|  |
| --- |
| *Security Impact Analysis*  *Add missing health checks back – CHG0030251*  *August 2021*  *Version 1.0* |



Prepared by:  
Deloitte and Touche LLP

[Intentionally Left Blank]

DOCUMENT HISTORY

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete reissue of the entire document. A revision shall be made whenever the cumulative changes reach ten percent (10%) of this document’s content.

REVISION HISTORY

|  |  |
| --- | --- |
| Document Name | Security Impact Analysis |
| Version Number | V1.0 |
| Date Approved |  |
| Effective Date |  |
| Author | Deloitte |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Pages Affected** | **Description** |
| 1.0 | July 27, 2021 | Deloitte | All |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Introduction

**What is a Security Impact Analysis?**

In NIST SP 800-53 Rev. 4, a Security Impact Analysis (SIA) is defined as “The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.” The objective of performing the SIA is ***not*** to generate an SIA artifact (document), but to integrate the SIAinto the configuration (change) management process and into the system development lifecycle (SDLC). Hence, the purpose of this document is to capture the changes or new functionality affecting the security of a Ginnie Mae service in a relatively complete and consistent manner, and is required by the Federal guidance mentioned above.

This document is intended to identify the impact on security controls or security processes for new systems or proposed changes to existing Ginnie Mae services, applications, or processes. It should also be used to identify and document the addition or deletion of security controls or service attributes.

**When should a SIA be completed?**

The SIA should be completed for all new systems, system modifications, or changes going through the change control process to ensure changes do not create security issues. The SIA should be started before the *Requirements Analysis* phase for a given change.

**Who should complete the SIA?**

The SIA should be written and reviewed by a combination of the component’s stakeholders (e.g., Project Management Team, Engineers, Developers, Security, and Senior Management). Consulting with various stakeholders is an important part of a SIA and allows people to highlight security risks and solutions based on their own area of interest or expertise. Consultation is an important part of the SIA process, but it does not have to be a separate step. It can be built into all stages of the process.

**Where should the completed SIA be sent?**

A copy of the completed SIA should be sent to the point of contact (POC) on the Ginnie Mae Security Team via email to [GinnieMaeSecurityTeam@deloitte.com](mailto:GinnieMaeSecurityTeam@deloitte.com). The Security Team will review the SIA and submit it for final Ginnie Mae approval. The Security Team will determine what additional privacy documentation is required and advise accordingly.

\*\*\* This document should be treated as a formal submission to the body of documentation supporting this Ginnie Mae service or application. As such, this Security Impact Analysis may be subject to review and assessment not only by Ginnie Mae System Owners, Security Officers, and Authorizing Officials, but also by external assessors and auditors operating under Federal authority.

# General Information About the Project/System

|  |  |
| --- | --- |
| **System Name/ System ID Number:** | **DMC3 – Morpheus** |
| **Contractor’s Tracking ID:** | **CHG0030251** |
| **Proposed Implementation Date:** | **8/18/2021** |
| **Program Area:** | **CAMO** |
| **Program Area Manager/ Contact Information:** | **Michael Escobar (miescobar@deloitte.com)** |
| **System Owner/Contact Information:** | **HUD AWS** |
| **Project Leader/Contact Information:** | **Thuan Tran (ttran@morpheusdata.com)** |

|  |  |
| --- | --- |
| Provide a general description of the system, project or change including ALL additions, modifications, deletions: | |
|  | Requesting to Create missing health checks in Morpheus. Update new check in DB with the instance container ID and add check in Morpheus to instance monitor group.  This change will be happening in both the Morpheus DB and Morpheus UI. We are requesting to add a container ID to the monitor\_check table in the DB.  Secondly, for every instance in Morpheus there is a VM monitor check created. This consists of the Monitor check and the Group check associated with the instance. So on the Morpheus UI side we are creating the check and then adding the check to the instance check group so they are associated with the check. |

