



**DEFENSE SECURITY SERVICE  
PRIVACY IMPACT ASSESSMENT  
GUIDANCE AND TEMPLATE**

**Version 1.0  
28 October 2008**

# DSS PRIVACY IMPACT ASSESSMENT

For

## Industrial Security Facilities Database (ISFD)

<b>Project Identifying Information</b>	
<b>Name of Information Technology (IT) System:</b>	<i>Industrial Security Facilities Database (ISFD)</i>
<b>OMB Unique Project Identifier (if applicable) and OMB Information Collection Requirement Number/Expiration Date (if applicable)</b>	<i>007-97-01-16-02-2854-00</i>
<b>Budget System Identification Number (SNAP-IT Initiative Number):</b>	<i>2854</i>
<b>System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository):</b>	<i>7522</i>
<b>Privacy Act System of Record Number (if applicable):</b>	<i>NA</i>
<b>Qualifying Questions</b>	
<p>A Privacy Impact Assessment is required for all DSS projects with IT systems that maintain Personally Identifiable Information (PII) of at least ten individuals in the public, not counting members of the Armed Forces (to including Reserve and National Guard personnel) and DoD civilian employees (including non-appropriated fund employees).</p>	
<p><i>Yes, ISFD contains PII and requires PIA notice.</i></p>	
<p>If the answer is “yes”, you are required to complete the Privacy Impact Assessment by completing the remaining questions on this form.</p>	
<b>Privacy Impact Assessment Questions</b>	

1.	Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).
	<p><i><u>Activity/Purpose:</u> ISFD is a centralized web-enabled database application containing information related to facilities participating in the National Industrial Security Program (NISP). The application provides the main functionality for the Defense Security Services (DSS) Industrial Security Program (ISP) to perform daily tasks to issue and maintain industrial facility security clearances for the Department of Defense, to include tracking of facility clearance requests, allows authorized users to verify facility information and receive to receive notifications when select facility information is changed.</i></p> <p><i><u>Present Lifecycle Phase:</u> Operations and Sustainment</i></p> <p><i><u>System Owner:</u> DSS</i></p> <p><i><u>System Boundaries and Interconnections:</u> The ISFD hardware is located in the DSS Server room is located at Braddock Place in Alexandria, VA. The system allows remote access through Virtual Private Network (VPN, which also applies to our failover site in Monterey, CA.</i></p> <p><i><u>Location of System and Components:</u> Braddock Place, Alexandria, VA</i></p> <p><i><u>System Backup/Failover Site:</u> DMDC, Monterey, CA</i></p>
2.	Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).
	<p><i>Identifying information of Key Management Personnel (KMP) is captured in association to clear a facility. The KMPs, full name, Social Security Number (SSN), Date of Birth, City of Birth, State of Birth, Country of Birth, Country of Citizenship and Immigration Status are collect (as applicable). The Facility Security Officer (FSO), full name, Social Security Number (SSN), Date of Birth, City of Birth, State of Birth, Country of Birth, Country of Citizenship, Immigration Status, and phone number are collect (as applicable)</i></p> <p><i>The information is indexed according to the facility's Commercial and Government Entity (CAGE) code.</i></p>
3.	Describe how the information will be collected (e.g. via the Web, via paper-based collection, etc.).
	<p><i>ISFD is web-based and provides a Graphical User Interface (GUI) that allows DSS to enter the data associated with a facility participating in the NISP.</i></p>

4.	Describe the requirement and why the information in identifiable form is to be collected (e.g. to discharge a statutory mandate, to execute a Component program, etc.).
	<i>ISFD requires this information in accordance with clearing a facility.</i>

5.	Describe how the information in identifiable form will be used (e.g. to verify existing data, etc.).
	<i>The information is used to identify KMPs associated with a facility.</i>

6.	Describe whether the system derives or creates new data about individuals through aggregation.
	The system does not derive or create new data about individuals through aggregation

7.	Describe with whom the information in identifiable form will be shared, both internal to DSS and external to DSS (e.g. other DoD Components, Federal agencies, etc.).
	<p><b>Internal to DSS:</b>  <i>Anyone within the DSS who is an authorized user of ISFD may have access to this information. The primary user is the Industrial Security Program (ISP) for maintaining facility information of those facilities participating in the NISP. The DoD Security Services Center in Columbus Ohio and Alexandria Virginia has access to information for facility verification purposes.</i></p> <p><b>External to DSS:</b>  <i>Anyone who has a valid need to verify a facility clearance may be granted access to ISFD. The only PII information available to External Users is the Name of the FSO and their phone number.</i></p>

8.	Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.
Consent Question:	If an individuals object to the collection of their PII information the individual will be excluded from the role of KMP and excluded from accessing classified information.

9.	<p>Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.</p> <p><i>The PII information is provided in an electronic Facility Verification Notification which contains the FSO name and phone number. The data contained in ISFD consists of personnel data that is considered sensitive and is protected in accordance with the Privacy Act (5 U.S.C. Section 5.5.2a).</i></p>
10.	<p>Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.</p>
<b>Concise narrative answer:</b>	<p><i><u>Administrative:</u> The user must submit a System Access Request (SAR) to DSS. SARs requesting an internal role and the requester is assigned outside of the Industrial Security Program and must be approved by the ISP Director or the Deputy Director of the Policy Implementation Division.</i></p> <p><i><u>Physical:</u> All servers located at Braddock Place in Alexandria Virginia and DMDC, Monterey, CA are in a room with access controls.</i></p> <p><i><u>Technical:</u> ISFD uses secure hypertext transfer protocol (HTTPS). Unique user identification and individual password are issued to authorized system users. The system prompts the user to enter their ID and password at the beginning of each session. System users are assigned as an internal, external or administrative user role. The external role only allows the viewing of select ISFD data and the user cannot 'write' to the facility information (read only). The internal role and administrative user roles permit full access capability, to include 'write', to the entire facility record. Users are prompted to change their password every 60 days. When a user enters the wrong user id or password the account is locked after the third failed attempt: the user must then contact the DoD Security Call Center to have their account unlocked.</i></p>
11.	<p>Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11 "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed.</p>
	<p>Information in the system is not accessed by an individual's PII. The information is indexed and retrieved by the facility CAGE code, therefore, a Privacy Act System of Records Identifier is not required.</p>

12.	Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risk in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.
	<p>Any breach (loss, theft, or compromise) of Personally Identifiable Information (PII) (Social Security number, date of birth, etc.) from/on DSS systems must be reported using the following timelines: To the US-CERT within one (1) hour of discovery, and to the Senior DSS (Les Blake) Official for Privacy within 24 hours of discovery. The Senior Component Official for Privacy, or their designee, shall thereupon submit an incident report to the Defense Privacy Office within 48 hours of being notified that a PII breach has occurred.</p> <p>Individual Affect: If PII on a system is breached, the FSO of the affected facility is immediately contacted and advised of the compromise.</p>

13.	State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.
	<p><u>Classification</u>: <i>Sensitive But Unclassified</i></p> <p><u>Publication</u>: Yes: On the DSS Internet Web site (www.DSS.mil)</p>

14.	Provide additional comments about the system should you feel it necessary.
	None

**Project Manager:** Signed October 30, 2008  
ISFD PM

**Information Assurance Official:** Signed October 30, 2008  
DSS Senior Information Assurance Officer

**DSS Privacy Officer:** Signed October 30, 2008  
DSS Chief, FOIA/PA

**REVIEWING OFFICIAL:** Signed October 30, 2008  
DSS Chief Information Officer