National Aeronautics and
Space Administration

Office of Inspector General
Washington, DC 20546-0001

November 16, 2010

TO: Jonathan Pettus
Chief Information Officer, Marshall Space Flight Center

Neil Rodgers
Deputy Chief Information Officer/NASA Enterprise Applications
Competency Center, Marshall Space Flight Center

FROM: Jim Morrison Jim Morrison
Assistant Inspector General for Audits

SUBJECT: Transmittal of the Final Report, "Information Technology Management Letter Comments," Prepared by Ernst & Young LLP in Connection with the Audit of NASA's Fiscal Year 2010 Financial Statements (IG-11-007-R; Assignment No. A-10-005-02)

The Office of Inspector General contracted with the independent public accounting firm Ernst & Young LLP (EY) to audit NASA's financial statements in accordance with the Government Accountability Office's *Government Auditing Standards* and Office of Management and Budget's Bulletin No. 07-04, "Audit Requirements for Federal Financial Statements," as amended.

As part of the NASA consolidated financial statement audit, EY performed procedures to assess the effectiveness of the information technology control environment (general and application controls) associated with NASA's core financial systems. Enclosed is the subject report, which contains the results of the assessment.

The Associate Director of Marshall Space Flight Center (MSFC) provided comments on the draft report, which were considered by EY when preparing the final report.

Management partially concurred with the two recommendations associated with the report's open findings. We will work with management to resolve these recommendations. MSFC concurred with the other two recommendations, which will be closed upon completion and verification of management's corrective actions.

EY is responsible for the enclosed report and the conclusions expressed therein. Accordingly, we do not express an opinion on NASA's financial statements, internal controls over financial reporting, or compliance with certain laws and regulations.

Enclosure Has Been Redacted for Public Release

We appreciate the courtesies extended during the assessment. If you have any questions, or need additional information, please contact Mark Jenson, Financial Management Director, Office of Audits, at 202-358-0629.

Enclosure

cc: Linda Cureton
NASA Chief Information Officer

Enclosure Has Been Redacted for Public Release

REDACTED FOR PUBLIC RELEASE

INFORMATION TECHNOLOGY MANAGEMENT LETTER COMMENTS

Prepared for:

National Aeronautics and Space Administration
Office of Inspector General
300 E Street, S.W.
Washington, D.C.

Prepared by:

Ernst & Young LLP
Information Technology Risk & Assurance
8484 Westpark Drive
McLean, VA 22102

Fiscal Year Ended September 30, 2010

Ernst & Young
Quality In Everything We Do

TABLE OF CONTENTS

INTRODUCTION

Ernst & Young LLP (EY) has completed its assessment of certain domains of the Information Technology (IT) Controls Assessment conducted during fiscal year (FY) 2010 at the National Aeronautics and Space Administration (NASA). The methodology used for the IT controls assessment was based on the United States Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM). The EY IT Risk and Assurance team conducted an IT General Controls Review (ITGCR) following FISCAM's six domains: Security Management (SM), Access Controls (AC), Configuration Management (CM), Segregation of Duties (SD), Contingency Planning (CP) and Application Controls (AS). The review was conducted as part of the audit of NASA's financial statements for the FY ended September 30, 2010.

NASA's Response

A draft of this report was provided to management for them to review and respond to the reportable findings and recommendations. EY obtained and reviewed NASA's responses to the findings. NASA management concurred with all of the findings except for the two noted below, which they partially concurred with:

- Access Control Finding #1; NASA management does not agree with the portion of the finding related to the SAP Oracle database. We agree with the fact that forcing the SAP account password to expire could cause the application to stop working. Furthermore, the manual control to change this account's password is considered an effective control. However, the finding pertains to all other SAP Oracle database accounts that currently do not enforce password expiration and have no implications in doing so. EY recommends that such database accounts be configured to systematically enforce password expiration.
- Access Control Finding #2; NASA management partially concurs with this finding and responded that there was a recertification process for MdM whereby all accounts expired annually and had to be revalidated through the NASA Account Management System (NAMS). However, EY validated that this control was not in place during our test procedures. Additionally, the recommendation specifies that the users and their access levels should be reviewed periodically for appropriateness. As the action plan in response to this finding is in the process of being implemented, EY would recommend a more frequent occurence than annually as an enhanced control.

In all other instances, NASA communicated that they have either remediated the condition or are conducting further research to determine a plan of action to mitigate the risk presented by the condition. EY considers the responses appropriate based on the reportable exceptions.

