September 30: New initiations in NBIS Agency end

November 30: NBIS Agency shuts down. Cases still in an IRA phase must be re-initiated in DISS

FY target: Initial investigations using the PVQ are planned to become available in DISS.

DISS and NBIS Changes:
Are You Prepared?

DCSA is moving key personnel-vetting functions into DISS, with several deadlines ahead. These updates affect how cleared companies initiate, review, and manage personnel clearances.

What's changing

IRA returns to DISS: Initiation, Review, and Authorize functions are moving back into DISS, creating one workflow for personnel vetting. eApp will remain the applicant portal for completing forms.

New Personnel Vetting Questionnaire: This will replace Standard Forms. It introduces streamlined questions and shorter look-back periods for many disclosures.

Individual self-reporting: Expected in September, the Individual Engagement Platform will allow personnel to submit certain reportable life events directly. Security personnel will review and act on that information in DISS.

FSO Services provides hands-on DISS, NISS, and personnel-clearance management support for cleared contractors. We can help review your access, prepare active cases for transition, and keep your program ready for DCSA oversight.
Need support navigating these changes? Contact FSO Services to discuss your security program.



AI Is Accelerating Personnel Vetting.

Is Your Security Program Ready?

DCSA is advancing personnel-vetting modernization with artificial intelligence pilots designed to automate risk triage, improve alert accuracy, and reduce manual processing.
For cleared contractors, the goal is clear: routine, low-risk actions may move faster, while security teams can focus attention on cases that require informed review and follow-up. DCSA's broader efforts also include enhanced automation, e-Adjudication for cases without substantive issues of concern, and real-time Continuous Vetting alerts.

As vetting workflows become more automated, accurate data and disciplined system management matter even more. Facility Security Officers will still play a critical role in initiating cases, monitoring status, responding to issues, and maintaining compliant personnel-clearance records.

Need support with DISS, NBIS, or personnel-clearance management?

Contact FSO Services to strengthen your program.



CMMC Phase II Is Suspended, but Cybersecurity Responsibilities Remain

The Department of War has suspended CMMC Phase II requirements, including the planned transition to Phase II contract requirements that had been scheduled to begin November 10, 2026.

The suspension took effect July 13, 2026, while the Department conducts a 60-day review of the program.

For contractors, this is a pause, not a reason to set aside cybersecurity compliance.

Use this time to validate your current security practices, address documented gaps, and keep assessment records current. Strong cybersecurity controls remain essential to protecting government information, supporting contract performance, and maintaining a resilient security program.

Stay tuned for more CMMC updates.
Visit: fso-services.com

What remains in effect?

- CMMC Phase I self-assessment requirements
- NIST SP 800-171 Rev. 2 compliance through self-assessments and select government-led assessments
- Your obligation to protect covered defense information under DFARS 252.204-7012