

Privacy Impact Assessment (PIA)

Name of Project: Integrated Siebel Platform GSS (ISE GSS)

Project's Unique ID: ISE/NISP

Legal Authority(ies):	Computer Security Act of 1987 (P.L. 100-235) Government Performance and Results Act of 1993 (GPRA) (P.L. 103-62) E-Government Act of 2002 (P.L. 107-347) Freedom of Information Act (5 U.S.C. § 552. as amended) Privacy Act of 1974 (5 U.S.C. § 552a) Clinger-Cohen Act of 1996 Office of Management and Budget (OMB) No. A-130 Health Insurance Portability and Accountability Act of 1996 (HIPAA) Federal Information System Management Act of 2002 (FISMA) Authority for Maintenance of the System: 44 U.S.C. 2108, 2110, and 2907.
------------------------------	--

Purpose of this System/Application: NARA has developed applications that assist the public, Federal agencies, and internal staff with locating, ordering, tracking, and managing the physical aspects of both agency owned and accessioned non-electronic records. NARA uses Oracle's Siebel Customer Relationship Management (CRM) framework as the base infrastructure for these applications and as the central vehicle for providing online customer service for access to and reproductions of its non-electronic records holdings.

Oracle Siebel CRM Framework:

The Oracle Siebel CRM framework consists of the following applications:

- a) Expanding NARA Online Services (ENOS):
 - Order Online!
 - Siebel Order Fulfillment Application (SOFA)
 - Siebel Content Management Application (SCMA)
- b) Archives Records Center Information System (ARCIS)
- c) Records Centers Program Billing System (RCPBS)
- d) Holdings Management System (HMS)
- e) Case Management and Reporting System (CMRS)

All of these applications reside on a shared Oracle Solaris Unix and Microsoft Windows platform with storage for the Siebel-based environment provided by a Storage Access Network (SAN). This shared environment along with the six CRM applications is referred to as the Integrated Siebel Environment (ISE)/NARA Integrated Siebel Program (NISP) GSS.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:		
Employees		The ISE GSS has no specific data elements, but serves as the common support platform for RCPBS, ARCIS, ENOS-HMS, and CMRS (i.e., sometimes referred to as NISP applications within this PIA). The data elements reside in the individual application and not on the ISE GSS.
External Users		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
Audit trail information (including employee log-in information)		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
Other (describe)		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?		
NARA operational records		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
External users		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
Employees		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
Other Federal agencies (list agency)		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
State and local agencies (list agency)		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
Other third party source		See the PIA for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.
Section 2: Why the Information is Being Collected		
1. Is each data element required for the business purpose of the system? Explain. Yes, however, the ISE GSS has no specific data elements, but serves as the common support platform for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.		
2. Is there another source for the data? Explain how that source is or is not used?		

The ISE GSS has no specific data elements, but serves as the common support platform for RCPBS, ARCIS, ENOS-HMS, and CMRS. The data elements reside in the individual application and not on the ISE GSS.

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

Yes, the new derived data elements will be part of either RCPBS, ARCIS, ENOS-HMS, and CMRS applications.

2. Will the new data be placed in the individual's record?

Yes, the new derived data elements will be part of either RCPBS, ARCIS, ENOS-HMS, and CMRS applications.

3. Can the system make determinations about employees/the public that would not be possible without the new data?

N/A

4. How will the new data be verified for relevance and accuracy?

The new derived data elements will be part of either RCPBS, ARCIS, ENOS-HMS, and CMRS applications.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

NARANet implements Microsoft Active Directory to manage access control, identification, authentication, and logging.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

All individual systems that are hosted on the ISE GSS require users to enter a unique username and password to gain access to the system.

7. Generally, how will the data be retrieved by the user?

For the systems that ISE GSS support, users retrieve data via web portal after logging into the application. Users only have access to data that has been authorized by a System Administrator, commensurate with the employees' official assigned duties as it pertains to that system. Once validated as an authorized user, users retrieve data using pre-built queries and reports defined within the application.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier?

If yes, explain and list the identifiers that will be used to retrieve information on an individual.

Data is retrievable from the systems that are supported by ISE GSS. There are various fields that are available in respective systems that allow data to be retrieved. Additional details can be found in the respective PIAs in Section 1a for NARA staff and contractors and 1 b for external users.

9. What kinds of reports can be produced on individuals? What will be the use of these reports?

Who will have access to them?

Systems supported by ISE GSS have the capability to produce a variety of reports such as:

- system usage
- access date
- access time
- transactions conducted
- information accessed

The ISE GSS primarily serves as the base infrastructure for these applications and as the central vehicle for providing online customer service for access to and reproductions of its non-electronic records holding.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

N/A

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.

ISE GSS supports individual systems that require identification and authentication with a unique username and password and monitoring that can be completed by the systems that ISE GSS support. The ISE GSS primarily serves as the base infrastructure for these applications and as the central vehicle for providing online customer service for access to and reproductions of its non-electronic records holding.

12. What kinds of information are collected as a function of the monitoring of individuals?

Collection of information as a function of the monitoring of individuals are completed at the system level. ISE GSS conducts monitoring for each of the NISP applications primarily to provide availability of user services.