BACKGROUND

IT general controls are the policies, procedures, and practices that apply to all or a large segment of an entity's information systems to determine their proper operation. They impact the overall effectiveness and security of computer operations, rather than specific computer applications. IT general controls consist of the following critical elements:

- **Security Management controls** - to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls.

- **Access controls** - to limit or detect access to computer resources (data, program, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.

- **Configuration Management controls** - to prevent implementation of unauthorized programs or modifications to existing programs.

- **Segregation-of-duty controls** - to provide policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations and thereby conducting unauthorized actions or gaining unauthorized access to assets or records.

- **Contingency Planning controls** - to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected from destruction.

- **Application controls** – to ensure application software controls are properly configured to enforce management policies and procedures and to prevent users from bypassing key controls.

Vulnerability assessment procedures were designed to remotely (via internet) as well as locally (within NASA's Marshall Space Flight Center facilities) scan the designated targets and validate security configuration controls were in place to protect systems relevant to the financial statement audit. Our procedures included only non-destructive testing techniques (i.e., no files or data were modified or changed).

NASA FINANCIAL SYSTEMS OVERVIEW

The NASA Enterprise Applications Competency Center (NEACC) was created for an agency-wide transformation of NASA's business systems and processes to improve NASA's fiscal and management accountability.

The core financial system includes the following SAP modules: Standard General Ledger, Accounts Receivable, Accounts Payable, Purchasing, Cost Management, Materials Management and Integrated Asset Management Module (for NASA personal property). In addition to SAP, the NEACC is responsible for administering Metadata Manager (MdM), a subcomponent of the eBudget suite used to create and approve Work Breakdown Structure (WBS) elements that link the costs incurred/paid to the capital assets in Asset Accounting. Lastly, the Contractor Held Asset Tracking System (CHATS) application is managed by IT personnel at Goddard Space Flight Center (GSFC). This system is used by the top contractors (based on total value of their property balance) that are required to report their property balances on a monthly basis.

SCOPE

In connection with the audit of NASA's FY 2010 financial statements, we conducted an IT general controls review of the IT processes related to the financial systems noted above, which support business processes that are linked to significant cycles in the financial statements. The IT controls assessment was conducted based on the guidance promulgated in the GAO FISCAM and Financial Audit Manual (FAM).

A majority of administration activities for IT supporting the core financial module and MdM are performed at the NEACC; however, each center also performs certain control procedures related to access controls. These procedures include granting and terminating user access to the core financial module as well as managing network vulnerability assessments. We visited the following sites to test the IT security administration activities:

- Marshall Space Flight Center, including the NEACC, in Huntsville, AL;
- Langley Research Center in Hampton, VA;
- Johnson Space Center in Houston, TX; and
- Goddard Space Flight Center in Greenbelt, MD (to review CHATS).

EY also performed the following procedures:

- Followed-up on the FY 2009 audit findings
- Performed a limited vulnerability assessment to assess external and internal vulnerabilities
- Performed quarterly Journal Entry Computer Assisted Audit Techniques for the EY accounting team and;
- Reviewed the various GAO/Office of Inspector General (OIG) reports and considered the corresponding findings and needs for improvements.

SUMMARY OF FINDINGS

This section provides a brief summary of all findings noted during the current year audit as well as a status on FY 2009 findings. Note, the findings below do not include those identified through the penetration testing as they were communicated to management through a separate report prepared by EY and issued by the NASA OIG.

Overall, the findings in this document are separated into three sections:

1. **Open Findings** (detailed in Appendix A) are comprised of findings noted by EY in the current year, or in our follow-up on prior year findings, that were not resolved by NASA as of September 30, 2010. Either these findings are scheduled for resolution after September 30, 2010, or NASA has the recommendations under consideration.

2. **Resolved Findings** (detailed in Appendix B) are comprised of findings noted by EY in the current year and deemed resolved based on management's representation before September 30, 2010.

3. **Status of FY 2009 Findings** provides a synopsis on status of FY 2009 EY IT findings as of September 30, 2010.

In the past few years, we have noted a number of material weaknesses and significant deficiencies regarding the functioning of significant financial related controls at NASA. The level of risk associated with the IT issues noted below depends in part upon the extent to which financial related compensating controls (such as reconciliations and robust reviews of output) are in place and operating effectively during the audit period. Certain controls designed to detect errors or inappropriate processing may also not be executed in a manner that can be expected to identify errors which, while perhaps not material to the financial statements as a whole, may subject NASA to risks regarding safeguarding of assets. Within the context of overall weaknesses identified in the NASA control environment, the information technology related issues discussed below merit continued management focus.

