OMB Approval Date:
OMB No: 0704-0427
Expiration Date:

DEFENSE SECURITY SERVICE INDUSTRIAL SECURITY REVIEW DATA

Agency Disclosure Notice

Public reporting burden for this collection of information is estimated to average 5.3 hours/minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (OMB NO. 0704-0427), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that not withstanding any other provision of law, no person shall be subject to any penalty for failing to comply with this collection of information if it does not display a currently valid OMB control number. **Please do not return your response to the above address.**

Privacy Act Statement

Authority: 50 USC, Sections 781– 887, "Internal Security Act of 1950;" Executive Order (EO) 9397, "Numbering System for Federal Accounts Relating to Individuals," November 22, 1943; EO 10865, "Safeguarding Classified Information Within Industry," February 20, 1960 as amended by EO 10909, January 16, 1961, and EO 11382, November 27, 1967; EO 11935, "Citizenship Requirements for Federal Employment;" EO 12333, "United States Intelligence Activities," December 8, 1981; EO 12656, "Assignment of Emergency Preparedness Responsibilities," November 18, 1988; EO 12829, "National Industrial Security Program", January 6, 1993 as amended by E.O. 12885, December 14, 1993; EO 12958, "Classified National Security Information," April 17, 1995, as amended March 25, 2003 and 5 USC Section 301, "Department Regulations."

Principle Purpose(s): Utilized for evaluative purposes to make security determinations for initial access to classified information, sensitive areas, or equipment; or to permit assignment to sensitive national security positions. The data is also used as part of a review process to evaluate continued eligibility for access to classified information. The Social Security Number will be used to verify, identify and locate existing records.

Routine Use(s): Provided to federal, state or local government agencies if necessary to obtain information for a personnel security clearance, or making a personnel security determination concerning retention in a sensitive position, or letting a contract. May be provided to a congressional office in response to an inquiry made at the request of the individual; or to foreign or domestic law enforcement, security, investigative, and administrative authorities to comply with domestic and/or international agreements. Provided to the Department of Justice in pending or potential litigation to which the record is pertinent. For records management purposes data may be provided to the General Services Administration and National Archives and Records Administration. Data may also be disclosed for counterintelligence activities, authorized by Federal Law or Executive Order, within and outside the DoD or the U.S. Government.

Disclosure: Voluntary; however, failure to furnish the requested information may result in our being unable to retain the contractor's facility clearance (FCL) in a valid status.

DEFENSE SECURITY SERVICE INDUSTRIAL SECURITY REVIEW DATA

As a result of the Security Review, DSS shall retain information pertaining to the Facility's security posture and safeguarding capability for a period of two years after termination of the FCL. Information pertaining to other industrial security actions shall be retained for a period of two years after completion of the action. All information gathered shall be marked and handled as "For Official Use Only" and/or with a classification marking, as appropriate.

1.1. Information to be maintained includes, but is not limited to:

1.1.1. Basic FCL and storage capability information:

1.1.1.2. Contractor legal name.

1.1.1.3. Contractor alias names.

1.1.1.4. Contract and Government Entity (CAGE) code.

1.1.1.5. Physical address.

1.1.1.6. Unclassified mailing address.

1.1.1.7. Classified/overnight mailing address.

1.1.1.8. Facility Security Officer (FSO) name.

1.1.1.9. Phone number/e-mail address.

1.1.1.10. FCL level.

1.1.1.11. Clearance date.

1.1.1.12. Approved storage capability and level.

1.1.1.13. Special access categories.

1.1.1.14. Key Management Personnel (KMP) identifying information.

1.1.1.14.1. Name.
1.1.1.14.2. Title.
1.1.1.14.3. Social Security Number.
1.1.1.14.4. Date and place of birth.
1.1.1.14.5. Personnel Security Clearance status.
1.1.1.14.6. Citizenship.

1.1.1.15. Parent/Home Office (HOF)/Principle Management Facility (PMF) information, if applicable.

1.1.1.16. Information pertaining to approved off-site locations, if applicable.

1.2.1. Contractor information pertaining to approval actions (e.g., Automated Information Systems (AIS), Standard Practice Procedures, and/or reports of changed conditions, suspicious contacts, security violations, adverse information and administrative inquiries. Information may include:

1.2.1.1. Full name.
1.2.1.2. Social Security Number.
1.2.1.3. Date and place of birth.
1.2.1.4. Citizenship.
1.2.1.5. Home address.
1.2.1.6. Physical work site.
1.2.1.7. Employment status.
1.2.1.8. Personnel Security Clearance Status.
1.2.1.9. Circumstances generating the report/approval.
1.2.1.10. Classified material/equipment involved.

1.3.1. Results of Security Reviews.

1.3.1.1. Contractor input pertaining to security review findings.

1.3.1.2. Corrective action required and actions taken.

1.4.1. Type of business.

1.4.2. Business/Legal structure.

1.4.3. Contract/subcontract information.

1.4.4. Foreign Ownership Control or Influence (FOCI) mitigation instrument, if applicable.

1.5.1 Number of employees.

1.5.1.1. Number of cleared employees by clearance level and justification for continued clearance.

1.5.1.2. Cleared employees assigned to uncleared locations.

1.5.1.3. Numbers and types of Limited Access Authorizations.

1.5.1.4. Numbers and types of Non-U.S. citizens.

1.6.1. Numbers and types of storage containers and facilities.

1.6.2. Numbers and types of classified material – documents, hardware, software.

1.6.3. Numbers and types of AIS.

1.6.3.1. AIS inter/intra connections and Memorandums of Agreement

1.6.4. Information Material Controls.

1.6.4.1.Classified Material Controls/Accountability.

1.6.4.2. Receipt and Dispatch Records.

1.6.4.3. Reproduction and Disposition.

1.6.5. Classification Management and Markings.

1.6.6. Visitor Control.

1.6.7. Transmission/Transportation.

1.7.1. Applicable threat assessments.

1.8.1. International involvement.

1.8.1.1. Foreign classified contract information.

1.8.1.2. Export authorizations.

1.8.1.3. Foreign Military Sales (FMS).

1.8.1.4. Foreign Government Information (FGI).

1.8.1.5. Technology Control Plans (TCPs).

1.8.1.6. Program/Project Security Instructions.

1.8.1.7. Foreign visitors as they relate to TCPs and access to classified.

1.8.1.8. Employees at overseas locations.

.

1.9.1. Physical security controls.

1.10.1. Special Programs.

1.11.1. Other special requirements imposed by the Government Contracting Agency(s) on the contractor.

1.12.1. Security Education and Counterintelligence Awareness.

1.12.2. FSO Training.

1.12.3. Self-Inspection Program.

1.13.1. Management support to security.

1.14.1. Natural Disaster/Emergency Preparedness Procedures.