Audit Report

OIG-10-037

AUDIT REPORT

INFORMATION TECHNOLOGY: Improvements Needed in CDFI Fund's Access Controls and Configuration Management

February 25, 2010

Office of Inspector General

Department of the Treasury

Contents

Appendices

Abbreviations

CDFI Fund	Community Development Financial Institutions Fund
FTP	File Transfer Protocol
NIST	National Institute of Standards and Technology
OIG	Treasury Office of Inspector General
SNMP	Simple Network Management Protocol

OIG

Audit Report

The Department of the Treasury
Office of Inspector General

February 25, 2010

Donna Gambrell
Director
Community Development Financial Institutions Fund

The objective of this audit was to determine if the Community Development Financial Institutions (CDFI) Fund had sufficient protections in place to prevent intrusions into its network and systems.

To accomplish our objective, we performed a series of vulnerability assessments and penetration tests of the CDFI Fund's network and systems. Additionally, we performed a series of social engineering tests to determine if users of the CDFI Fund's network and systems were aware of cybersecurity threats and users' role in protecting agency information technology resources.

We performed our fieldwork at CDFI Fund facilities in Washington, DC, from February through April 2009. The audit was performed in accordance with generally accepted government auditing standards.[1] Our objective, scope, and methodology are described in appendix 1.

Results in Brief

We determined that, for the most part, the CDFI Fund has sufficient protection in place for its network and systems. Specifically, most CDFI Fund systems were up to date with the latest patches. Also, CDFI Fund staff had implemented a suite of monitoring tools for its network that reported current patch levels,

[1] Government Accountability Office, *Government Auditing Standards*, GAO-07-731G (July 2007).

monitored for suspicious activities, and provided notification to administrators of potentially suspicious activities. As result, we were unsuccessful in establishing remote connection into the CDFI Fund's network. However, we noted that improvements are needed in key access controls and in configuration management to prevent unauthorized users from gaining access and compromising data on the CDFI Fund's public Web site and within its network.

We found the following weaknesses:

1. Weak passwords were used in CDFI Fund applications and systems.
2. CDFI Fund systems were configured with insecure default settings.
3. A critical patch was not applied for one CDFI Fund system.

We are making seven recommendations to the CDFI Fund Director to address the findings noted above.

In a written response, the CDFI Fund Director provided plans for corrective actions that are responsive to the intent of our recommendations (see appendix 2).

Background

The CDFI Fund's mission is to expand the capacity of financial institutions to provide credit, capital, and financial services to underserved populations and economically distressed communities in the United States. The CDFI Fund was created to promote economic revitalization and community development through investment in and assistance to community development financial institutions. The CDFI Fund was established by the Riegle Community Development and Regulatory Improvement Act of 1994.

Since its creation, the CDFI Fund has awarded $1.13 billion to community development organizations and financial institutions (as of September 30, 2009). The CDFI Fund was further expanded in fiscal year 2009 with the enactment of legislation that created the Capital Magnet Fund, which will be implemented in fiscal year 2010, subject to funding availability. In addition, the CDFI Fund has allocated $26 billion in tax credit authority to Community Development Entities through the New Markets Tax Credit program.

To help ensure the important mission of the CDFI is fulfilled, strong security controls are necessary to protect the confidentiality, integrity, and availability of the Fund's data and systems. Weak controls provide unauthorized users an opportunity to launch various programs that could allow them to view sensitive information, change or delete data, discover user names and passwords, initiate denial-of-service attacks, attack other entities, and impair the reputation and mission of the CDFI Fund.

Findings and Recommendations

Finding 1 Weak Passwords Were Used in CDFI Fund Applications and Systems

We determined that weak passwords were used in CDFI Fund applications and systems and that weak default passwords were used on the myCDFI Web site. In addition, 21 user accounts had passwords that were set to never expire. Two of these were end-user accounts for information technology personnel and one was an administrative account. We also found that databases had login accounts containing either blank passwords, passwords identical to the login name, or easily guessed passwords. One of these login accounts had full administrative rights on the databases and access to both personally identifiable information and potentially sensitive information. While the CDFI Fund password policy specifically addresses user accounts, it does not establish requirements for passwords used by applications and services.

We also found six printers that we were able to log onto using File Transfer Protocol (FTP) with blank login user IDs and passwords. A user would be able to use this access to view and download files sent to the printer and utilize the FTP service to attack other systems on the network. It should be noted that the CDFI Fund quickly corrected this problem after we discovered it. It should also be noted that we subsequently verified these accounts were in fact disabled. Therefore, we are not making a recommendation to address this particular issue.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 2, Recommended Security Controls for Federal Information Systems, states that an information system should enforce assigned authorizations for controlling access to the system in accordance with applicable policy and that an organization should enforce password minimum and maximum lifetime restrictions. In addition, as noted above, CDFI Fund password policy requires use of strong passwords for user accounts.

The Web site and database password weaknesses resulted from poor implementation of security procedures during the development of custom CDFI Fund applications. We were unable to determine the specific cause of the nonexpiring passwords but nonexpiring passwords typically result from administrators' efforts to minimize the need to synchronize passwords for network devices and shared administrative accounts. The six printers that we were able to log onto using FTP with blank login user IDs and passwords were printers on which the CDFI Fund network administrator was unaware that FTP service was active.

Poor administrative practices, such as failure to change default password or allowing the use of easily guessed passwords or blank passwords, often result in successful attacks on systems because they make it easier for attackers to gain unauthorized access. Once attackers gain access, they can both obtain sensitive information from a system and gather information that makes further attacks easier. Attackers who have gained access to a system are in a much better position to launch additional attacks that reach further into a system and to install backdoors that can bypass other security protections.

Recommendations

We recommend that the Director of the CDFI Fund do the following:

1. Update the CDFI Fund password policy to require strong passwords and password expirations for CDFI Fund applications

and databases and enforce this policy for all CDFI Fund applications and databases.
2. Generate unique passwords for new user accounts and require that new users change their assigned default password during their initial login to the myCDFI application.

Management Response

The CDFI Fund has updated its password policy to require strong passwords and password expirations for all applications and databases. The CDFI Fund is currently enforcing this policy.

The CDFI Fund has generated unique, strong passwords for all new and current user accounts. The CDFI Fund requires that new users change their assigned default password during their initial login to the myCDFI application. This mitigation action was completed November 15, 2009.

OIG Comment

Management's reported corrective actions are responsive to the intent of our recommendations.

Finding 2 CDFI Fund Systems Were Configured With Insecure Default Settings

We determined that some CDFI Fund systems were running software with insecure default configuration settings. Based on our network scans, we found the following:

- Ten systems where users could obtain the Windows password policy without authentication.

  The Windows password policy contains sensitive information about minimum password length, password lockout threshold, password lockout duration, and so on.

- As discussed in Finding 1 above, six printers running the FTP server service were found that did not have passwords.

  The FTP service is installed by default on many printer controllers and often is configured in an unsecure manner. The CDFI Fund network administrator indicated that they were unaware the service was active on these printers and that it was unnecessary. The administrator subsequently disabled the service on each printer.

- Ten systems with default or guessable Simple Network Management Protocol (SNMP) read-only community names.

  SNMP is a commonly used network service that provides network administrators with information about devices connected to the network. Ten SNMP servers were configured with simple default community names, which should be changed by the system administrators prior to deployment. The community name functions as the password for access to the device. Anyone who knows the read-only community name and has a network connection to the device can retrieve sensitive technical information about the device configuration.

- Four systems with default or guessable SNMP read/write community names.

