# NASA Security Procedure Requirement (NSPR-1600-1)

## Office of Security and Program Protection

Effective: January 19, 2007
NRW 1400-4
NM 1600-46
NPR 1600.1

## Security Identification System Requirements

## 1. Purpose

This requirements document establishes Agency-wide policy for the issuance of, and access to the Universal Uniform Personal Identification Code (UUPIC).

## 2. Scope

The requirements identified within this document cover all information technology systems and applications that either request or use a UUPIC number.

## 3. Applicability

This policy applies to all NASA facilities, employees, contractors, recipients of NASA grants and cooperative agreements, partners and visitors, where appropriate, in achieving NASA missions, programs, projects, and institutional requirements.

## 4. Authority:

a. 42 U.S.C. § 2473(c)(1), Section 203(c)(1) of the National Aeronautics and Space Act of 1958 amended
b. 44 U.S.C. § 3541 et seq., Federal Information Security Management Act (FISMA) of 2002.
c. 40 U.S.C. § 11331, the Computer Security Act
d. E-Government Act of 2002, Public Law 347-107

## 5. Responsibilities:

The Assistant Administrator, Office of Security and Program Protection (OSPP) is the system owner of the UUPIC system, and is responsible for ensuring the proper functioning, assignment, use and protection of the UUPIC database.

Working in concert with the Office of the Chief Information Officer (OCIO), OSPP will ensure that access to the UUPIC system is properly documented and that Service Level Agreements (SLA) or Memoranda of Understanding (MOU) detailing the purpose and authority for accessing the UUPIC system are in place before granting system access.

## 5.1 Discussion

To enhance employee privacy, while ensuring positive identification throughout NASA information technology systems, NASA has created the Universal Uniform Personal Identification Code (UUPIC) as a replacement for the Social Security Number (SSN). The Office of Security and Program Protection (OSPP) has the chartered responsibility for personnel security, which includes administrative identity management in the UUPIC system. UUPIC numbers play an important role in IT account management, as well as synchronizing and replicating data across Agency wide and Center applications. The authoritative source for identity is spread between Personnel and the Physical Security Office as well as other sources, and is a separate issue from the SSN replacement effort.

The vast majority of individuals working with NASA pass through the Physical Security Offices at a NASA facility; however, individuals working with NASA computer systems receive accounts and cyber access to resources and may never physically access a NASA facility. Therefore, the requirement for UUPIC extends to the account management process that will be centrally managed, but with distributed administration.

The UUPIC population includes NASA civil service employees, contractor, visitors and partners who access NASA facilities and information technology (IT) resources. The UUPIC system will generate UUPIC numbers to aid in the positive identification of these individuals across NASA IT systems. At a minimum, the UUPIC system must be supplied with the first, middle, and last name, SSN, and date of birth of the individual being assigned a UUPIC number. The UUPIC database stores UUPIC numbers internally along with the minimum seed data to uniquely associate the UUPIC with one person. The UUPIC number is then provided to a NASA Identification Management System to enable a common data point across NASA IT systems, eliminating their use of the SSN. To insure that a UUPIC number will never be reused, once a UUPIC number is generated, it will permanently remain in the system.

## 5.2 System Description and Functional Requirements

The system description and functional requirements of the UUPIC system are contained within the UUPIC System Requirements document dated March 13, 2003 (see Appendix A).

## 5.3 Approval to Access the UUPIC System

To accomplish the objective of replacing the Social Security Number (SSN) and to better safeguard the electronic identity information on NASA employees, contractors, partners and visitors, where appropriate, systems within NASA may require access to the UUPIC database to insure the proper identification of individuals accessing NASA facilities and IT resources. Before any system access can occur, each system owner must execute a Service Level Agreement (SLA) or Memoranda of Understanding (MOU) with OSPP. At a minimum, the SLA/MOU must provide information that details the purpose for accessing the UUPIC system, and provide information that reflects the IT security plan number assigned to the system requiring UUPIC system access.

The system owner requiring access to the UUPIC system must submit a signed SLA/MOU to the Common Badge Access Control System (CBACS) Configuration Control Board (CCB). The CBACS CCB will work with the system owner to ensure proper documentation, and authority to access the UUPIC system. On behalf of the AA/OSPP, the CBACS CCB will approve/disapprove UUPIC system access.

In the event of a denial for UUPIC access, the requesting system owner may appeal by sending a letter, along with the SLA/MOU, to OSPP and OCIO. OSPP and OCIO will respond a final decision within 60-days of receipt of the appeal.

## 5.4 Use of the UUPIC

As discussed above, the UUPIC will serve as a replacement for the Social Security Number by providing a unique identifier that can serve as a data point across NASA information systems. Therefore, the UUPIC may not be used as a login identifier or user account name for any information systems, databases, web site, et al. With the exception of account initiation in the Identity Management System, use of the UUPIC for any identification purposes outside those needed for positive identification of individuals across and only within information systems is prohibited without the consent of the CBACS CCB. The UUPIC may never be posted on any Internet accessible web site. Any deviation from this policy must be coordinated with OSPP through OCIO in advance.

## 5.5 Initiation of UUPIC Issuance

UUPICs will only be issued through the population of seed data (name, Social Security Number (or in the case of a foreign national without a Social Security Number, the NASA Foreign National Management System (NFNMS) visitor number) and date of birth) into the UUPIC database. This information is required for all NASA civilians, contractors, partners, and virtual IT system users. Any request for a UUPIC will be initiated via an approved work flow method. The UUPIC database will auto-populate the IdM, IDMS and CBACS upon returning a UUPIC number.

