# COMPUTER ACCESS CLEARANCE/SECURITY FORM

**EMPLOYEE INFORMATION:**

**Request Type**: ☐ New Account ☐ Existing Employee (select one option below)

☐ Update Name/Title/Phone ☐ Update Profile

Previous/Prior Name (if applicable)

(Name should be the same as on the SF 52 – Please Print)

| **LAST Name:** | **FIRST Name:** | **MIDDLE Initial:** |
|---|---|---|
| DOE | JANE | A. |

**Official Title**: **Federal Supervisor/Point-of-Contact**:

**Region/Department/Office Name**:

**Mail/Office Code**: **Phone Number with extension** (if applicable):

**Status** (check one): ☐ Permanent ☐ Temporary ☐ Term ☐ Intern ☐ Volunteer

☐ Contractor On-Site ☐ Contractor Offsite

**Start Date**: **Office File Server Name**:

**Complete SBA Mailing Address**:

**FOR CONTRACTOR PERSONNEL ONLY:**

**Company Name and Address**:

**Contract Number**:

**Contract Expiration Date:**

**Contracting Officer Representative (COR) name and phone number**:

**Contract Company Program Manager/POC name and phone number**:

# COMPUTER ACCESS CLEARANCE/SECURITY FORM (cont.)

## DATA SECURITY REQUIREMENTS:

Some of the data maintained on SBA's network contain sensitive and Personally Identifiable Information (PII) that is subject to the provisions of the Privacy Act of 1974 as amended, and SBA SOP 40 04 3 "Privacy Act Procedures". In addition, users accessing SBA's information systems and applications are responsible for complying with the following security requirements:

a. Data retrieved from SBA's network may be disclosed only in accordance with SBA SOP 40 04 011, "Release of Information."

b. Passwords/Security codes for access to SBA's network shall not be shared, disclosed or transferred.

c. Contractors will not remotely access SBA's network without written approval from the Office of Chief Information Officer, the Chief Information Security Officer or without the use of Agency approved secure technology required for remote access.

d. Users may access only that data for which they have been authorized by the approving official and agree to follow all SBA procedures and policies pertaining to safeguarding sensitive and PII in hard copy and electronic format.

e. Failure to follow these security procedures may constitute a formal security violation under SBA regulations and may result in an investigation by the Office of Inspector General. (See SOP 90 47 3 for security violation penalties).

f. Users will be responsible for completing Computer Security Awareness Training (CSAT) upon initial network access; rules of behavior will be acknowledged during this training.

| **Account Requirements** (Completed by Program Office) | | **Expiration Date** (Determined by OHRS/OIG/COR/ITSC) | |
|---|---|---|---|
| LAN/WAN: | _____ | (Expiration Date: | _____) |
| EXCHANGE (Email): | _____ | (Expiration Date: | _____) |
| VPN ACCOUNT: | _____ | (Expiration Date: | _____) |
| OTHER (Mobile Device, etc.): | _____ | (Expiration Date: | _____) |

****Expiration date will be determined by person creating account. Temporary and term employees' accounts shall not exceed 12 months and permanent government employees' accounts shall not exceed 3 years.**

For access to GLS, Sybase, Mainframe Systems, JAAMS, other applications and information systems and Virtual Private Network (VPN) access for teleworkers, fill out templates located on the IT Security portal.

## ACCESS APPROVAL:

The above named individual is authorized to access data associated with the listed projects.

**Office of Human Resources Solutions (Workforce Acquisitions Division)** - SBA employees only or **Office of Inspector General – Human Resources** (IG personnel only)

SIGNATURE: _____ DATE: _____

**Office of Human Resources Solutions (Suitability/Security Division)** or **Office of Inspector General – Office of Security Operations** (IG personnel only)

**RECOMMEND APPROVAL** (based on required preliminary background screening)

SIGNATURE: _____ DATE: _____

**Office of the Chief Information Officer (OCIO)**

SIGNATURE: _____ DATE: _____