  Anyone who knows the read/write community name and has a network connection to the device can retrieve information about the device configuration, change the configuration, or disable the device.

- One system with two vulnerabilities related to the default sample programs installed on the Apache Tomcat server.

  A Tomcat server is used to host Web-based applications utilizing the Java programming language. An attacker could exploit these vulnerabilities to send attack code to the user's Web browser. This code can be used to retrieve information stored in the browser, redirect the user to another Web site, or issue additional Web page requests on the user's behalf.

NIST's Recommended Security Controls for Federal Information Systems requires organizations to configure their information systems to provide only essential capabilities and specifically prohibit or restrict the use of agency-defined functions, ports, protocols, or services. In addition, NIST SP 800-123, Guide to General Server Security, recommends SNMP be removed or disabled if it is not required. NIST SP 800-44, Guidelines on Securing Public Web Servers, recommends that system administrators remove all example or test files from servers, including scripts and executable code.

Default settings on network services existed because administrators did not harden the systems before placing them in the production environment.

Anonymous access to domain password information allows attackers connected to the CDFI Fund network without authentication to design password attacks within the confines of the policy. Customizing the password attack list significantly decreases the number of passwords an attacker would have to guess. Unnecessary services can provide methods of attack that would not be possible if the service was disabled. If SNMP community names are not changed from the default, attackers can use them to view and modify system configurations. Finally, the presence of known vulnerable sample applications on the Apache server can allow attackers to steal login IDs and other information from legitimate users of the system.

Recommendations

We recommend that the Director of the CDFI Fund do the following:

3. Implement Windows security settings that prevent unauthenticated users from accessing domain policies.
4. Scan all CDFI systems on a regular basis to determine if unnecessary services are present and remove unnecessary services.
5. Change SNMP community names to comply with Treasury password requirements or remove or disable unnecessary SNMP services on network devices.
6. Remove sample applications installed on the Apache Tomcat server.

Management Response

The CDFI Fund has implemented windows security settings that prevent unauthenticated users from accessing domain policies. The CDFI Fund currently performs monthly Federal Information Security Management Act compliant and Federal Desktop Core Configuration vulnerability scans and all unneeded services have been removed from all the CDFI Fund's servers. Additionally, CDFI Fund has changed all SNMP read/write community strings to passwords that meet/exceed Treasury requirements. Finally, the CDFI Fund removed the Documentum services from the enterprise in November of 2009. The Documentum application/service contained two Tomcat vulnerabilities that were identified in the OIG's audit.

OIG Comment

Management's reported corrective actions are responsive to the intent of our recommendations.

Finding 3 A Critical Patch Was Not Applied for One CDFI Fund System

Although most CDFI Fund systems had current critical security patches installed, we identified one system missing a critical patch which allowed remote exploitation. We succeeded in exploiting this vulnerability during our test and gained system-level access, which allows full control of a system. While system level access did give us full control of the specific system that lacked the critical patch, that system had no access privileges to other CDFI Fund systems. As a result, we were unable to directly access CDFI Fund network servers based on the access level gained on this system. However, an attacker could use this level of access to reconfigure or disable the system, store and transmit information, or serve malicious content to CDFI Fund users from within the network. The system that lacked the patch is used specifically to control a printer and is not a critical system.

Treasury Directive Publication 85-01, Treasury Information Technology Security Program, requires bureaus to ensure that security patches are tested and installed on a timeline in accordance with the criticality of the patches.

According to the CDFI Fund system administrator, the system had not been patched because it was part of a printer.

Without the critical patch, the printer was vulnerable to attack. An attacker could view any documents sent to the printer, modify printer settings, and use the compromised printer to attack other CDFI Fund systems.

Recommendation

We recommend that the Director of the CDFI Fund do the following:

7. Apply critical security patches on the identified system, disable the identified system, or provide another compensating control(s) if patches are not available.

Management Response

The actual system identified in the OIG's findings was a printer which was disabled and removed from the network in January of 2010. The CDFI Fund has also removed similar systems from the network to mitigate any future risk.

OIG Comment

Management’s reported corrective action is responsive to the intent of our recommendation.

* * * * * *

I would like to extend my appreciation to the Director of the CDFI Fund and to CDFI Fund staff for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-5171 or Susan Miller, Audit Manager, at (202) 927-5746. Major contributors to this report are listed in appendix 3.

/s/

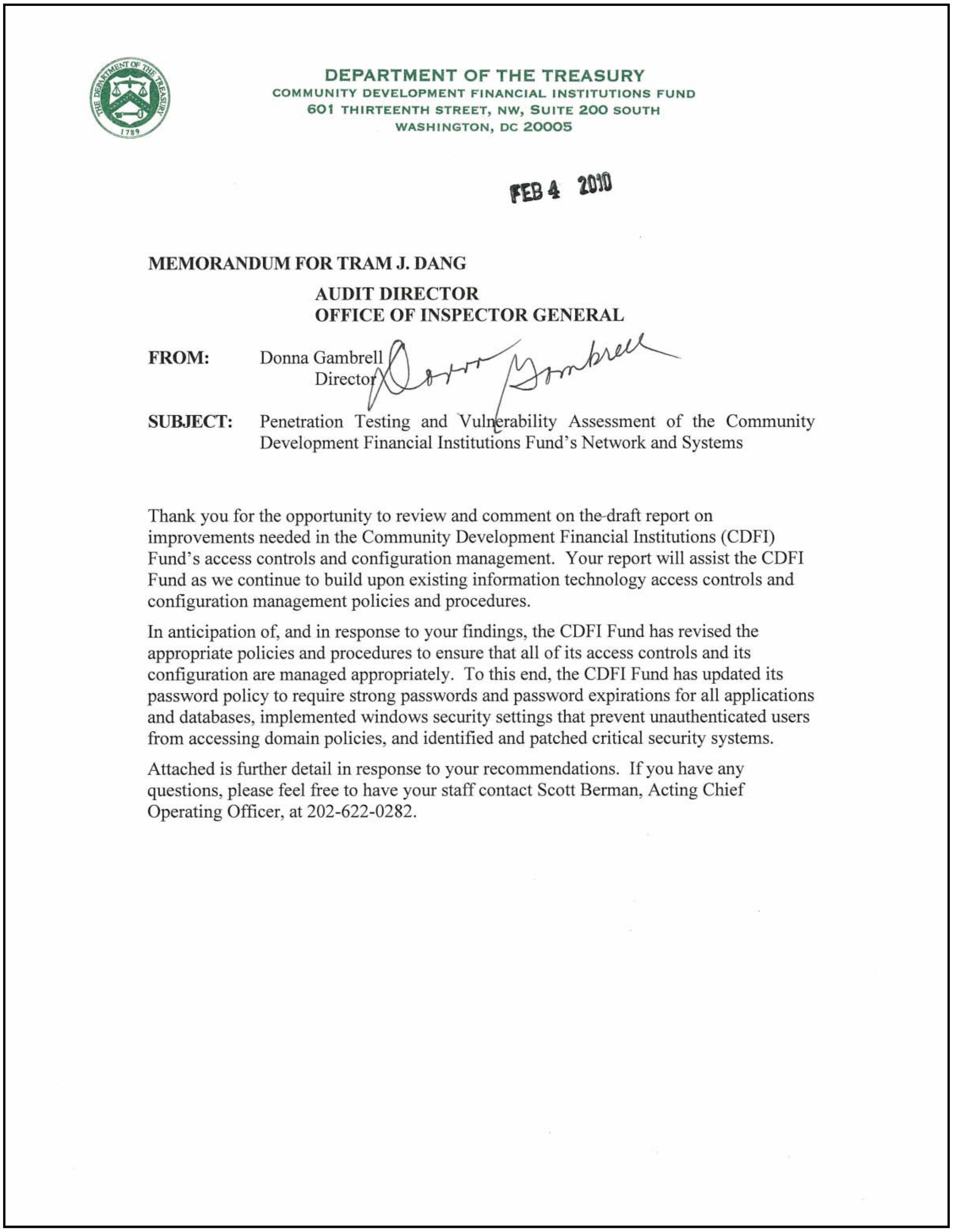
Tram Jacquelyn Dang
Audit Director

Appendix 1
Objective, Scope, and Methodology

The purpose of this audit was to assess the security of the Community Development Financial Institutions (CDFI) Fund's network and systems. Our overall objective was to determine if the CDFI Fund had sufficient protections in place to prevent intrusions into its network and systems.

