



DEFENSE SECURITY SERVICE

**Personnel Security Investigative File Automated
Subsystem, to be known henceforth as the
improved Investigative Records Repository
(iIRR)**

PRIVACY IMPACT ASSESSMENT

November 20, 2008

VERSION 1.0

DSS PRIVACY IMPACT ASSESSMENT FOR iIRR

Project Identifying Information

Name of Information Technology (IT) System:	<i>Personnel Security Investigative File Automated Subsystem, to be known henceforth as the improved Investigative Records Repository (iIRR)</i>
OMB Unique Project Identifier (if applicable) and OMB Information Collection Requirement Number/Expiration Date (if applicable)	007-97-01-16-02-2880-00
Budget System Identification Number (SNAP-IT Initiative Number):	2880
System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository):	<i>(DSS DITPR) 9878</i>
Privacy Act System of Record Number (if applicable):	V5-01

Qualifying Questions

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).

Yes

If the answer is “yes”, you are required to complete the Privacy Impact Assessment by completing the remaining questions on this form.

Privacy Impact Assessment Questions

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).

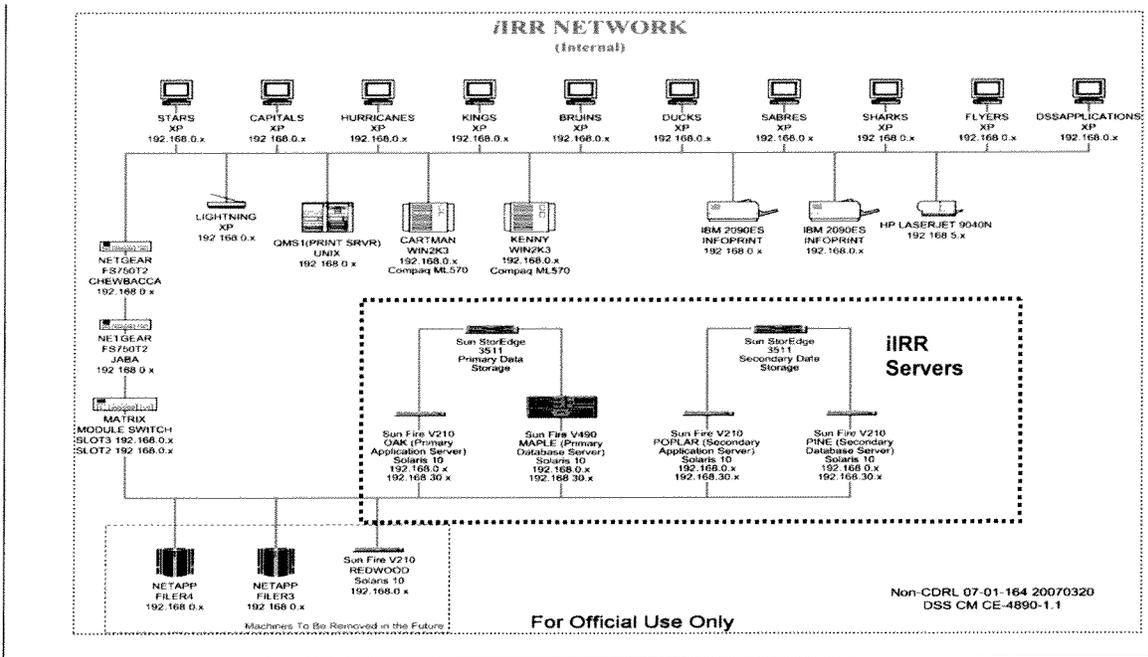
The improved Information Records Repository (iIRR) is a modern Information Technology (IT) system based on the application of industry best practices, and is

compliant with the Enterprise Security System (ESS) architectural practices. It provides its user community access to and retrieval of legacy investigative records in a fashion that optimizes operational and cost efficiency. Legacy investigative records are defined as the subject records of any personnel security investigation within the Case Control Management System – Information System (CCMS-IS) prior to its decommissioning on 3 February 2006. Legacy investigative records exist in four primary data formats:

- ◆ Electronically generated and stored subject investigative data used to maintain personal information, Electronic Personnel Security Questionnaire (EPSQ) form data, and the results of investigative lead results developed during the course of an investigation.
- ◆ Electronically scanned/maintained image documents and/or files collected during the investigative process.
- ◆ Microfiche containing investigative records with case dates of 1998 or older. (Records were previously being scanned and saved electronically. However, at this time there are still over 1,200,000 microfiche.)
- ◆ Hardcopy investigative records and supporting documents.

In the *i*IRR, authorized users collocated with the system request and/or retrieve the investigative records of the subject of a legacy personnel security investigation. In addition, these authorized users can manually copy electronically submitted batch requests to the *i*IRR. The *i*IRR processes these batch requests for investigative records using a format defined in its published Interface Control Document (ICD). Results of user requests and batch requests are generated by the *i*IRR. These results are returned to requestors via a number of delivery mechanisms outside of the scope of the *i*IRR based on the results of the records search. The data contained in these results is further described in Answer 2 below.

