DEPARTMENT OF TREASURY
Washington, D.C. 20220

Departmental Offices Local Area Network (DO LAN)
General Support System (GSS)
Privacy Impact Assessment (PIA)

December 04, 2007

A. Identification

System Name:	Departmental Offices, Local Area Network (DO LAN)
OMB Unique Identifier:	015-00-02-00-01-1070-00-404-140
System Owner:	Office of the Chief Information Officer (OCIO) Director, Headquarters Information Technology

Contact	Director, Disclosure Services:	Hugh Gilmore
	Privacy Act Officer:	Dale Underwood

Address: FOIA/PA Request
Disclosure Services
Department of the Treasury
Washington, D.C. 20220

Telephone: (202) 622-0930
Fax: (202) 622-3895

B. Scope

The scope of this Privacy Impact Assessment includes the Departmental Offices Local Area Network (DO LAN) general support system (GSS) and its computing resources to include minor applications that reside on the DO LAN. The scope of this PIA does not include Treasury or Departmental Offices Major Applications that may reside on the DO LAN. This assessment is limited to the data stored and processed on the GSS and the minor applications that reside within the security controls of the DO LAN.

C. System / Application General Information

The DO LAN supports the general computer office automation and information processing needs of the personnel of the Departmental Offices. As such it is referred to as a General Support System (GSS).

1. Does the system contain any information in identifiable form (IIF)?

   Yes

2. What is the purpose of the system / application?

   The purpose of the DO LAN is to provide the backbone network and general purpose office automation systems for the processing, storing, and transmission information in support of the mission of US Treasury Departmental Offices. Office automation functions include file services, network printing, electronic mail and collaboration, internet access, and word processing. The DO LAN also provides infrastructure for the development and operation of minor business applications that support the Departmental Offices mission.

3. What legal authority authorizes the purchase or development of this application / system?

   The DO LAN is included in the Capital Planning and Investment Control (CPIC) Office of Management and Budget (OMB) 300 titled "Treasury-wide Integrated IT Infrastructure". This program identifies and takes advantage of opportunities to apply common infrastructure solutions across the Department, to achieve economies of scale through Treasury's collective buying power, and to enhance IT governance, delivery and service.

   http://www.treas.gov/exhibit300/docs/FY2008_TreasuryITSuperPortfolio_AllBureaus.pdf

4. Under which Privacy Act System of Record Notice (SORN) does this system operate?

   Treasury .003, Treasury Child Care Tuition Assistance Records
   Treasury .004, Freedom of Information Act/Privacy Act Request Records
   Treasury .005, Public Transportation Incentive Program Records
   Treasury .006, Parking and Carpool Program Records
   Treasury .007, Personnel Security System
   Treasury .008, Treasury Emergency Management System
   http://www.treas.gov/foia/privacy/issuances/treasurypa.html

   DO .003, Law Enforcement Retirement Claims Records
   DO .007, General Correspondence Files
   DO .010, Office of Domestic Finance, Actuarial Valuation System
   DO .015, Political Appointee Files
   DO .144, General Counsel Litigation Referral and Reporting System
   DO .193, Employee Locator and Automated Directory System
   DO .194, Circulation System

http://www.treas.gov/foia/privacy/issuances/dopa.html

D. Data in the System

1. What categories of individuals are covered in the system?

   As a general support system (GSS) that provides infrastructure to support the mission of the Departmental Offices it associated applications, the following types of categories of individuals may exist in the GSS:

   Employee and Contractor

2. What are the sources of the information in the system?

   The information that is processed, stored and transmitted on the DO LAN to support the Departmental Offices mission maps to the following NIST SP 800-60 information categories:
   - *Administrative Management*
   - *Financial Management*
   - *General Government*
   - *Human Resources*
   - *Information and Technology Management*
   - *Knowledge Creation and Management*
   - *Legislative Relations*
   - *Litigation and Judicial Activities*
   - *Planning and Resource Allocation*
   - *Public Affairs*
   - *Regulatory Development*
   - *Revenue Collection*
   - *Supply Chain Management*
   - *International Affairs and Commerce*

   a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

      Refer to the System of Record Notices (SORN) listed in section C.4 for information sources.

   b. What Federal agencies are providing data for use in the system?

      Refer to the System of Record Notices (SORN) listed in section C.4 for other Federal Agencies that provide data for use in the System of Records that reside on the DO LAN GSS.

c. What State and/or Local agencies are providing data for use in the system?

None

d. From what other third party sources will data be collected?

None

e. What information will be collected from the employees, government contractors and consultants, and the public?

Refer to the System of Record Notices (SORN) listed in section C.4 for information that is collected.

3. Accuracy, Timeliness, and Reliability
   a. How will data collected from sources other than Treasury records be verified for accuracy?

For data collected from sources described in the SORNs listed in section C.4 which are other than Treasury records, each system owner implements processes and procedures for data verification and accuracy specific to the system and its purpose.

b. How will data be checked for completeness?