To accomplish our objective, we performed a series of vulnerability assessments and penetration tests of the CDFI Fund's network and systems. Penetration testing was performed external to the CDFI Fund's network using only information available to the general public. Vulnerability assessments inside the CDFI Fund's network were performed from an administrative perspective with full knowledge and system access. We performed a series of social engineering tests to determine whether CDFI Fund users were aware of cybersecurity threats and users' role in protecting agency information technology resources. The results of this audit may be used to support our work undertaken in accordance with the requirements of the Federal Information Security Management Act.

We performed our fieldwork at CDFI Fund facilities in Washington, DC, from February through April 2009. The audit was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



DEPARTMENT OF THE TREASURY
COMMUNITY DEVELOPMENT FINANCIAL INSTITUTIONS FUND
601 THIRTEENTH STREET, NW, SUITE 200 SOUTH
WASHINGTON, DC 20005

FEB 4 2010

MEMORANDUM FOR TRAM J. DANG
AUDIT DIRECTOR
OFFICE OF INSPECTOR GENERAL

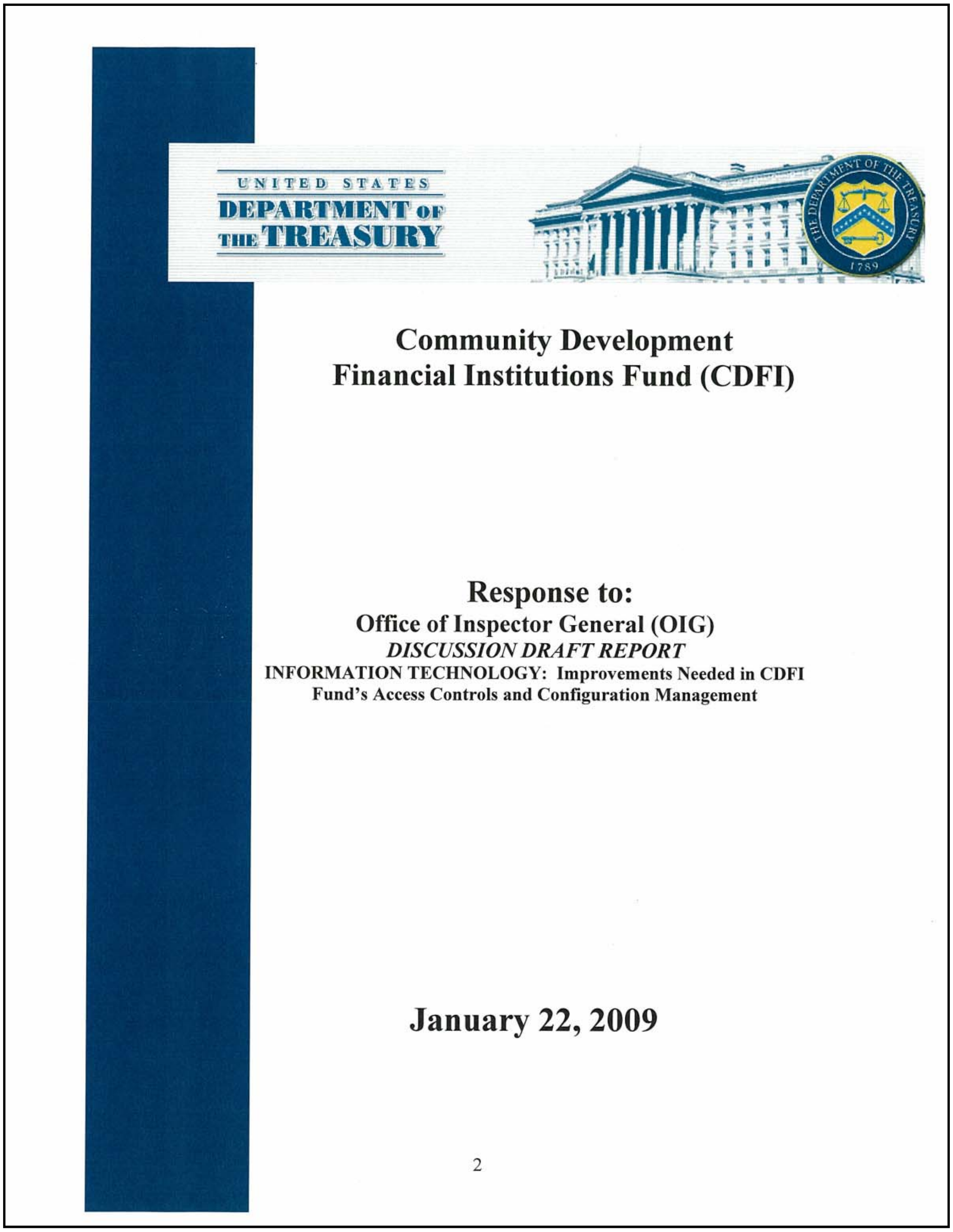
FROM: Donna Gambrell
Director

SUBJECT: Penetration Testing and Vulnerability Assessment of the Community Development Financial Institutions Fund's Network and Systems

Thank you for the opportunity to review and comment on the draft report on improvements needed in the Community Development Financial Institutions (CDFI) Fund's access controls and configuration management. Your report will assist the CDFI Fund as we continue to build upon existing information technology access controls and configuration management policies and procedures.

In anticipation of, and in response to your findings, the CDFI Fund has revised the appropriate policies and procedures to ensure that all of its access controls and its configuration are managed appropriately. To this end, the CDFI Fund has updated its password policy to require strong passwords and password expirations for all applications and databases, implemented windows security settings that prevent unauthenticated users from accessing domain policies, and identified and patched critical security systems.

Attached is further detail in response to your recommendations. If you have any questions, please feel free to have your staff contact Scott Berman, Acting Chief Operating Officer, at 202-622-0282.