13. What controls will be used to prevent unauthorized monitoring?

The Siebel COTS software being used has extensive security controls built into the core functionality of the system. Only authorized system administrators and application administrators have the authority to perform system monitoring. These individuals have the appropriate approvals before monitoring authority is granted.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

ISE GSS is not web-based and does not use persistent cookies. It is the Siebel platform that supports the NISP systems.

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

Each system has various types of users such contractors, internal and external users, system administrators, and developers.

At the NISP infrastructure level there are the following:

- Contractors employed by NARA to provide system administration for the NARA IT infrastructure that will ensure availability of user services.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?

Access is limited to the Operations and Maintenance (O&M) support team for ISE GSS applications. Standard NARA procedure is followed prior to granting anyone access to ISE GSS. User access is initiated by the completion of an access request form for the user. That form is reviewed and approved by the user's supervisor. Annually, all user accounts are reviewed for accuracy and updated as appropriate.

3. Will users have access to all data on the system or will the user's access be restricted?

Explain.

The principle of "least privilege" is employed and access is based on the role of personnel, so that individuals have access only to information necessary to do their job.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?

Access to the data is restricted (as mentioned above). Audit trail functionality is included to identify any unauthorized access. Contractors for ISE GSS are tasked with identifying, reporting, and correcting any conditions that may contribute to failure of user services.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, the Privacy Act contract clause is included.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.

Yes, however, the ISE GSS is a platform that support the system boundaries that engress and ingress PII data.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

Yes, the certification process is addressed under the SA&A certification for RCPBS, CMRS, ARCIS and ENOS-HMS and the PIAs for those systems.

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The ISE GSS System Owner is responsible for protecting the privacy rights of the public and employees affected by the interface. NARA's Senior Agency Official for Privacy is responsible for ensuring compliance with the privacy rights of the public and NARA employees.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

Yes, however, ISE GSS is only responsible for ensuring that the necessary patches are applied and the availability and avoid any failure to user services.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

The is not applicable at the ISE GSS level; however, the NISP systems are subject to the policies that have been put in place by NARA.

2. Does the system ensure “due process” by allowing affected parties to respond to any negative determination, prior to final action?

Not applicable.

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).

The NISP systems must adhere to the NARA standards for ensuring data accuracy, timeliness, and completeness. At the ISE GSS level, it is the responsibility of O&M to perform the following:

- Backup and Disaster Recovery
- Scheduled backups of the NISP applications and devices
- Performance Monitoring and Reporting on the hardware and software components within the NISP
- Monitor the servers, at a minimum, for disk utilization, CPU usage, critical errors, connectivity, and nightly backup status
- Identify, report, and correct any conditions that may contribute to failure of user services

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

While the platform is accessible from more than one site, the system itself is only in one location.

3. What are the retention periods of data in this system?

The ISE GSS is responsible for performing scheduled backups of the NISP application and devices with the intent of having recoverable systems, data, and services. These backups are disposed or rewritten every 30 days.

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

The NISP applications have disposition procedures documented in various operational manuals and must adhere to policies set forth by NARA.

At the ISE GSS level, O&M personnel are tasked with performing functions to ensure the overall integrity of NISP data as defined in NARA Files Maintenance and Records Disposition Manual (FILES 203) and the NARA Records Schedule.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

No.

6. How does the use of this technology affect public/employee privacy?

N/A

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?

Yes. All systems must undergo an assessment and authorization in order to obtain an authorization to operate (ATO) and meet the requirements of FISMA. This system was granted an ATO on July 13, 2009, and is under continuous monitoring.

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?

Yes. All risks identified go through the plan of action and milestone (POA&M) process until remediation. In addition, as part of the continuous monitoring at NARA, there are various activities that are conducted (e.g., scans, self-assessments, etc) to ensure risk surface is minimized and kept under control.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

NARA standard Assessment and Authorization (A&A) is completed every three (3) years to recertify that the system is authorized to operate.

10. Identify a point of contact for any additional questions from users regarding the security of the system.

Questions regarding the security of this system may be addressed to Edward Graham (IT PM) and Timothy Rhodes (COR).

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

NARA 35 covers the CMRS component system.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain. N/A

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

No, there were no pertinent issues that arose during the drafting of this assessment.

2. If so, what changes were made to the system/application to compensate?

N/A

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA

System Manager (Project Manager)



(Signature)

8/7/18

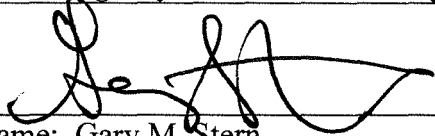
(Date)

Name: David Weinberg

Title: Director, Federal Records Center Program

Contact information: 301-837-3115

Senior Agency Official for Privacy (or designee)



(Signature)

8/1/18

(Date)

Name: Gary M. Stern

Title: General Counsel

Contact information: 301-837-1750

Chief Information Officer (or designee)



(Signature)

8/10/18

(Date)

Name: Swarnali Halder

Title: Chief Information Officer

Contact information: 301-837-1583