It is noteworthy that NASA management has taken significant steps to resolve a majority of the FY 2009 findings.

A brief summary of the findings (open and resolved) as well as the status on FY 2009 findings is included below.

Open Findings

The following findings were noted during our fieldwork and have not been resolved as of September 30, 2010. The resolution of these issues is either scheduled for later than September 30, 2010, or NASA has the recommendations under consideration. For complete details of the open findings, refer to Appendix A.

Access Control (AC)

#	Condition
1	In performing a review of the Oracle database infrastructure supporting SAP and MdM, EY identified the following configuration settings that may not adequately protect the security of the database: [redacted]
2	Based on a review of the logical access user administration process for the MdM application, it was noted that a formal process is not in place to periodically recertify users at the application-level for appropriateness based on current job responsibilities.

Resolved Findings

This section is comprised of findings noted by EY in the current year and deemed resolved based on management's representation before September 30, 2010 (current year audit). For complete details of the resolved finding, refer to Appendix B.

Access Controls (AC)

#	Condition
3	In performing a review of the Windows 2003 infrastructure supporting the NASA Data Center (NDC) domain, EY identified more than 300 dormant accounts that were enabled and had not been logged into for more than 90 days.
4	In performing a review of the Oracle database infrastructure supporting CHATS, EY identified two privileged accounts [redacted] used by database administrators that are assigned the default profile. The default profile does not enforce strong password controls, such as maximum lifetime, minimum length, and account lockout.

Status of FY 2009 Findings

This section provides a synopsis on the status of FY 2009 EY findings as of September 30, 2010. The detailed follow-up on each FY 2009 finding is documented in a separate report to NASA OIG.

Access Control (AC)

#	Condition	Status
1	*External:* During EY's penetration testing into the Marshall Space Flight Center (MSFC) network from EY's penetration testing lab in Baltimore, Maryland, we noted a server that allowed access to the Documentum web application through auto-authentication. By accessing a particular file on the server, it was possible to view different Documentum applications. *Internal:* During EY's penetration testing into the MSFC network while being physically connected to the MSFC network, we found one web server running a GSFC web application which allowed access with no password. Finally, we discovered two Z/VM hosts that allowed access with passwords equivalent to the username. These hosts were only accessible through a web interface.	Partially Resolved[1]
2	During EY's penetration testing into the Marshall Space Flight Center (MSFC) network while being physically connected to the MSFC network, we found one Virtual Networking Computer (VNC) server running which allowed access with a password of "password". This host appeared to be a training computer.	Resolved
3	*External:* During EY's penetration testing into the Marshall Space Flight Center (MSFC) network from EY's penetration testing lab in Baltimore, Maryland, we noted five internet protocol (IP) addresses that redirected to a single web application called NASA Acquisition Internet Service (NAIS). This application had a feedback page that did not properly validate	Resolved

[1] A finding was noted in the current year penetration testing report related to the External portion of this condition. As previously noted, the results of the penetration testing were communicated to management in a separate report and are not included in the management letter.

#	Condition	Status
	input data. Since this application communicated with a back-end MySQL database and with the improper checks on user input, we were able to determine that application was vulnerable to an attack called Structured Query Language (SQL) injection. This web application was only viewable over Hypertext Transfer Protocol Secure (HTTPS) which means that all of the data, including an attack, would be encrypted. This implies that Network Intrusion Detection Systems (NIDS) would probably not be able to alert on this type of attack. Due to the defined scope of penetration testing which was performed in support of the financial statement audit, EY did not conduct a web application assessment so we could not determine if there are other web-based vulnerabilities within the NAIS application. *Internal:* During EY's penetration testing into the MSFC network while being physically connected to the MSFC network, we found the same NAIS web application and associated SQL injection vulnerability.	

Configuration Management (CM)

#	Condition	Status
4	During testing of the Contractor Held Asset Tracking System (CHATS) at Goddard Space Flight Center (GSFC), we were unable to determine a complete population of changes to the CHATS application. Although configuration management is done within Polytron Version Control System (PVCS), a complete population of changes could not be obtained nor relied upon due to dependence on manual entry.	Resolved

Appendix A – Detailed Open Findings

Access Control (AC)

Finding # 1

Condition
In performing a review of the Oracle database infrastructure supporting SAP and MdM, EY identified the following configuration settings that do not adequately protect the security of the database:

- [redacted]

While IT management has implemented a manual process to change the 'sapr3' account password on the database supporting SAP, this does not require the other database account passwords to be changed.