UNITED STATES
DEPARTMENT OF THE TREASURY

THE DEPARTMENT OF THE TREASURY 1789

Community Development Financial Institutions Fund (CDFI)

Response to:

Office of Inspector General (OIG)

DISCUSSION DRAFT REPORT

INFORMATION TECHNOLOGY: Improvements Needed in CDFI Fund's Access Controls and Configuration Management

January 22, 2009

2

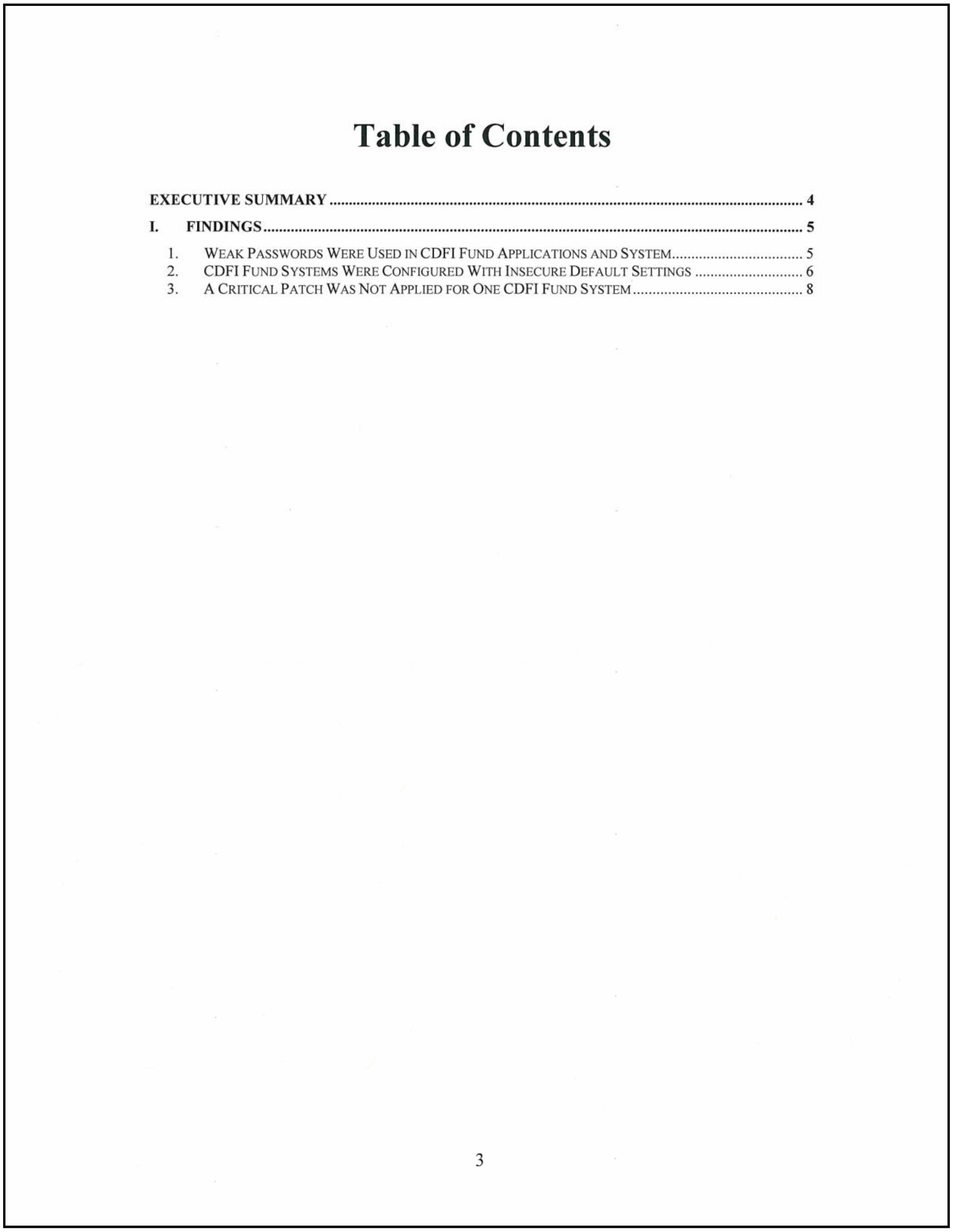
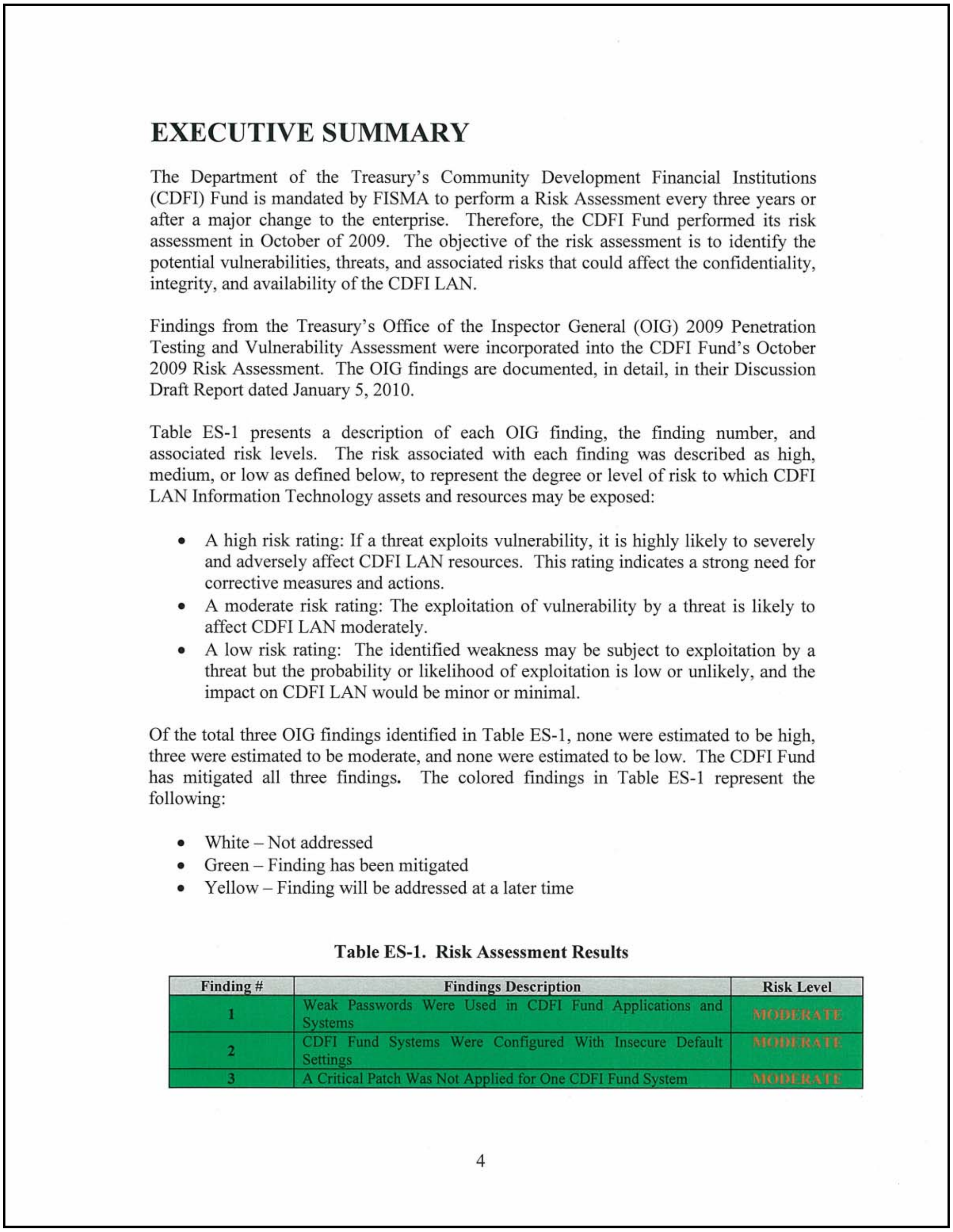


Table of Contents



EXECUTIVE SUMMARY

The Department of the Treasury's Community Development Financial Institutions (CDFI) Fund is mandated by FISMA to perform a Risk Assessment every three years or after a major change to the enterprise. Therefore, the CDFI Fund performed its risk assessment in October of 2009. The objective of the risk assessment is to identify the potential vulnerabilities, threats, and associated risks that could affect the confidentiality, integrity, and availability of the CDFI LAN.

