Description of document: Three (3) United States African Development Foundation (USADF) documents:

- USADF Security Assessment Plan (SAP) Synopsis, 2019
- USADF IT Security Implementation Handbook Table Of Contents, 2019
- MS-460 – ADF IT Security Policies and Procedures, 2012

Requested date: 01-April-2019

Release date: 14-May-2019

Posted date: 09-September-2019

Source of document:
FOIA Officer
U.S. African Development Foundation
1400 I Street NW
Suite 1000
Washington, D.C. 20005

From: Nina-Belle Mbayu <NBMbayu@usadf.gov>
Cc: June Brown <jbrown@usadf.gov>
Sent: Tue, May 14, 2019 1:55 pm
Subject: USADF FOIA 19-02 Appeal Response
Via Email

May 14, 2019

RE: USADF FOIA-19-02 Appeal

This is in response to your appeal under the Freedom of Information Act (FOIA), 5 USC § 552, dated April 1, 2019, which was received on April 2, 2019 by the FOIA Office at the United States African Development Foundation (USADF). In your appeal you requested segregable, releasable portions of the documents responsive to your request for the USADF Risk Assessment Plan and the USADF Security Handbook/Manual.

We have reviewed the documents and are releasing redacted and segregable portions of responsive documents – the Preface to the Risk Assessment Plan and the Table of Contents for the Security Handbook Manual – and are releasing USADF's IT Security Policy Manual in its entirety. The non-releasable portions of the documents you requested fall under the following exemptions to disclosure under FOIA: 1) records that are "specifically exempted from disclosure by statute", 2) records that are "related solely to the internal personnel rules and practices of an agency", 3) records that are "trade secrets and commercial or financial information", and 4) records containing "personnel and medical files and similar files" that if disclosed "would constitute a clearly unwarranted invasion of personal privacy". 5 USC § 552(b)(2),(3),(4), and (6).

The Federal Information Security Modernization Act (FISMA) of 2014 requires agencies to "take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security". 44 U.S.C. §?3551. Next, the Privacy Act of 1974 requires agencies to safeguard its information systems to prevent the unauthorized release of personal records. 5 U.S.C. § 552a. Under the Privacy Act, the term "record" means information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history. 5 USCS § 552a(4). USADF's information security systems established under FISMA include systems containing or related to personnel information, personally identifiable information (or "PII", covered by the Privacy Act) such as medical history/disability status, confidential information, and business proprietary information. Additionally, FISMA requires USADF to ensure the protection of information that if disclosed would risk the security of, not only USADF's systems, but also that of other interconnected agencies. 44 U.S.C. §?3551(2). USADF's security systems are interconnected with other government agencies who are service providers to USADF for contract/procurement, personnel and EEO matters and have access to USADF's protected information. Also, the information requested relates solely to internal personnel rules and practices as the documents are clearly marked for "Internal USADF Use" only and are intended only for use by and guidance to USADF staff. In sum, disclosure of the withheld information would risk jeopardizing the security of USADF's information systems and expose statutorily protected information contained in those systems.

Pursuant to 22 C.F.R. § 1502.7, there is no charge for USADF's services in responding to your request. Please contact me or USADF's Chief FOIA Officer, June Brown (202-233-8882; jbrown@usadf.gov), if you have any questions.

Best,

Nina-Belle S. Mbayu
Attorney Advisor/FOIA Public Liaison
U.S. African Development Foundation
1400 I Street NW
Washington, D.C. 20005
Tel.: 202-233-8808
Email: nbmbayu@usadf.gov

USADF SECURITY ASSESSMENT PLAN (SAP) SYNOPSIS

MAY 2019

The requested information falls under the following exemptions to disclosure under FOIA: 1) records that are “specifically exempted from disclosure by statute”, 2) records that are “related solely to the internal personnel rules and practices of an agency”, 3) records that are “trade secrets and commercial or financial information”, and 4) records containing “personnel and medical files and similar files” that if disclosed “would constitute a clearly unwarranted invasion of personal privacy”. 5 USC § 552(b)(2),(3),(4), and (6).

The Federal Information Security Modernization Act of 2014 (FISMA) requires USADF to protect risk assessments and other computer security measures, as such information that is inherently sensitive and warrants protection from disclosure. It is in the organization’s interest to take appropriate steps to ensure the protection of its information which, if disclosed, may adversely affect information security. In this regard, USADF’s information systems contain information that is solely related to internal personnel rules and practices of the agency, commercial and financial information from private businesses and organizations doing business with USADF, and detailed information on USADF staff members’ medical history and similar personnel files. Thus, under the aforementioned exemptions, USADF must protect the integrity of its information systems.

As a matter of discretion, the USADF is providing the preface as responsive to the requested information.