Cause
The MdM application and supporting infrastructure were inherited by the NEACC and as a result, the standard Oracle database configuration was not applied. As it relates to the SAP database, management does not rely on the systematic control to enforce password expiration. Instead, there is an automated Activity Request within the Remedy ticketing system to remind database administrators to change passwords every 60 days.

Criteria

Federal Information Security Management Act of 2002 (FISMA) requires that all automated information systems processing or storing sensitive information provide adequate security controls.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* Family: Identification and Authentication, IA-5: Authenticator Management addresses the following password requirements:

Control: The organization manages information system authenticators for users and devices by:

a) Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
b) Establishing initial authenticator content for authenticators defined by the organization;
c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e) Changing default content of authenticators upon information system installation;
f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
g) Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
h) Protecting authenticator content from unauthorized disclosure and modification; and

i) Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Control Enhancements (note: bolded items directly apply to this condition):
(1) The information system, for password-based authentication:

a) **Enforces minimum password complexity of** [Assignment: organization-defined requirements for case sensitivity, **number of characters**, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
b) Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created;
c) Encrypts passwords in storage and in transmission;
d) **Enforces password minimum and maximum lifetime restrictions** of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and
e) Prohibits password reuse for [Assignment: organization-defined number] generations.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* Family: Configuration Management, CM-6: Configuration Settings addresses the following configuration settings:

Control: The organization:
a) Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
b) Implements the configuration settings;
c) Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d) Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology," Section 20.2.1, states that "NASA shall ensure that all access controls identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented including, but not limited to:

> a. Implementing logical access controls on NASA systems and applications based on impact levels, policy, and permissions established by the management official responsible for the particular system, application, subordinate systems, or group of systems."

In addition, Section 2.3.5.2 of NPR 2810.1A, requires the information system security official to "periodically use tools to verify and/or monitor compliance with the NASA password policy for systems under their authority."

Effect
Not enforcing strong passwords and other security settings at the database-level could result in unauthorized access to financial data. However, the risk associated with this condition is minimized by the multiple layers of authentication required in order to gain

access to the production Oracle databases. A user must authenticate to the NASA Data Center (NDC) domain followed by the UNIX host.

Recommendation

We recommend that NEACC Oracle database administrators configure password, auditing, and default security configurations on the production SAP database to be in-line with the standard build documents and NIST SP 800-53 revision 3. In addition, we recommend that NEACC management treat inherited systems, such as MdM, similar to those built in-house and implement a process to assess key system configurations to ensure security settings are appropriate.

Finding # 2

Condition
Based on a review of the logical access user administration process for the Metadata Manager (MdM) application, it was noted that a formal process is not in place to periodically recertify users at the application-level for appropriateness based on current job responsibilities.

Cause
The current policy documents do not require the organization to perform a periodic review of users and their access levels for the MdM application. As a result, a user recertification process was never designed and implemented for MdM.

Criteria

Federal Information Security Management Act of 2002 (FISMA) requires that all automated information systems processing or storing sensitive information provide adequate security controls.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* Family: Access Control, AC-2: Account Management addresses the following password requirements:

Control: The organization manages information system accounts, including: (note: bolded items directly apply to this condition)

a) Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
b) Establishing conditions for group membership;
c) Identifying authorized users for the information system and specifying access privileges;
d) Requiring appropriate approvals for requests to establish accounts;
e) Establishing, activating, modifying, disabling, and removing accounts;
f) Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
g) Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to know/need-to-share changes;
h) Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
i) Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
j) Reviewing accounts [*Assignment: organization-defined frequency*].

NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology," Section 20.2.1, states that "NASA shall ensure that all access controls identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented."

Effect
Lack of a periodic access review could result in users retaining unnecessary, or inappropriate access. However, the risk that this condition could compromise NASA's

financial data is considered to be low because EY performed sample-based testing to validate the appropriateness of MdM users and did not identify any exceptions.

Recommendation

We recommend that NEACC management update their policy to include periodic user access reviews for the MdM application. In order to comply with the updated policy, MdM system administrators should implement a formal process to perform a user access recertification on a periodic basis (frequency to be defined by management).