Findings from the Treasury's Office of the Inspector General (OIG) 2009 Penetration Testing and Vulnerability Assessment were incorporated into the CDFI Fund's October 2009 Risk Assessment. The OIG findings are documented, in detail, in their Discussion Draft Report dated January 5, 2010.

Table ES-1 presents a description of each OIG finding, the finding number, and associated risk levels. The risk associated with each finding was described as high, medium, or low as defined below, to represent the degree or level of risk to which CDFI LAN Information Technology assets and resources may be exposed:

- A high risk rating: If a threat exploits vulnerability, it is highly likely to severely and adversely affect CDFI LAN resources. This rating indicates a strong need for corrective measures and actions.
- A moderate risk rating: The exploitation of vulnerability by a threat is likely to affect CDFI LAN moderately.
- A low risk rating: The identified weakness may be subject to exploitation by a threat but the probability or likelihood of exploitation is low or unlikely, and the impact on CDFI LAN would be minor or minimal.

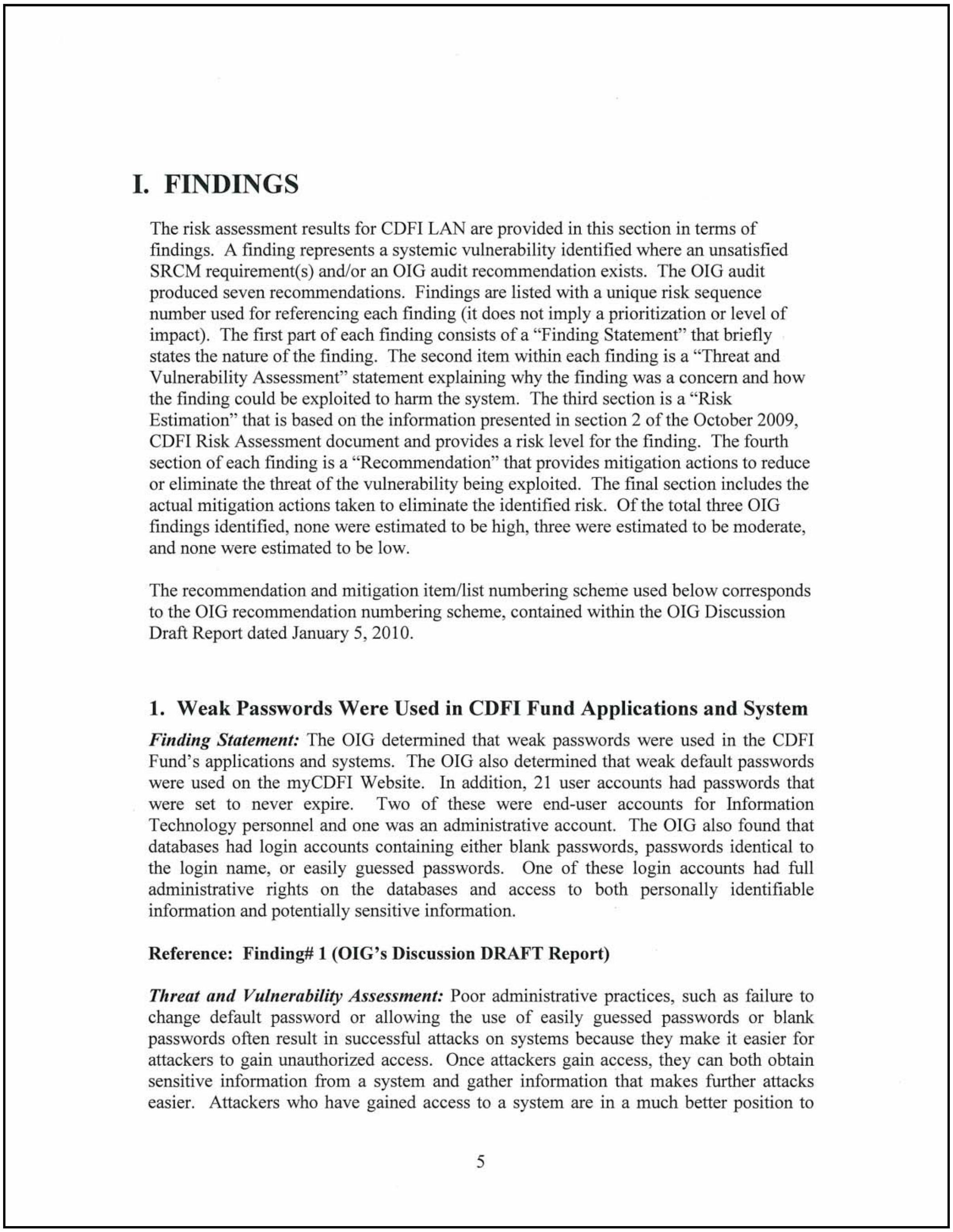
Of the total three OIG findings identified in Table ES-1, none were estimated to be high, three were estimated to be moderate, and none were estimated to be low. The CDFI Fund has mitigated all three findings. The colored findings in Table ES-1 represent the following:

- White – Not addressed
- Green – Finding has been mitigated
- Yellow – Finding will be addressed at a later time

Table ES-1. Risk Assessment Results

Finding #	Findings Description	Risk Level
1	Weak Passwords Were Used in CDFI Fund Applications and Systems	MODERATE
2	CDFI Fund Systems Were Configured With Insecure Default Settings	MODERATE
3	A Critical Patch Was Not Applied for One CDFI Fund System	MODERATE

4



I. FINDINGS

The risk assessment results for CDFI LAN are provided in this section in terms of findings. A finding represents a systemic vulnerability identified where an unsatisfied SRCM requirement(s) and/or an OIG audit recommendation exists. The OIG audit produced seven recommendations. Findings are listed with a unique risk sequence number used for referencing each finding (it does not imply a prioritization or level of impact). The first part of each finding consists of a "Finding Statement" that briefly states the nature of the finding. The second item within each finding is a "Threat and Vulnerability Assessment" statement explaining why the finding was a concern and how the finding could be exploited to harm the system. The third section is a "Risk Estimation" that is based on the information presented in section 2 of the October 2009, CDFI Risk Assessment document and provides a risk level for the finding. The fourth section of each finding is a "Recommendation" that provides mitigation actions to reduce or eliminate the threat of the vulnerability being exploited. The final section includes the actual mitigation actions taken to eliminate the identified risk. Of the total three OIG findings identified, none were estimated to be high, three were estimated to be moderate, and none were estimated to be low.

The recommendation and mitigation item/list numbering scheme used below corresponds to the OIG recommendation numbering scheme, contained within the OIG Discussion Draft Report dated January 5, 2010.

