U. S. Department of Commerce
National Oceanic and Atmospheric Administration
Integrated Program Office

IPO LAN SYSTEM
NOAA 5017

PRIVACY IMPACT ASSESSMENT

June 2009

Prepared by: KELVIN L. MOORE, INFORMATION ASSURANCE MANAGER
Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

NESDIS Integrated Program Office Local Area Network

Unique Project Identifier: 006-00-02-00-02-0000-00 (NOAA NESDIS Infrastructure)

IT Security System: NOAA 5017 (NESDIS IPO Local Area Network)

System Description:

The Integrated Program Office (IPO) system is an administrative LAN. The IPO was established on 3 October 1994 to meet the congressional mandate of converging U.S. civilian and defense polar-orbiting satellite programs. The IPO organizationally resides within NOAA's National Environmental Satellite, Data, and Information Service (NESDIS). The IPO is staffed with personnel from the Department of Defense (DoD), Department of Commerce (DOC), and the National Aeronautics and Space Administration (NASA). The DOC, through NOAA, has overall responsibility for the program and for satellite operations. The DoD, through the Air Force, has the primary responsibility to acquire and support the converged satellites. NASA has responsibility for facilitating development and insertion of new cost-effective technologies that may enhance the ability of the converged system to meet its operational requirements.

The National Polar-orbiting Operational Environmental Satellite System (NPOESS) will use these satellites to monitor global environmental conditions and collect and disseminate data related to weather, atmosphere, oceans, land, and near-space environment.

The purpose of the IPO is to facilitate and allow the various civilian and defense organization to communicate effectively, share data, and maintain control of the satellite system.

The IPO Administrative LAN supports this purpose by providing IT resources to IPO personnel for purchasing, logistics, facility management, inventory, general management functions, office automation, payroll, human resources, and contract administration support.

This PIA has been developed to comply with the requirement in Section 208 of the E-Government Act of 2002 (44 U.S.C. 36) and the Department of Commerce IT Privacy Policy.

1. What information is to be collected (e.g., nature and source)?

Personally identifiable information (PII) collected or stored on the IPO LAN System is limited to: name, address, phone, e-mail address, organization name, organization address, position description, payroll, and performance evaluations.

2. Why is the information being collected (e.g., to determine eligibility)?

In most cases the information is being collected to provide a method of contacting office personnel in case of emergencies and providing supplemental information pertaining to

IPO personnel actions, pay issues, performance evaluations, and budgetary items for divisions within the IPO.

3. What is the intended use of the information (e.g., to verify existing data)?

The information is stored within the IPO LAN System for archival and historical purposes.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

This information is never made available to other Agencies or the public. The information is accessed only by those personnel that have a "need-to-know" requirement in order to perform their mission to the organization.

5. 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 may individuals grant consent?

Personally identifiable information is required in order to administratively support the staff members that support the IPO's mission. Explanation and links to the NOAA privacy policy are provided. No additional options are needed or given.

6. How will the information be secured (e.g., administrative and technological controls)?

Annual security awareness training with a section on data privacy is mandatory for all IPO employees and contractors. Training includes a section on Privacy Act information.

The physical IPO LAN System is protected from access outside of NOAA and outside of the NOS by a system of firewalls and routers. Whenever feasible, applications are hosted within the internally protected network to limit access to NOAA personnel only.

Users authenticate using a unique login ID and password to the Windows 2003 AD Domain Controllers. Once authenticated, the user's credentials/tokens are then used to map to shared drives and to the user's network home directory on the File Sharing server. Users now have access to administrative, budget and scientific data necessary to carry out their respective job functions.

An internal secure Web–database application for personnel and asset information is hosted on the Human Resources server using role-based access rules.

A Security Certification and Accreditation (C&A) in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) for this system is in force. The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years.

Data log extract and verify requirement:

The IPO LAN system generates audit records for the following events: **Successful login, failed login, logout, policy/configuration Change, Account management, object access, system events, directory services, and process tracking**. The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail. The information system provides the capability to manage the selection of events to be audited by individual components of the system. Debugging captures all events generated by the firewall**.**

The IPO LAN IT Security System Owner (ISSO) reviews/analyzes weekly the audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. The IPO IT Security Staff organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. The IPO IT Security Staff also employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: **Abnormal traffic, security signatures violations, and security permission violations**.

The IPO LAN System retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated.

Audit files are backed up as part of the IPO LAN backup procedures. Tapes are stored off-site for one year. The tapes are than returned to the IPO LAN and destroyed according to IPO's media sanitization and disposal procedures.

The logging software and SIEM provide a monitoring console that is monitored through dedicated network and security operation monitors systems. E-mail notifications are configured based on the correlation engine and/or criticality of the event log. In addition, System Administrators review the event logs as defined in their operating procedures.

The IPO ISSO reviews all Audit Logs via automated and manual procedures to verify and track extracts (if applicable) of the log files for investigative purposes. These reviews are conducted on a weekly basis.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?
No. The existing Privacy Act system of records notice (SORN) for NOAA-11, NOAA Mailing Lists applies to most of the personal information in this system. Other SORNs that apply include:

- DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
- DEPT-5, Freedom of Information and Privacy Request Records
- DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies
- DEPT-20, Biographical Files

8. Are these records covered by an approved records control schedule?

The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. In accordance with GRS 20, item 3, the data is presently being retained indefinitely.

System Contact:
Kelvin L. Moore
Information System Security Officer
(301) 713-4713
kelvin.moore@noaa.gov