## 6 Point of Contact

The Director, Security Management Division is the OSPP point of contact concerning this UUPIC policy. The DSMD can be reached at 202-358-2010.

/S/
David A. Saleeba
Assistant Administrator
Office of Security and Program Protection

# Universal Uniform Personal Identification Code (UUPIC)

## Systems Requirements

Frank E Martin 03/13/03

Code X

Paul A Strassmann 03|13|03

Code AO

## UUPIC Requirements

### 1.1 Background

The need to place a unique identifier termed the Universal Uniform Personal Identification Code (UUPIC) within the Travel Manager (TM) became apparent when the use of the Social Security Number (SSN) was found to be counter to existing Privacy laws and regulations. In TM the SSN is being used as an employee ID and is being displayed to individuals, such as document preparers and approving officials, who do not have a need to know individuals SSN.

The NASA Office of the CIO (Code AO) has been charged to come up with an appropriate UUPIC that would cover the entire range of personnel from Civil Servants to Contractors to Temporary Visitors and other NASA affiliates.

The requirement for a replacement for the SSN and to better safeguard the electronic identity information on NASA employees, Contractors and partners is separate from the issue of who is the authoritative source for the data, which is actually spread between Personnel and the Physical Security Office as well as other sources. The place were the majority of people pass through is the physical Security Offices at each Center but there are people that work with NASA and our computer systems that receive accounts and cyber access to our facilities that may never enter a NASA Center. The requirement for UUPIC extends to Code-X and to the account management process that will be centrally managed with a distributed administration (NISSU), Code-AO.

The Office of Security Management and Safeguards (Code X) has the chartered responsibility for personnel security, which includes administrative identity management. (NPD 1600.2)

UUPIC numbers will play an important role in IT account management as well as synchronizing and replicating data across Agency wide and Center applications

### 1.2 System Description

The UUPIC system will generate UUPIC numbers to aid in the identification of personnel. The UUPIC numbers are stored internally along with their first, middle and last names, and other information necessary to uniquely associate the UUPIC with a person. Once an ID is generated, it will never be removed from the system to ensure the ID is not reused. Individual personnel data may be removed from a record according to record retention schedules, which vary from date of last use of 5 years for visitors to 50 years for personnel with classified status.

## 2.0 System Requirements

### 2.1 User Operational Description and System Objectives

Generation of UUPIC numbers will be accomplished in two manners. Initially, UUPIC numbers for NASA Civil Servants will be generated off a flat file from NPPS. An output file will be generated by the UUPIC system that contains a UUPIC number for each NPPS entry.

Additionally, a web based user interface is required to assign UUPIC numbers to new visitors and other personnel including NASA's research and industry partners.

## 2.2 Functional Requirements

The following list describes the UUPIC requirements.

1 Characteristics of the UUPIC number

   a. The UUPIC number will be a 9 digit numerical code without any significance as to the characteristics of the Individual, i.e., civil servant, contractor or partner.

   b. The UUPIC will be displayed as 3 x 3 x 3 number so as not to be confused with a social security number.

   c. The UUPIC number will not be subject to reverse engineering based on other data contained within the UUPIC application.

2. Characteristics of the UUPIC Application

   a. UUPIC numbers will be issued in random sequence, consistent with NASA policy.

   b. The UUPIC application shall retain the minimal state data needed to create a new UUPIC number and match input data to an existing UUPIC number.

   c. The UUPIC application will be accessible through a standard API for programmatic UUPIC number assignment.

   d UUPIC numbers will be issued only once, UUPIC numbers that have expired shall not be reissued to another user.

   e. Data formats that can be supported include but are not limited to flat file, XML, LDIF, or SQL statements.

   f. An administrative interface shall be provided to the UUPIC application for error correction purposes.

   g. An electronic audit trail of changes will be maintained.

   h. A continuity of operations plan shall be established for the UUPIC system.

3. Because the UUPIC number represents a person, the number must be correlated with personal information.

   a. The reliable assignment of the UUPIC to persons shall be by the use of at least two unique attributes, in addition to name attributes, from the documents as specified in the Department of Justice Form I-9, Employment Verification Data.

b. Date of birth is always a required attribute, and when available SSN shall be a required attribute.

c. When SSN is not available, as in the case of foreign nationals, then another attribute will be used as described.

4. Because UUPIC will contain privacy act information, the systems have a high confidentiality, integrity, and reliability requirement.

   a. The system will be protected using physical security procedures, firewalls, encryption techniques, and strong authentication.

   b. Administrative access to UUPIC will be controlled using two-factor authentication.

   c. There shall be no user level access to UUPIC system or database.

   d. The agency directory will serve as the UUPIC repository for general access to the UUPIC number.

   e. Access to the UUPIC system by other applications shall be strictly controlled

5. Initial UUPIC generation process

   a. NPPS data will be used to initially generate civil servant information. For each civil servant an UUPIC will be generated.

   b. The process for generating contractor UUPICs will be similar to the NPPS process using information from each centers badge database and other appropriate contractor identification databases.

6. Methods to assign UUPIC numbers during unplanned system and network outages will be developed.