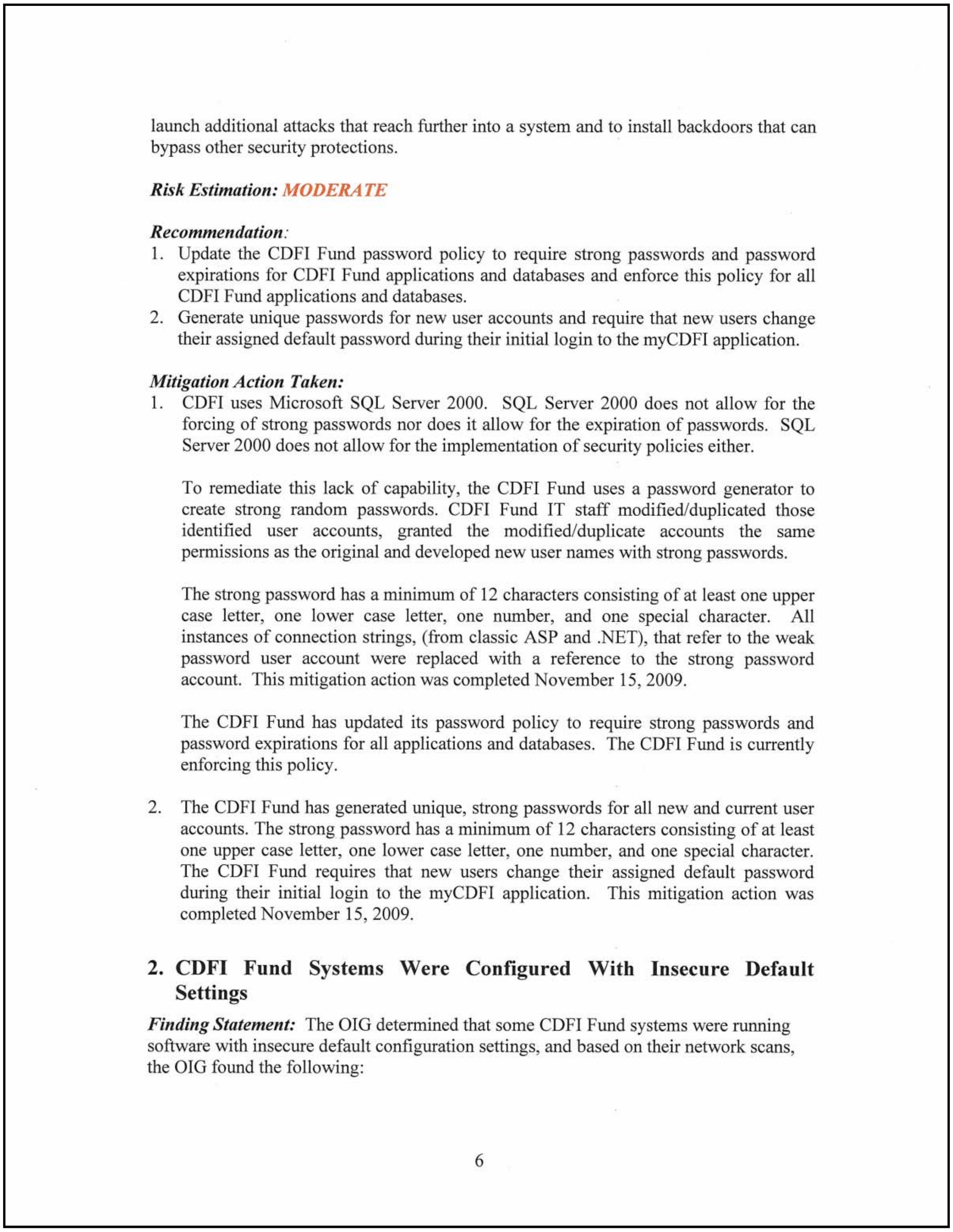
1. Weak Passwords Were Used in CDFI Fund Applications and System

Finding Statement: The OIG determined that weak passwords were used in the CDFI Fund's applications and systems. The OIG also determined that weak default passwords were used on the myCDFI Website. In addition, 21 user accounts had passwords that were set to never expire. Two of these were end-user accounts for Information Technology personnel and one was an administrative account. The OIG also found that databases had login accounts containing either blank passwords, passwords identical to the login name, or easily guessed passwords. One of these login accounts had full administrative rights on the databases and access to both personally identifiable information and potentially sensitive information.

Reference: Finding# 1 (OIG's Discussion DRAFT Report)

Threat and Vulnerability Assessment: Poor administrative practices, such as failure to change default password or allowing the use of easily guessed passwords or blank passwords often result in successful attacks on systems because they make it easier for attackers to gain unauthorized access. Once attackers gain access, they can both obtain sensitive information from a system and gather information that makes further attacks easier. Attackers who have gained access to a system are in a much better position to

5



launch additional attacks that reach further into a system and to install backdoors that can bypass other security protections.

Risk Estimation: ***MODERATE***

Recommendation:

1. Update the CDFI Fund password policy to require strong passwords and password expirations for CDFI Fund applications and databases and enforce this policy for all CDFI Fund applications and databases.
2. Generate unique passwords for new user accounts and require that new users change their assigned default password during their initial login to the myCDFI application.

Mitigation Action Taken:

1. CDFI uses Microsoft SQL Server 2000. SQL Server 2000 does not allow for the forcing of strong passwords nor does it allow for the expiration of passwords. SQL Server 2000 does not allow for the implementation of security policies either.

   To remediate this lack of capability, the CDFI Fund uses a password generator to create strong random passwords. CDFI Fund IT staff modified/duplicated those identified user accounts, granted the modified/duplicate accounts the same permissions as the original and developed new user names with strong passwords.

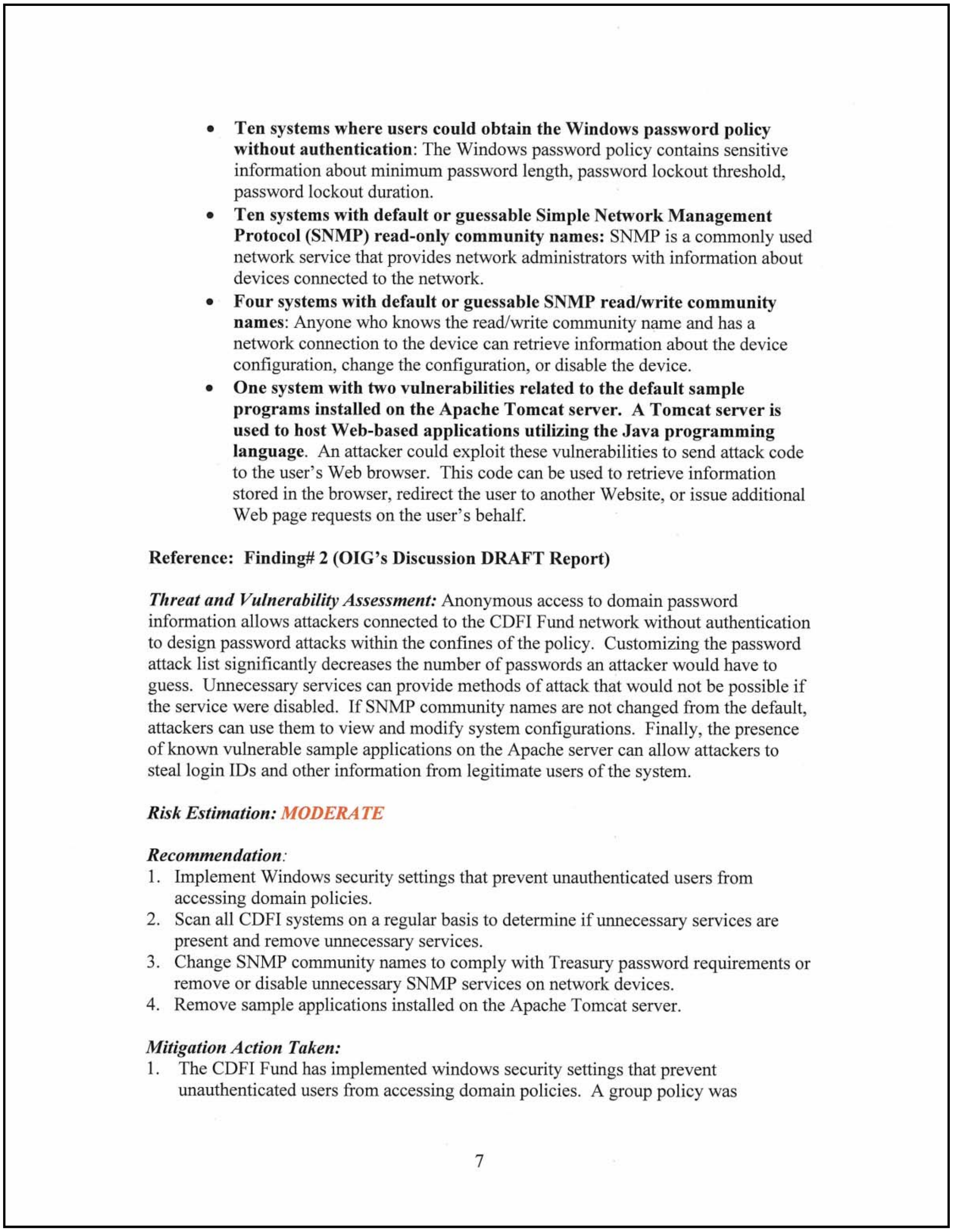
   The strong password has a minimum of 12 characters consisting of at least one upper case letter, one lower case letter, one number, and one special character. All instances of connection strings, (from classic ASP and .NET), that refer to the weak password user account were replaced with a reference to the strong password account. This mitigation action was completed November 15, 2009.

