The Security Review – Meeting with DCSA

Note: not ALL of these happen, but if they happened 2-4 times, we added it to the list. Also – this does not include any items DCSA asked you to complete prior to the review such as documentation in NISS and security interview schedules.

Room set-up: We usually recommend water, coffee and some healthy snacks. Meeting room with outlets, WIFI and pw maybe a large screen if available; silence your phone/laptop.

Introductions, DCSA presents their credentials, discusses anything new (new Director) and provides overview:

There are four categories today in the security review.

1. Senior management support – Does leadership support the security program?
2. NISPOM Implementation – All administrative compliance items.
3. Security awareness - CISA and MCMO
4. Security community – Member of organizations

Opening Meeting with Senior Management Official:

- Senior Management Official: Explain the projects that you're currently working on? The areas of service that you actively provide for the federal government.
- Do you have any potential expansion of this work planned?
- How many personnel do you currently have working on this project?
- DD254s – How many active? Do you have any personnel working on the DD254? Contracts Administration/DD254s – who receives that and makes the FSO aware?
- Specialized Briefing Requirements: NATO, FGI, CNWDI?
- Any Subcontracting companies? If yes, how are your verifying their FCL information?
- Do you have any International Contracts with foreign entities?

Company Documentation Review with FSO:

- NISS Profile – all correct? Review.
- ITBL Updated on the profile?
- Signed DD441? Updated SF328?
- How many personnel do you currently have working on cleared contracts?
- DD254s – How many active? Do you have any personnel working on the DD254? Contracts Administration/DD254s – who receives that and makes the FSO aware?
- Any exclusions?
- Who are your NISS users currently?
- Any unreported or planned changes that would affect your FCL?
- FOCI Mitigation tools – all approved?

Personnel Review with FSO:

- DISS account Management? NBIS Account Management? Backups for each? Training up to date? Yes
- What do you use for Fingerprints?
- Onboarding: Walk us through the steps of a new clearance start to finish.

- Onboarding of a cleared person process.
- Has anyone ever refused to sign an SF312?
- DISS Records: Is everyone in access or in CV? What are the clearance levels?
- Do you have any out-going long-term visitors? Process?
- Do personnel know what to report? (such as 13 Adjudication Guidelines and SEAD 3)
- If someone were to have something adverse to report or foreign travel – how would that be handled?
- Where are the reports kept?
- Are any of your personnel in DISS a non-W2? Do they have Consultant Certificates signed by the Independent Contractor and the SMO?
- Tell us about your Training and Briefings? What are your personnel required to take? Onboarding, Annual/Insider Threat, Foreign Travel – anything extra?
- When do you provide your training?
- How do you provide your training?
- Do you give them a timeframe?
- How do you confirm they have taken it? Where do you keep the records? What do you do if someone refuses to complete the training?
- Do your employees access work on government or company provided issued tech (computers, phones?) Any Government Furnished Equipment? Do they have government emails?
- Do they have badges or CACs? How is that collected upon termination?
- Tell me about your off-boarding procedures

FSO and ITPSO Information Review with FSO and ITPSO

- Have you completed your FSO Training? Do you have an appointment letter?
- Have you completed insider threat training? Do you have an appointment letter?
- Are they in NISS?
- Do you have an Insider Threat Plan with current References?
- Who are the Members of the insider threat working group?
- How often do you meet?
- Do you take minutes or notes?
- Where are the minutes/notes kept?
- What do you do if an Insider Threat Indicator is confirmed?
- Have they taken the "Insider Threat Working Group" Training?
- Have you any compromise of CUI are higher information?
- How is the relationship between FSO and HR or payroll?
- Have you had to make any adverse reports? If yes or no – can you walk me through the process for that?
- As far as your company - have there been any successful cyber intrusions with your company? Anybody breach your networks, especially with a phishing, email, anything of that nature? Have you been sent any kinds of phishing emails, spam? If yes, who handles that at your company? If it is outsourced, how are reports provided?

SPP Review

- Do you have an SPP?
- Does it indicate your SEAD 3 procedures?

- If someone were to have a security violation – do you have a graduated scale of disciplinary procedures? Is the scale in your SPP?
- Is foreign travel procedures in your SPP?
- Are the security procedures specific to your organization in your SPP?
- Is this SPP made available to your personnel? If yes, how?

Self-Inspection Review – Reviewed with the FSO

- Tell us about your Self-Inspection – how often do you do a self-inspection? When do you do that each one?
- What do you use to complete a self-inspection?
- When was your last self-inspection?
- Did you identify any findings? If yes, did you discuss this with your Senior Management Official?
- Did you complete any interviews with your personnel?
- How did you self-certify your self-inspection?
- Did you use a memo or report?

Counterintelligence and Marketing – Reviewed with your FSO

- Any visits from our local PD NCIS FBI?
- Do you know what MCMO and who your CISA is?
- Do you advertise your FCL anywhere or offer compromising information?
- Are you a member of any Security Associations? If yes, how do you participate? How often?
- (Any interaction or do you know who your Counter Intelligence Special Agent is?)
    - Monthly update for reports, foreign travel briefings and Trade shows.
    - Suspicious contacts from your website, Linked in?
    - Even if you're not considering them as potential candidates.
    - McMo Information

Exit Briefing:

- DCSA will provide any follow up email with findings and ratings. The Senior Management official will receive a Letter to Management (LTM) that will be signed by our Field Office Chief.
- In addition to that, there will be a summary of what was what was discussed and FSO comment sheet with actions to take or recommendations.
- If there is anything to correct, you will have 30 days from today to get us back that plan of action for any administrative finding. That 30-day clock starts on the day of the Review.