SUMMARY

The purpose of the Security Assessment Plan is to provide the outline for the security assessment process and the documentation that will be developed during the annual Security Assessment and Authorization (SA&A) for the United States African Development Foundation (USADF). The Security Assessment Plan identifies the assessment environment, assessment team roles and responsibilities, assessment procedures, and security and privacy controls to be assessed. The assessment plan was based on the NIST Framework, which offers detailed and robust guidance that can provide the USADF leaders with confidence in the effectiveness of their IT system capabilities, process, and controls. The process of conducting effective security and privacy control assessments described in the Security Assessment Plan follows the NIST Special Publication 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations.

ASSESSMENT ENVIRONMENT

The first part of Security Assessment Plan includes a description of the USADF information systems and their environments of operation that are subject to assessment. Describing the current information system is essential in setting the scope of the assessment.

ASSESSMENT TEAM ROLES AND RESPONSIBILITIES

The second part of Security Assessment Plan includes the roles and responsibilities of the Security Assessment Team. The conduct of security and privacy control assessments is the primary responsibility of USADF information system owners and common control providers with oversight by their respective authorizing officials. There is also involvement in the assessment process by other parties within the organization who have a vested interest in the outcome of the assessments. Other interested parties include mission/business owners, information owners, information security personnel, and designated privacy staff.

The Security Assessment Team is responsible for conducting USADF SA&A, ensuring clear and open communication between stakeholders, and identifying, addressing, and solving problems that may arise during the assessment. The Security Assessment Team is also responsible for providing oversight on project status while staying within budget and ensuring deliverables are completed on time.

ASSESSMENT PROCEDURES

The Security Assessment Plan advises that all testing procedures during the assessment shall follow NIST Special Publication 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations. During the course of this security assessment, IT Security specialists will conduct the assessment in accordance with 800-53A. Upon completion of the assessment, a formal Security Assessment Report will be developed and presented to the organization.

SECURITY AND PRIVACY CONTROLS TO BE ASSESSED

The Security Assessment Plan includes security and privacy controls selected and a part of the controls for NIST 800-53. Prior to the assessment, it is determined what security and privacy controls for the identified security categorization are to be evaluated against the organization’s information systems. The selected controls are critical to the security of the USADF information systems, and their selection addresses specific organizational needs for the testing of the system.

Note: NIST SP 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations is reviewed for the conduct of a tailored Security Control Assessment.

USADF IT SECURITY IMPLEMENTATION HANDBOOK

TABLE OF CONTENTS

MAY 2019

The requested information falls under the following exemptions to disclosure under FOIA: 1) records that are “specifically exempted from disclosure by statute”, 2) records that are “related solely to the internal personnel rules and practices of an agency”, 3) records that are “trade secrets and commercial or financial information”, and 4) records containing “personnel and medical files and similar files” that if disclosed “would constitute a clearly unwarranted invasion of personal privacy”. 5 USC § 552(b)(2),(3),(4), and (6).

The Federal Information Security Modernization Act of 2014 (FISMA) requires USADF to protect risk assessments and other computer security measures, as such information that is inherently sensitive and warrants protection from disclosure. It is in the organization’s interest to take appropriate steps to ensure the protection of its information which, if disclosed, may adversely affect information security. In this regard, USADF’s information systems contain information that is solely related to internal personnel rules and practices of the agency, commercial and financial information from private businesses and organizations doing business with USADF, and detailed information on USADF staff members’ medical history and similar personnel files. Thus, under the aforementioned exemptions, USADF must protect the integrity of its information systems.

As a matter of discretion, the USADF is releasing a segregable Table of Contents as part of the requested information.

Table of Contents

ADF MANUAL TRANSMITTAL MEMORANDUM

TM No. 142

DATE: **July 13, 2012**

TO: **ADF MANUAL HOLDERS**

FROM: **Lloyd Pierson, President and CEO**

SUBJECT: **ADF Manual Section Update Project – Updated IT Manual**

BACKGROUND:

A comprehensive review of all IT security-related policies, plans, and procedures was conducted over a 12-month period that included certification and accreditation activity, a FISMA audit, and an independent IT documentation assessment by an outside consulting firm. As a result, Manual Section 462 has been revised to focus strictly on IT security policy that establishes IT security goals and compliance and implementation priorities. All specific IT security implementation plans and procedures are eliminated from MS 462 and now reside in specific IT security implementation planning documents maintained outside the ADF Manual. The ADF Manual affected is summarized in the table below:

Old Manual Number and Name	Updated Manual Number and Name
MS-462 – IT Security Program Policy and Minimum Implementation Standards – 2011-05-03	MS-460 – IT Security Program Policy

MANUAL MAINTENANCE:

SECTION	DATE	ACTION	EFFECTIVE DATE
MS-462	05/03/2011	Remove manual section from current ADF Manual	07/13/2012
MS-460	7/13/2012	Insert in current ADF Manual	07/13/2012

Clearance: June B. Braun for DMM
Doris M. Martin, General Counsel
Date: July 13, 2012

Approved: Lloyd O. Pierson
Lloyd O Pierson, President and CEO
Date: July 15, 2012

ADF MANUAL

SUBJECT:	ADF IT Security Policies and Procedures
SECTION:	MS-460
DATE:	July 13, 2012
RESPONSIBLE OFFICE:	Office of Information Technology
SUPERSEDES:	MS 462 – IT Security Program Policy and Minimum Implementation Standards

Table of Contents:

1.0 AUTHORITY

“Federal Information Security Management Act of 2002”, (35 USC, Title 44, Subchapter III). This manual section incorporates by reference the Public Laws, Federal and Departmental regulations listed in Appendix B, IT Security Laws and Federal Regulations.