   The CDFI Fund has updated its password policy to require strong passwords and password expirations for all applications and databases. The CDFI Fund is currently enforcing this policy.

2. The CDFI Fund has generated unique, strong passwords for all new and current user accounts. The strong password has a minimum of 12 characters consisting of at least one upper case letter, one lower case letter, one number, and one special character. The CDFI Fund requires that new users change their assigned default password during their initial login to the myCDFI application. This mitigation action was completed November 15, 2009.

2. CDFI Fund Systems Were Configured With Insecure Default Settings

Finding Statement: The OIG determined that some CDFI Fund systems were running software with insecure default configuration settings, and based on their network scans, the OIG found the following:



- **Ten systems where users could obtain the Windows password policy without authentication**: The Windows password policy contains sensitive information about minimum password length, password lockout threshold, password lockout duration.
- **Ten systems with default or guessable Simple Network Management Protocol (SNMP) read-only community names:** SNMP is a commonly used network service that provides network administrators with information about devices connected to the network.
- **Four systems with default or guessable SNMP read/write community names**: Anyone who knows the read/write community name and has a network connection to the device can retrieve information about the device configuration, change the configuration, or disable the device.
- **One system with two vulnerabilities related to the default sample programs installed on the Apache Tomcat server. A Tomcat server is used to host Web-based applications utilizing the Java programming language**. An attacker could exploit these vulnerabilities to send attack code to the user's Web browser. This code can be used to retrieve information stored in the browser, redirect the user to another Website, or issue additional Web page requests on the user's behalf.

Reference: Finding# 2 (OIG's Discussion DRAFT Report)

Threat and Vulnerability Assessment: Anonymous access to domain password information allows attackers connected to the CDFI Fund network without authentication to design password attacks within the confines of the policy. Customizing the password attack list significantly decreases the number of passwords an attacker would have to guess. Unnecessary services can provide methods of attack that would not be possible if the service were disabled. If SNMP community names are not changed from the default, attackers can use them to view and modify system configurations. Finally, the presence of known vulnerable sample applications on the Apache server can allow attackers to steal login IDs and other information from legitimate users of the system.

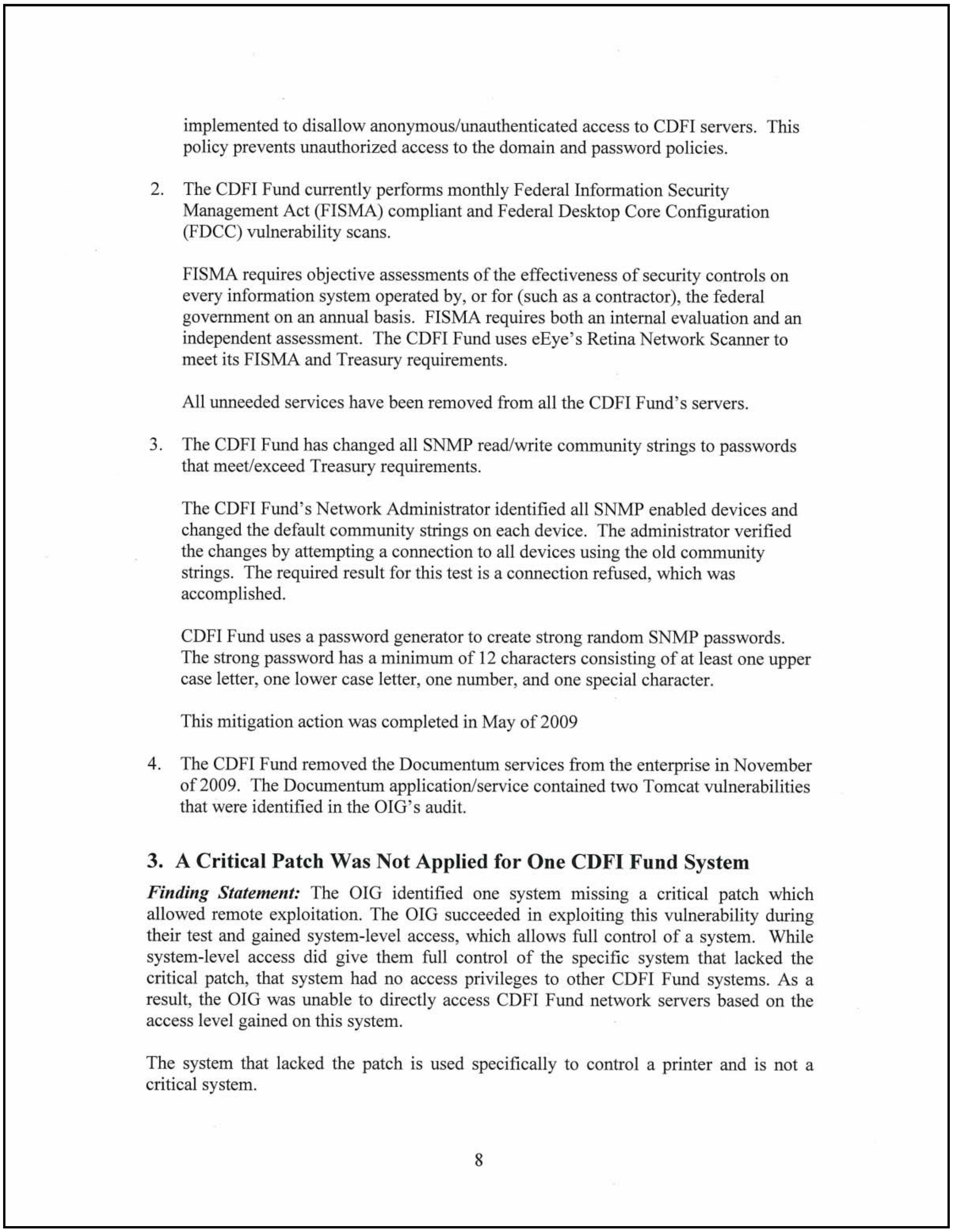
Risk Estimation: MODERATE

***Recommendation**:*

1. Implement Windows security settings that prevent unauthenticated users from accessing domain policies.
2. Scan all CDFI systems on a regular basis to determine if unnecessary services are present and remove unnecessary services.
3. Change SNMP community names to comply with Treasury password requirements or remove or disable unnecessary SNMP services on network devices.
4. Remove sample applications installed on the Apache Tomcat server.

