**DCSA ISR Inspection Preparation**

**Who will be in attendance?**

* Company: FSO, A-FSO, KMP/SMO, ITPSO, ISSM, ISSO
* DCSA: ISR, CISSP, CISA

**Initial overview of company operations (SMO/KMP)**

* Company business overview and org chart
* Review of active classified contracts
* Potential future classified / sensitive work you’re going after
* Any changes that may impact FCL (address, KMP, company ownership?) – closed area addition, SCIF/JWICs plans, other expansion?
* Details on how SMO is involved with security program (self-inspection reviews, regular meetings, monthly reports, staffing education, etc.)
* Explanation of the classified contract deliverable lifecycle (CCDL) *– be prepared to provide a summary of* ***each*** *CCDL for active classified contracts*

**Inspection Roles**

* Facility: ISR, FSO, A-FSO, ITPSO, SMO/KMP
* Information Security: CISSP, ISSM, ISSO
* Counterintelligence Security: CISA, Staff (random selection for interviews)

**Four Review Areas:** (all equal value)

1. NISPOM Implementation
2. Management Support
3. Security Awareness (CISA input and result of interview is critical to this)
4. Security Community

Have on hand (Compliance Area):

* CCDLs (see above) (1)
* Self-assessment checklist, summary letter to SMO (1)
* SCSA Form 381-R Facility Clearance Request/Approval Letter (1)
* DD Form 441 – DoD Security Agreement (1)
* Facility clearance verification (1)
* List of DD254s (1)
* Physical DD254s (1)
* List of cleared active employees (1)
* List of uncleared active employees (1)
* List of exited cleared employees & what their NTK was before they left (1)
* FSO, A-FSO, ITSPO training certificates (1)
* Initial and annual training briefings (1/3)
* COMSEC training and briefing information (1/3)
* List of NATO-briefed staff (1)
* NATO briefing (1)
* Insider Threat Plan (1)
* Suspicious contact reports (1/3)
* Reported security incidents and violations reports (1/3)
* Foreign National visits (packages on hand) (1)
* List of FSO/A-FSO community and training events attended (w/ certs if available) (4)
* KMP List (1)
* FSO and A-FSO appointment letter (1)
* ITPSO appointment letter (1)
* Security Policy Letter (1)
* Insider threats reporting (1)
* PCL processing (i.e., SF-86 and eQip, SF-85) (1)
* Consultant management (1)
* Foreign travel reporting information (1/3)

Have in location and ready for review:

* Visitor logs (1)
* Facility signage throughout (i.e., hotline posters, security posters, shred/destruction signage, no electronics, etc.) (1/3)
* Closed area perimeter monthly log (if applicable) (1)
* Container logs (w/ each container and completed sheets in binder) (1/3)

**Management Support – SMO Involvement (2)**

These are the areas to expect the ISR to inquire about during the inspection. These topics are areas that the SMO and/or the FSO should be able to provide examples/proofs.

* Facility maintains a sustained high level of management support for the security program.
	+ Example PROOFS: (1) Engagement with the security team in multiple weekly meetings, (2) active engagement on the execution and monitoring of the OPSEC posture of the facility, (3) regular review of NTK lists, (4) participation in any insider threat risk mitigation strategies required for the CAGE code
* Management includes security staff in senior level meetings and business decisions affecting the security program.
	+ Example PROOFS: (1) FSO attends meetings involving facilities short and long term facilities planning with senior leadership, (2) FSO attends high level meetings to discuss SCIF/JWICS customer needs, (3) FSO included in discussions related to the OPSEC needs of local customer, (4) other . . .
* Management provides security staff the resources to oversee the security program (as needed) consistently and effectively.
	+ Example PROOFS: (1) company investment in staffing, (2) investment in resources that protect information to include closed area, closed/classified networks, safes/containers, IDS, access control systems, security information database (i.e., SIMS, MSAccess), implementation of AIP, staff training (i.e., corporate training system, CDSE course, etc.)
* Management is consistently and fully informed of the facility’s classified operations.
	+ Example PROOFS: (1) frequency of communication b/t the SMO and FSO/Security Team (meetings, Teams, personal phone comms 24/7 availability, open door policy to address any security concern)
* Management is consistently and routinely informed of approach vectors applicable to the facility and supports implementation of measures to counter potential threats.
	+ Example PROOFS: (1) SMO knowledge of cyber threats, ITAR/EAR risks, foreign contact reporting, security incidents/violations regardless of severity, visitor lists, foreign national visitors
* Management makes decisions based on threat reporting (classified and unclassified) and their thorough knowledge, understanding, and appreciation of threat information and potential impacts caused by a loss of classified information, classified contract deliverables, and technology.
	+ Example PROOFS: (1) SMO coordination w/ senior company management on understanding of threats to the organization (i.e. insiders, cyber, etc.)
* Senior Management Official retains accountability for the management and operations of the facility without delegation to a subordinate manager.
	+ Example PROOFS: (1) direct SMO involvement demonstrated by knowledge of all of the above
* Management embeds a culture of security throughout the organization.
	+ Example PROOFS: (1) ability of the staff to demonstrate their security awareness (review area #3) in:
		- What the facility and staff member protect related to classified contracts and programs, SCGs, and approach vectors.
		- The facility and staff member’s responsibility to protect and safeguard classified information in their possession or what they have access to.
		- Understand what a reportable event is and how to report one in areas applicable to their role.
		- Provide a Q&A for staff to review prior to inspection.