For data collected from sources described in the SORNs listed in section C.4 which are other than Treasury records, each system owner implements processes and procedures for data completeness examination specific to the system and its purpose.

c. Is the data current?

For data collected from sources described in the SORNs listed in section C.4 which are other than Treasury records, each system owner implements processes and procedures to ensure the data is as current as required to meet the purposes of the system.

d. What steps or procedures are taken to ensure the data is current and not out-of-date?

Steps and procedures are specific to the minor applications that reside on the DO LAN. Refer to C.4 SORNs.

e. Are the data elements described in detail and documented?

Yes, the Department of the Treasury has documented its Information Systems Life Cycle (ISLC) methodology which includes specification for documentation of system and data design. This information has been documented for the DO LAN and the minor applications which reside on the infrastructure.

E. Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is designed?

   The DO LAN as a general support system provides infrastructure to support user productivity and services for minor applications that support Departmental Offices functions. Refer to section C.4 SORNs for specific information regarding the data which is collected and associated purposes for data on the DO LAN.

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

   No

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

   Not Applicable

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

   No

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

   Not Applicable

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

   Data is not being consolidated.

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

   Not Applicable

8. How will the data be retrieved? Does the personal identifier retrieve data? If yes, explain and list the identifiers that can be used to retrieve information on the individual.

   Refer to section C.4 for individual SORNs regarding data retrievability.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

   Refer to section C.4 for individual SORNs and the associated reports that may be produced by these systems. All Treasury systems and personnel must comply with Treasury IT Security Policy TD 85-01 and Treasury physical, personnel and information security policy TD 15-71 which govern policy regarding information access and sharing.

F. Maintenance and Administrative Controls

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

   The DO LAN is a network system installed in a campus type environment in the DC downtown area. The DO LAN is replicated at the DO disaster recovery site The DO LAN Configuration Change Board (CCB) monitors and approves changes to both the primary and disaster recovery sites.

   Data maintained on the DO LAN is replicated in near real time to the disaster recovery site to ensure consistent use. The system can be maintained through personnel located at the primary and disaster recovery sites. Additionally, the systems can be remotely managed through a VPN connection from a Treasury contractor facility.

2. What are the retention periods of the data in the system?

   Refer to the SORNs listed in section C.4.

3. 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?

   Refer to the SORNS listed in section C.4

4. Is the system using technologies in ways that Treasury has not previously employed (e.g., monitoring software, smart cards, caller-ID)?

   No

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

   Not Applicable

6. Will this system provide the capability to identify, locate, and monitor individuals?

   The system implements security auditing of user access to the system and to network resources.

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

   The system audit trail tracks the user identification number, date and time of security event, and the security event. Treasury policy TDP 85-01 defines the security events which must be audited by Treasury information systems which are based on NIST SP 800-53.

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

   The DO LAN security plan is based on NIST SP 800-53. NIST SP 800-53 specifies security controls associated with access control and auditing. The DO LAN must meet Department of Treasury policy for certification and accreditation of these security controls as well as continuous monitoring of the controls for continued compliance with the security plan.

9. Under which Privacy Act SORN does the system operate?

   Refer to section C.4.

10. If the system is being modified, will the Privacy Act SORN require amendment or revision?

    Not Applicable.

G. Access to Data

1. Who will have access to the data in the system?

   Users are granted access to the system based on need. Users comprise Treasury employees, other government agency personnel, and contractors.

2. How is access to the data by a user determined?

Access to data is determined based on the individual's need and office affiliation. This need and office is determined by their supervisor and/or contracting officer technical representative, in the case of contractors, and must also be approved by the DO LAN system owner.

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

   The policy of least privilege is implemented which restricts users to only the information needed to perform their duties. This is performed using a group-based access control system complemented with need to know controls.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

   The DO LAN is categorized as a FIPS PUB 199 HIGH system. As such, the HIGH baseline for NIST SP 800-53 has been implemented and tested. These security controls ensure that users are not granted access to information. A DO LAN Rules of Behavior communicates responsibilities to all users of the systems. Users must sign and acknowledge these responsibilities. Finally, auditing and intrusion detection is used to detect any attempts to circumvent these security controls.

5. Are contractors involved with the design and development of the system and will / are contractors involved with maintenance of the system?

   Yes

6. Do other systems share data or have access to the data in the system? If so, explain.

   Not on a routine basis. Data may be shared under Court order. Outside experts and others, including individuals at other Government agencies must either sign confidentiality agreements before receiving such data or be allowed such access as part of a legitimate law enforcement activity. Additionally, information may also be shared when required by law for compliance with the Freedom of Information Act (FOIA) requests. In these cases, individually identifiable information is redacted according to FOIA policy and procedures.

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

   The DO LAN Information Owner, DO LAN Authorizing Official, and the DO Privacy Act Officer.

8. Will other agencies share data or have access to the data in this system (e.g., Federal, State, Local, other)?

   None

9. How will the data be used by the other agency(s)?

   Not Applicable

10. Who is responsible for assuring proper use of the data?

    Not Applicable