[This page intentionally left blank]

Appendix B – Detailed Resolved Findings

Access Control (AC)

Finding # 3

Condition
In performing a review of the Windows 2003 infrastructure supporting the NASA Data Center (NDC) domain, EY identified more than 300 dormant accounts that were enabled and had not been logged into for more than 90 days.

Cause
NDC domain administrators do not have a process in place to identify and disable/remove dormant accounts. In this specific instance, the organization was undertaking a major network restructuring that involved moving the NASA center domains underneath one NASA domain. At the time of our testing, the domain accounts had not been cleaned up leading to the identification of this condition.

Criteria

Federal Information Security Management Act of 2002 (FISMA) requires that all automated information systems processing or storing sensitive information provide adequate security controls.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations*, Family: Access Control, AC-2: Account Management addresses the following password requirements:

Control: The organization manages information system accounts, including: (note: bolded items directly apply to this condition)

a) Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
b) Establishing conditions for group membership;
c) Identifying authorized users for the information system and specifying access privileges;
d) Requiring appropriate approvals for requests to establish accounts;
e) Establishing, activating, modifying, disabling, and removing accounts;
f) Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
g) Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to know/need-to-share changes;
h) Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
i) Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
j) Reviewing accounts [*Assignment: organization-defined frequency*].

Control Enhancements:
(3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology," Section 20.2.1, states that "NASA shall ensure that all access controls identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented."

Effect

The existence of dormant accounts on the NDC domain increases the risk that the accounts are compromised and unauthorized access may occur without detection. However, this condition does not directly compromise NASA's financial data because unauthorized access to the NDC domain does not grant the user access to the core financial systems due to layered security approach involving authentication controls at the network (password controls and Demilitarized Zone (DMZ) set up), and application level.

Recommendation

We recommend that NEACC domain administrators implement a process, whether automated or manual, to identify and disable dormant NDC domain accounts.

Finding # 4

Condition

In performing a review of the Oracle database infrastructure supporting CHATS, EY identified two privileged accounts [redacted] used by database administrators that are assigned the default password profile. The default password profile does not enforce strong password controls such as maximum lifetime, minimum length, and account lockout.

Cause

The privileged accounts in question were primarily used for exporting data using a datadump utility. As a result, the standard Oracle database password profile, which all other database accounts are set to, was not applied. Additionally, the [redacted] account is no longer required and can be removed from the database.

Criteria

Federal Information Security Management Act of 2002 (FISMA) requires that all automated information systems processing or storing sensitive information provide adequate security controls.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* Family: Identification and Authentication, IA-5: Authenticator Management addresses the following password requirements:

Control: The organization manages information system authenticators for users and devices by:

j) Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
k) Establishing initial authenticator content for authenticators defined by the organization;
l) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
m) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
n) Changing default content of authenticators upon information system installation;
o) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
p) Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
q) Protecting authenticator content from unauthorized disclosure and modification; and
r) Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Control Enhancements (note: bolded items directly apply to this condition):
(1) The information system, for password-based authentication:

f) **Enforces minimum password complexity of** [Assignment: organization-defined requirements for case sensitivity, **number of characters**, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

g) Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created;
h) Encrypts passwords in storage and in transmission;
i) **Enforces password minimum and maximum lifetime restrictions** of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and
j) Prohibits password reuse for [Assignment: organization-defined number] generations.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* Family: Configuration Management, CM-6: Configuration Settings addresses the following configuration settings:

Control: The organization:
e) Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
f) Implements the configuration settings;
g) Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
h) Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology," Section 20.2.1, states that "NASA shall ensure that all access controls identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented including, but not limited to:

> a. Implementing logical access controls on NASA systems and applications based on impact levels, policy, and permissions established by the management official responsible for the particular system, application, subordinate systems, or group of systems."

In addition, Section 2.3.5.2 of NPR 2810.1A, requires the information system security official to "periodically use tools to verify and/or monitor compliance with the NASA password policy for systems under their authority."

Effect
Not enforcing strong password settings for privileged accounts at the database-level could increase the risk in unauthorized access to financial data. However, the risk associated with this condition is minimized due to limited number of privileged account accompanied by the multiple layers of authentication required in order to gain access to the production Oracle database. A user must authenticate to the NASA Data Center (NDC) domain followed by the Linux host.

Recommendation
We recommend that GSFC Oracle database administrators configure the [redacted] account to be assigned the standard password profile, making it in-line with password control requirements defined in NIST SP 800-53 revision 3. Additionally, we recommend the [redacted] account be removed from the database if it is no longer required.