2.0 PURPOSE

This manual section sets out the minimum policies and practices governing the security of the African Development Foundation’s (ADF) computer systems with the goal of preserving the integrity, availability, and confidentiality of the agency’s computer information systems.

3.0 SCOPE

This manual section applies to all ADF employees and contract personnel in the United States. Overseas posts are subject to the policies and requirements of this manual section to the extent they have been provided with the appropriate equipment and have the technical capacity to do so.

4.0 WAIVER

When necessary to achieve program objectives or when special circumstances make deviation clearly in the best interest of the United States Government, the President of ADF may waive any part of this manual section in writing provided such waiver does not conflict with any law or regulation applicable to the Foundation's program.

5.0 GENERAL DEFINITIONS

5.1 **General support system (GSS)** is an interconnected technology resource that automates routine office functions. It normally includes hardware, software, information, data, applications, and communications, and provides support for a variety of users and applications. Individual applications support different mission-related functions. The ADF's general support system briefly can be described as a local area network (LAN) based on Microsoft Active Directory Domain Services (Windows 2008-level functional forest/domain) architecture. Other functions supported by the ADF LAN are e-mail, word processing, spreadsheets, and graphics. The highest level of information accessed and processed on the system is "Sensitive, But Unclassified" (SBU).

5.2 **Program support system (PSS)** is a core business system application that ADF uses to support the management of the grant budgets and disbursement activity.

5.3 **Rules of behavior** constitute the requirements, practices, and controls (do's and don'ts) governing the use, security, and acceptable level of risk of an IT system.

5.4 **Sensitive information** or **Sensitive But Unclassified Information** ("SBU Information") is information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes: (1) information the improper use or disclosure of which could adversely affect the ability of an agency to accomplish its mission; (2) proprietary information; (3) information requiring protection under the Privacy Act; and (4) information protected from disclosure under the Freedom of Information Act. The term does not include classified information.

5 .5 **Technical controls** consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

6.0 GENERAL IT SECURITY POLICY AND GOALS

6.1 General Policies

It is the policy of the ADF to ensure the security of the Agency's computer systems, including the systems' physical components and the information stored within each system. The security requirements and procedures in this manual section are intended to establish measures that will eliminate or reduce the risk of security threats to the Agency's systems to an acceptable level and protect against the financial and program costs that result when information is lost, compromised, or unavailable when needed.

6.2 Goals

The IT security policies and procedures in this manual section are intended to help achieve three goals: the availability, integrity and confidentiality of the Agency's systems.

1) Availability

   Computer systems must be available for use in a timely fashion. Any denial of a system's use or substantial delay in a system's processing could adversely affect the ability of an individual, office, or program to conduct business. Accordingly, protections from physical destruction, theft, or virus outbreaks, for example, should be in place.

2) Integrity

   The integrity of the information in the Agency's computer systems must be maintained. To achieve its statutory purpose, the Agency must be able to rely on the authenticity of the information maintained in its computer systems, such as financial records, e-mails, and program and administrative data. Integrity can be compromised by human error when entering data; when transmitting data from one computer to another; by software bugs or viruses; by hardware malfunctions, such as disk crashes; or by natural disasters, such as fires or floods. The integrity of the Agency's systems should be protected by appropriate handling by the user and by utilizing a system architecture designed to protect data from corruption and recover lost or corrupted information.

3) Confidentiality

Sensitive information must be protected against unauthorized access or disclosure. Sensitive information is often included in legal, financial, national policy, budget, personnel, contractual, procurement, proprietary, or agency-critical information.

6.3 Compliance

Provided available resources, on an annual basis, the Chief Information Officer (CIO) or designate will review, maintain, and update three IT Security Implementation plans to ensure that minimum implementation standards found in the (current version of) National Institute for Standards and Technology Special Publication 800-53 Rev 3 are a routine part of ADF IT operations. These documents are:

1) The USADF IT Security Implementation Plan;

2) The USADF Program Support System Security Support Plan; and

3) The USADF General Support System Security Support Plan.

To facilitate a coordinated approach to security the CIO or designate will ensure that technical controls are properly implemented in addressed in the development of the USADF IT Security Implementation Plan and system security plans with emphasis placed on implementation of priority level 1. Implementing controls for priority levels 2 and 3 will follow the achievement of level 1 and on an as needed basis. The USADF IT Security Implementation Plan will be used to support achieving compliance requirements identified by various FISMA audit and certification and accreditation activities, and updated as required.

6.4 Roles and Responsibilities

The IT Security Implementation Plan defines roles and responsibilities necessary to achieve the goals and objectives of this policy.