Non-NISP

Presented to: Small Business Roundtable

Presented by: Michael George
Security Specialist

What is a Non-NISP?

- A Non-NISP contractor employee is an employee who **DOES NOT** require access to classified information but **DOES** require access to sensitive data and/or IT-I or IT-II level system access.

3 Groups of Contractor Employees

GROUP 1

Contractors who require access to classified material in accordance with their labor category.
(Cleared Contractors)
Example: Acquisition Specialist

GROUP 2

Contractors who do not require access to classified material but does require access to IT systems and/or sensitive data.
(Non-NISP Contractors)
Example: Tool Room Issuer

GROUP 3

Contractors who do not require access to classified material nor do they require access to IT systems and/or sensitive data.
(Non-Sensitive Contractor)
Example: Grass Cutter

Who is responsible for processing?

- Within the Statement of Work (SOW) each labor category has it's own security requirements. Depending on the security requirements dictates who will process the investigation for that employee.

- **Group 1-** The Facility Security Officer (FSO) is responsible for initiating and processing these contractors for a Security Clearance.

- **Group 2-** The Local Command (Government Personnel Security Team) is responsible for initiating and processing these contractors for a "favorable" determination. **NOT** access to classified material.

- **Group 3-** The Contracting Officer Representative (COR) is responsible for processing these contractors for Installation Access Only using the Defense Biometric Identification System (DBIDS).

Is the Contract Sensitive?

- In accordance with NAVAIR Instruction 5510.38 All NAVAIR, PEO/Program Office and NAWCAD military, civil service, FRC and on-site Contractor Support Service (CSS) positions shall be considered sensitive.

- This means **ALL** contractors in accordance with the above mentioned will be initiated a T3 or T5 investigation depending upon the IT requirements.

What is considered when making a Security Determination

- **Security will make a local access determination based on the following 13 adjudicative guidelines**:
- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Use of Information Technology Systems

When making a local access determination based on the adjudicative guidelines the Security Specialist will take into account the following:

- Nature
- Knowledgeable participation
- Frequency and recency
- Age
- Rehabilitation
- Potential for pressure, coercion, exploitation or duress
- Likelihood of continuance

Obtaining a Common Access Card (CAC)

- Once a Non-NISP employee completes the e-QIP application and no derogatory information is found or mitigated. The employee is required to be fingerprinted which is reviewed by the FBI. If the fingerprint results return favorable the COR is notified that the employee has met the minimum qualifications to obtain a CAC.

- The minimum requirements to obtain a CAC is: A NACI, or DoD-determined equivalent, investigation has been submitted to OPM and an FBI fingerprint check has returned with favorable results.

No Local Access Determination

- When the Command Security Manager makes a No Local Access Determination, the government sponsor and contractor company would need to be willing to move the employee to non-sensitive duties under a non-sensitive contract with the company until a favorable adjudication takes place or the government sponsor may provide another candidate.
- **The company has the sole prerogative for continued employment decisions.**
- If a Contractor Employee is already in a denied status with the DODCAF as a result of a previous investigation, a No Local Access Determination will be made unless the employee can provide his/her due process package from the DODCAF. This package must contain the Letter of Intent and Letter of Notification. If the information contained within can be mitigated, the Command Security Manager would have to make a decision to submit a request for reconsideration to the DODCAF. The reconsideration takes approximately 8 months and the employee may not have access to sensitive information or sensitive IT systems until a final determination is made.

For processing of Non-NISP personnel contact:

Mike George- Non-NISP Point of Contact

Tel: 301-757-3672 E-mail: michael.d.george1@navy.mil

All Non-NISP requests are sent to the following email:

NAWCAD_7.4.1_NONNISP@navy.mil