Mitigation Action Taken:

1. The CDFI Fund has implemented windows security settings that prevent unauthenticated users from accessing domain policies. A group policy was



implemented to disallow anonymous/unauthenticated access to CDFI servers. This policy prevents unauthorized access to the domain and password policies.

2. The CDFI Fund currently performs monthly Federal Information Security Management Act (FISMA) compliant and Federal Desktop Core Configuration (FDCC) vulnerability scans.

   FISMA requires objective assessments of the effectiveness of security controls on every information system operated by, or for (such as a contractor), the federal government on an annual basis. FISMA requires both an internal evaluation and an independent assessment. The CDFI Fund uses eEye's Retina Network Scanner to meet its FISMA and Treasury requirements.

   All unneeded services have been removed from all the CDFI Fund's servers.

3. The CDFI Fund has changed all SNMP read/write community strings to passwords that meet/exceed Treasury requirements.

   The CDFI Fund's Network Administrator identified all SNMP enabled devices and changed the default community strings on each device. The administrator verified the changes by attempting a connection to all devices using the old community strings. The required result for this test is a connection refused, which was accomplished.

   CDFI Fund uses a password generator to create strong random SNMP passwords. The strong password has a minimum of 12 characters consisting of at least one upper case letter, one lower case letter, one number, and one special character.

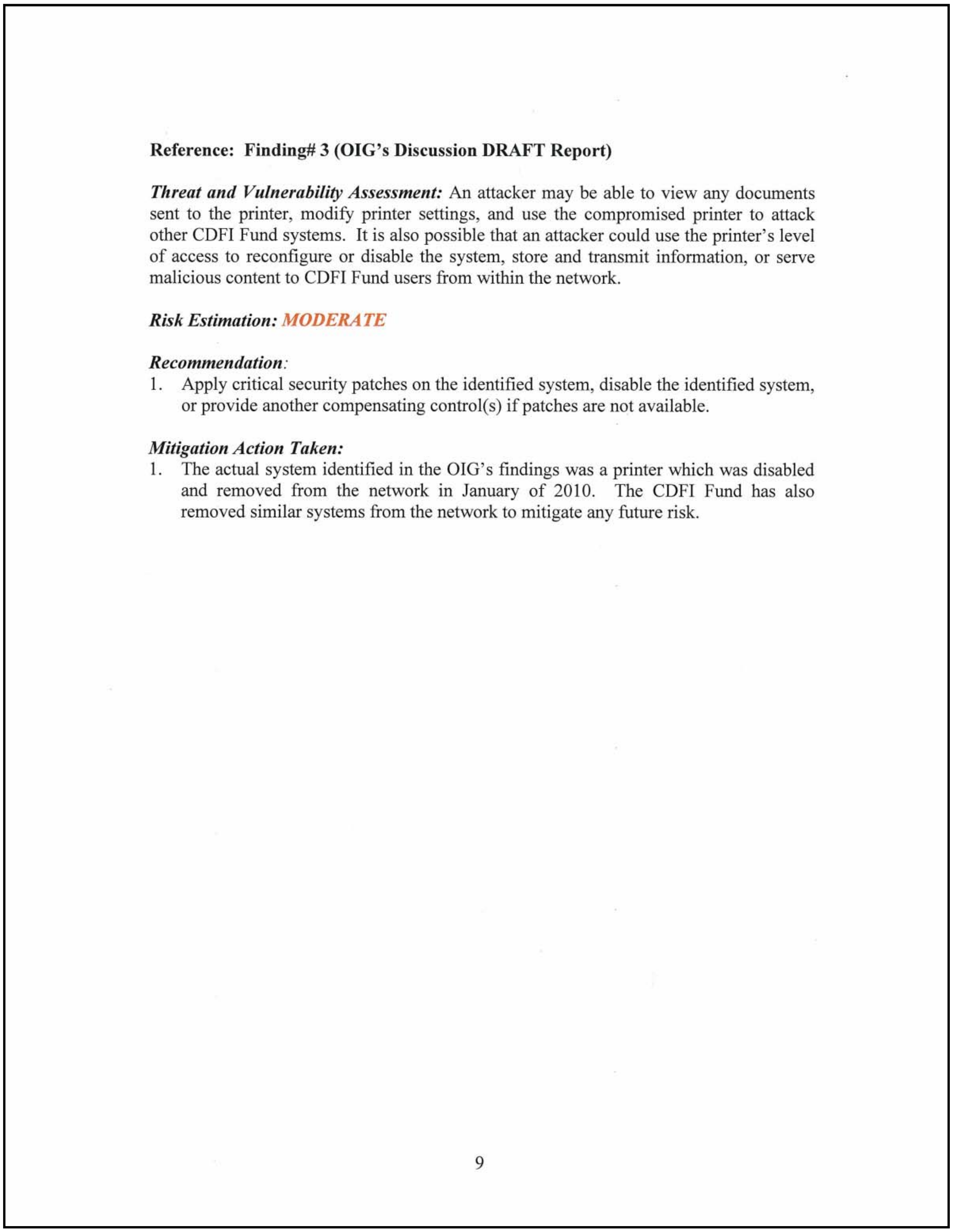
   This mitigation action was completed in May of 2009

4. The CDFI Fund removed the Documentum services from the enterprise in November of 2009. The Documentum application/service contained two Tomcat vulnerabilities that were identified in the OIG's audit.

3. A Critical Patch Was Not Applied for One CDFI Fund System

Finding Statement: The OIG identified one system missing a critical patch which allowed remote exploitation. The OIG succeeded in exploiting this vulnerability during their test and gained system-level access, which allows full control of a system. While system-level access did give them full control of the specific system that lacked the critical patch, that system had no access privileges to other CDFI Fund systems. As a result, the OIG was unable to directly access CDFI Fund network servers based on the access level gained on this system.

The system that lacked the patch is used specifically to control a printer and is not a critical system.



Reference: Finding# 3 (OIG's Discussion DRAFT Report)

Threat and Vulnerability Assessment: An attacker may be able to view any documents sent to the printer, modify printer settings, and use the compromised printer to attack other CDFI Fund systems. It is also possible that an attacker could use the printer's level of access to reconfigure or disable the system, store and transmit information, or serve malicious content to CDFI Fund users from within the network.

Risk Estimation: MODERATE

***Recommendation**:*

1. Apply critical security patches on the identified system, disable the identified system, or provide another compensating control(s) if patches are not available.

Mitigation Action Taken:

1. The actual system identified in the OIG's findings was a printer which was disabled and removed from the network in January of 2010. The CDFI Fund has also removed similar systems from the network to mitigate any future risk.

Office of IT Audits

Tram J. Dang, Director
Susan Miller, IT Audit Manager
Gerald J. Steere, IT Specialist (Lead)
Abdil Salah, IT Specialist
Jane E. Lee, IT Specialist
Larissa Klimpel, IT Specialist
Timothy Cargill, Referencer

Community Development Financial Institutions Fund

Director

Department of the Treasury

Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management
Office of the Chief Information Officer

Office of Management and Budget

Office of Inspector General Budget Examiner