WBSI
web business solutions inc.

Security Newsletter April 2017

Introduction to DISS

By: DSS

The Defense Information System for Security (DISS) is a family of systems that will serve as the system of record for comprehensive personnel security, suitability and credential management of all military, civilian and DoD contractor personnel. DISS also provides secure communications between adjudicators, security officers and component adjudicators in support of eligibility and access management. DISS is undergoing a phased deployment and is set to launch for Industry in the 3rd Quarter FY 17.

To achieve this vision, we are developing a new methodology based on:

-- knowing the assets at each cleared facility
-- analyzing and considering threats to those assets
-- understanding business processes related to assets
-- determining vulnerabilities to assets
-- implementing countermeasures to address the threats
-- developing tailored security programs
-- conducting continuous reviews of tailored security programs
-- comprehending and articulating to our partners the impact of compromise
-- remaining in frequent contact with facility security professionals and program managers.

Finally, we formed an enterprise-wide integrated project team to best identify assets at cleared facilities and maintain and continuously update the information.

Thank you for your dedication to DSS and our important mission."

Dan Payne, Director DSS

Security Clearance Process – The Interview

By: Clearancejobs.com

A lot of misconceptions about the security clearance process circulate throughout the years. All too often, these misunderstandings relate to an applicant's interaction with an investigator, almost all of which takes place during the personal interview. A number of resources exist to help you prepare for the personal interview…..below are some helpful hints of what you should and should not expect from your investigator(s).

Your investigator *should not:*

- Pretend he or she is a homicide detective. The personal interview is not a jailhouse interrogation. It is a consensual, amicable, fact-finding discussion between investigator and applicant.
- Schedule appointments solely around his or her schedule. Ideally, the investigator should meet at a mutually beneficial time, and at the appropriate location (either a government space or an employer site).
- Ask questions that alter from the language on the SF-86 questionnaire. While the interview should have a conversational tone, your investigator should read the questions on the SF-86 verbatim. An investigator who provides his or her own interpretation of the questions encroaches into risky territory, especially if an applicant misunderstands a question and the response substantially affects the final adjudication.
- Volunteer information to the applicant or sources about information provided by other sources over the course of an investigation, particularly if this information is adverse. The Privacy Act of 1974 governs this area.
- Indicate whether any information disclosed by the applicant will negatively impact the final adjudication. The adjudicative process is entirely separate from the field work conducted by investigators, which is an objective process.
- Meet the applicant or sources in public places where people can overhear sensitive dialogue.
- Update you with the status of your investigation. Once an applicant completes the personal interview, questions regarded to the status of an investigation should be directed to OPM or the appropriate security official overseeing the process.
- Tell the applicant how long the adjudicative process will take. Investigations are a complex, thorough undertaking, and their duration is unique to the facts in each every case.
- Discuss or elicit classified information at any point during the investigation.

Your investigator *should:*

- Display his credentials (badge) at the outset of any interview.
- Upon request, provide information about how an applicant can request a copy of his or her background investigation. This information is also easily accessible on the OPM web site.
- Clarify any questions that the applicant may not understand over the course of the interview, and provide the applicant a chance to clarify or expand upon any information before the close of the interview.
- As a corollary to the previous point, fully understand the questions he or she is asking.
- Be cordial, professional, and accessible throughout the investigative process. Both the applicant and the investigator share a common goal of completing the investigation efficiently and effectively. Contentiousness frustrates these ideals.
- Provide a list of disclaimers at the start of the interview, which may include the penalties for falsifying information, the purpose of the interview, and an oath or affirmation.
- Conduct interviews in person, whenever feasible. This reflects upon the credibility of both the investigator and the interviewee or record provider. Considering the importance of the subject matter, both parties should know exactly who they are speaking with.
- When scheduling the personal interview, provide the applicant with a reasonable estimation of how long the personal interview will last. This is not an exact science, but an experienced investigator who thoroughly researches the SF-86 beforehand should have a feel for the duration of the interview.
- Inform the applicant of any materials, items, or documents the applicant needs to bring to the personal interview (ID: always; a personal copy of the SF-86: usually a good idea to ensure there are no discrepancies with the investigator's copy).
- Promptly follow up with an applicant if important information was unavailable at the time of the personal interview. Failure to do so impacts the efficiency of the investigation and the reliability of the final adjudication.

OPSEC – Do's and Don'ts for Unclassified Information

By: DoD, Education Activity

DO NOT

- Post sensitive information on social networking sites such as Facebook, Twitter, YouTube etc.
- Post sensitive information on public websites
- Place sensitive information in trash cans or recycle bins
- Leave sensitive information in vacated offices
- Leave sensitive information unattended
- Allow access to those individuals without a "need-to-know"
- Place sensitive information on shared drives unless password protected

DO:

- Encrypt email when sending sensitive information
- Review information for sensitivity prior to posting on social networking sites
- Review information for sensitivity prior to posting on websites
- Look at information before throwing it in the recycle or trash bins
- Ensure you have enough supplies (burn/shred bags) on hand to discard sensitive information
- Look behind desk drawers and under desks for information that may have fallen
- Password protect information placed on shared drives and apply the "need-to-know" principle

NEW DoD HOTLINE:

Anyone may file a complaint with the DoD Hotline. While you may contact the DoD Hotline at any time, a more expeditious route towards the resolution of your problem might best be served to first CONTACT YOUR LOCAL SECURITY OR COMMAND-LEVEL IG OFFICE.

Please make note and bookmark the following website. The website allows you to select the type of complaint you wish to report as well as the method of reporting.

http://www.dodig.mil/hotline/

CONTACT US:

Holly Higgins/FSO: holly.higgins@wbsi.com

Charity DellaCamera/ALT FSO: charity@wbsi.com