The *i*IRR system is currently operational and is maintained by the Defense Security Service (DSS) Clearance Liaison Office (CLO), which is responsible for delivering the services and work products produced by the *i*IRR. The system is entirely located at the Iron Mountain Facility in Boyers, Pennsylvania and has no interconnections with any other systems. See the diagram of the *i*IRR private network shown below. The system has two backup systems: a NetBackup storage unit and weekly system tape back up. The *i*IRR relies on redundant components to achieve system reliability. (Reference *i*IRR Concept of Operations, Section 1.3)



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.).

Currently, no information is collected by this system. However, iIRR still has the responsibility to safeguard and protect the information. The iIRR only retrieves from a repository legacy records previously collected by the CCMS system prior to 3 February 2006. The data consists of the records of investigations conducted by DSS and clearance actions taken for contractors. Information may include investigative assignment records, which may serve as the basis for the investigation, or which serve to guide and facilitate investigative activity; information used to open and conduct the investigation; records on the type of investigation, on the type and number of leads assigned to DSS field elements and leads sent to National Agencies for investigations in progress and the results of those leads received from the National Agencies. The system also identifies the legacy status of an investigative request (open/closed/) and the status of individual leads being conducted, to include additions to, deletion of or amendment to those leads. The system also consists of records pertaining to clearance information on contractors, which may include name, Social Security Number, gender, date of birth, place of birth, case number, date and level of security clearance granted, results of interim or final eligibility determinations, clearance applications, record of clearance, foreign clearance and travel information, clearance processing information, adverse information and other internal and external correspondence and administrative memoranda relative to the clearance. (Reference: CCMS System of Records Notice, V5-03)

<p>3. Describe how the information will be collected (e.g. via the Web, via paper-based collection, etc.).</p> <p>No information is collected by this system. The <i>i</i>IRR only retrieves legacy records stored within the <i>i</i>IRR that were previously collected by the CCMS system prior to 3 February 2006. (Reference <i>i</i>IRR Concept of Operations, Section 1.3)</p>
<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.).</p> <p>The information contained in the <i>i</i>IRR was collected by the CCMS system prior to 3 February 2006 under the authority for maintenance of the system as defined in 5 U.S.C. 301, Departmental Regulations; DoD Directive 5105.42, Defense Security Service (32 CFR part 361); DoD Regulation 5200.2, Personnel Security Program (32 CFR part 156); and E.O. 9397 (SSN). (Reference: Current CCMS System of Records Notice, V5-03)</p>
<p>5. Describe how the information in identifiable form will be used (e.g. to verify existing data, etc.).</p> <p>The <i>i</i>IRR data are used by various requestors (as listed in the answer to question 7 below) as follows:</p> <ol style="list-style-type: none"> 1. As supporting information for the adjudication of current personnel security clearance applications 2. As supporting information for the conduct of other investigations under the jurisdiction of the requesting Government agency 3. As a result of a Freedom of Information Act (FOIA) request from the general public through the requesting Government agency.
<p>6. Describe whether the system derives or creates new data about individuals through aggregation.</p> <p>The system does not derive or create any new data about individuals. It only provides for the retrieval of legacy records previously collected and aggregated by the CCMS system decommissioned on 3 February 2006. (Reference: <i>i</i>IRR Concept of Operation, Section 1.3)</p>
<p>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> <p>Information is disseminated from the <i>i</i>IRR site in hardcopy or on DVDs to the following offices or agencies: Internal to DSS:</p>

1. DSS Freedom of Information Office (FOIA)
2. DSS Privacy Act Office (PAO)
3. DSS Defense Industrial Security Clearance Office (DISCO)

External to DSS:

1. Military Service Adjudicators
2. Office of Personnel Management (OPM)
3. Other Government Agencies including the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), and the National Security Agency (NSA)

(Reference: *i*IRR Concept of Operations, Section 3.5)

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.

The legacy information provided by this system was originally collected from individuals on a voluntary basis in connection with their application for a security clearance through DSS. Individuals have signed consent forms.

Consent Question: “The security processing for this contract is voluntary. Should you desire to be considered, sign below.” (Reference: Form G6772 Rev Mar 04)

9. 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.

*i*IRR will not directly provide individuals with subject file information. *i*IRR requests for FOIA/PA information will require a written signed consent from the individual to whom the record pertains or if the document is being requested on behalf of a DOD agency for official purposes, a request in writing on agency letterhead with a statement on why the Agency requires the document and how it will be used. Those requests will be faxed to Leslie Blake, Chief – DSS FOIA/PA, at (703) 325-5991.

*i*IRR will provide DSS FOIA/PA with a hard copy of the requested information. FOIA/PA will review the files and forward them to the individual requester.

10. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

Concise narrative answer:

Administrative:

Before providing access to any *i*IRR capabilities or resources, a request must be submitted by the prospective *i*IRR user’s first line or higher-level

supervisor. The request must subsequently be approved by the Program Management Office (PMO). The process for accessing *i*IRR resources is characterized by the following:

- ◆ Any changes to be made to a user's access privileges will use the same formal request format as the original access request – a System Access Request (SAR).
- ◆ Membership in a shared directory will be approved by the directory owner. The list of users with access to the directory will be reviewed and approved by the directory owner, at least quarterly.
- ◆ Each user will be assigned a unique personal user identifier (USERID) and specific access privileges. Assignment of these attributes will facilitate auditing of individual activities on the system.
- ◆ The PMO for the *i*IRR production system, to which a new user will be assigned, is responsible for verifying the adequacy and authenticity of the new user's request before authorizing the creation of a new user account.
- ◆ Before a new user is granted access and provided a password for any *i*IRR component or capability, the new user will acknowledge in writing they have read and will abide by the *i*IRR Rules of Behavior.
- ◆ The user's need-to-know for access to the *i*IRR application(s) will be certified in writing by the user's first line or higher supervisor before access is granted.

(Reference: *i*IRR Rules of Behavior, Section 2.2)

Physical:

The *i*IRR system is located in a controlled facility at Iron Mountain in Boyers, Pennsylvania. The Iron Mountain facility employs 100 percent access control, staffed by 24-hour security personnel. The CLO facility is certified as a "Secure Room" and is authorized for open storage of completed, compiled personnel security investigations and classified information up the Secret level. The facility is protected by cipher locks and intrusion detection devices. The room in which the system is housed is designated as an internal "Controlled Area." An access control list to the computer room will be maintained by the Information Assurance Officer (IAO) and updated when necessary. (Reference: *i*IRR Concept of Operations, Section 5.3.4.2))

Direct access to the *i*IRR system hardware within the network security accreditation boundary is restricted to authorized personnel for the purpose of system maintenance. Other than system management personnel, all

individuals are escorted within the room that houses the iIRR servers. Removal or alteration of computer hardware without prior coordination with the iIRR IAO and Systems Administrator is strictly prohibited. (Reference: iIRR Information System Security Policy, Section 2.5)

Technical:

Each iIRR user is required to login to the system with a user name and password. The iIRR password policies are in accordance with the Joint Task Force (JTF)-Global Network Operations (GNO) Communications Tasking Order (CTO) 06-02. An audit trail is maintained for each dissemination of data from the iIRR identifying the requestor/receiver of the data, the identity of iIRR user who processed the request, and the time/date of the request and the response. (iIRR System Requirements Specification, Section 3.4)

11. 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.

System of Records Notice for the Personnel Security Investigative File Automation Subsystem (iIRR) has been published in the Federal Register and is located at <http://www.defenselink.mil/privacy/notices/dss/V5-01.html>.

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.

The *i*IRR is not involved in collecting any information. It only uses the data to perform the function of disseminating information to the requesting agencies listed in the answer to question 7 above. The risks associated with this dissemination are as follows:

1. Improper use or handling of the information by the *i*IRR authorized users at the system site. This risk is mitigated by the procedures required for user's to gain access to and use the system as described in the answer to question 10 above. This risk is also mitigated by the logging of user activity on the system. These logs are available for auditing to detect any unauthorized user activity. This risk is also mitigated by the rules of behavior enforced at the *i*IRR site. All *i*IRR users are required to sign a statement that they will adhere to these rules and all *i*IRR users are required to have a current TS/SSBI.
2. Dissemination of the information to improper requestors. All information dissemination is logged by the *i*IRR system. This log uniquely identifies both the *i*IRR user involved in the dissemination and the requestor/receiver of the information as described in the answer to question 10 above. This log is available for auditing to detect any improper user activity.
3. Compromise of the information during the dissemination process. Once the *i*IRR prints the output report or writes it to DVD, the dissemination to the requestors is done manually. The methods used include FEDEX, courier, and email. Mitigation of these risks is beyond the scope of the *i*IRR system.

The *i*IRR itself does not provide individuals any opportunity to object or consent to the dissemination of the information to the requesting agencies or any notification of such dissemination. Whether the requesting agency provides this type of interaction with the individuals is not known and is beyond the scope of the *i*IRR.

Further risks would involve unauthorized modifications to the software or hardware to compromise the security features inherent in the *i*IRR system. These risks are mitigated by all of the rules of behavior identified in the *i*IRR Rules of Behavior document. All *i*IRR users must sign a statement that they will adhere to these rules.

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.

Classification: Controlled Unclassified Information (Reference: iIRR Information System Security Policy, v1.4)

Publication: The PIA may be published since it does not contain any classified information and can be published in full form.

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

iIRR Project Manager: _____
Title: DSS PM

Signed

20 Nov 2008

Information Assurance Manager: _____
Title: DSS Information Assurance Manager

Signed

20 Nov 2008

Chief of PLCM: _____
Title: Chief of Project Lifecycle Management

Signed

20 Nov 2008

Senior Information Assurance Officer: _____
Title: DSS Senior Information Assurance Officer

Signed

20 Nov 2008

DSS Privacy Officer: _____
Title: DSS Chief, FOIA/PA

Signed

20 Nov 2008

REVIEWING OFFICIAL: _____
Title: DSS Chief Information Officer

Signed

20 Nov 2008