# Security Impact Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Select as Appropriate: | | | | |
|  |  | | New system/application | |
|  |  | | Change/deletion of an existing module | |
|  |  | | Creation of a new module | |
| Has the Ginnie Mae System Owner been notified of and approved the proposed changes? | | | | |
|  |  | | Yes If yes, date: [Insert date] | |
|  |  | | No | |
| Who/what department will be responsible for the application maintenance after implementation of the proposed changes? | | | | |
|  | | **Ginnie Mae Program Area:** | | **Deloitte Platform Team** |
|  | | **POC Name:** | | **Michael Escobar** |
|  | | **Title:** | | **Lead** |
|  | | **Telephone:** | | **(215) 239 – 2138** |
|  | | **Email:** | | **miescobar@deloitte.com** |

|  |  |  |
| --- | --- | --- |
| Who/what department will be responsible for the documentation, including hardware/software inventories, diagrams, and associated documentation after implementation of the proposed changes? | | |
|  | **POC Name:** | **Thuan Tran** |
|  | **Title:** | **Ginnie Mae O&M** |
|  | **Telephone:** | **(301) 518 - 9351** |
|  | **Email:** | **ttran@morpheusdata.com** |

# Security Impact Areas

In the section below, describe with as much detail as is necessary, the proposed changes to the service, application, or environment for each of the listed areas. If there is no applicable change for an area, please enter “None.”

The areas below are derived from NIST SP 800-37 Rev. 1 RMF TASK 6-1, “Determine the security impact of proposed or actual changes to the information system and its environment of operation.”

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| What environments are impacted by the change? | | | | | | | | |
|  | |  | | Production |  | Development | | |
|  | |  | | Disaster Recovery |  | Test | | |
|  | |  | | SIT |  | UAT | | |
|  | |  | | Other (please specify) [Add response here] | | | | |
| Is the Technical Lead and/or Project Lead aware of any potential security-related issues or challenges associated with this change? If so, briefly describe them or provide an attachment describing them. | | | | | | | | |
|  | |  | | Yes | | | |
|  | |  | | No | | | | |
|  | | If yes, briefly describe the potential security related issues or challenges.  [Add description here] | | | | | | |
| Are there changes to hardware or will additional hardware be required? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | Please list the infrastructure components used by this change and indicate whether it is existing within the system or new:  [List infrastructure components used here] | | | | | | |
| Are there changes to software or will additional software be required? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | Please list the software components used by this change and indicate whether it is existing within the system or new:  [List software components used here] | | | | | | |
| Are there changes to any ports, protocols or services? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | Please list the ports, protocols and services used by this change and indicate whether they are existing within the system or new: | | | | | | |
| Are there changes to firmware? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | Please list the firmware components used by this change and indicate whether it is existing within the system or new:  [List firmware components used here] | | | | | | |
| Are there changes to features? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | If yes, please list the changes: | | | | | | |
| Are there changes to hosting networks or hosting facilities? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | If yes, please list the changes: | | | | | | |
| Are there changes to user roles or permissions for the system? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | If yes, please list the changes:  [List changes here] | | | | | | |
| Are there changes to the mission or business use of the system? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | If yes, please list the changes:  [List changes here] | | | | | | |
| Are there changes in the threat threshold? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | If yes, please list the changes:  [List changes here] | | | | | | |
| Are there changes in the organization risk strategy? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | If yes, please list the changes:  [List changes here] | | | | | | |
| Are there changes to the security state of the system, service, or environment? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | If yes, please list the changes:  [List changes here] | | | | | | |
| Change Types Please review the list of Change Types below. In the second column, mark each applicable change. Provide a brief explanation of why applicable change types are selected in the third column. The changes are not intended to be mutually exclusive, so multiple change types may be selected for a single initiative/release. If none of the change types are applicable, please mark “Other change” and provide a description of the change in the third column. | | | | | | | | |
|  |  | | **Change Type** | | **Applicable** | | **Explanation (If Applicable)** | |
|  |  | | New network device(s) (e.g., router, switch, firewall, VPN gateway) | |  | |  | |
|  |  | | New Server | |  | |  | |
|  |  | | Other new hardware | |  | |  | |
|  |  | | Decommissioning of hardware | |  | |  | |
|  |  | | New Virtual Server | |  | |  | |
|  |  | | New OS | |  | |  | |
|  |  | | New COTS application | |  | |  | |
|  |  | | Upgrade/Patch of COTS application | |  | |  | |
|  |  | | New custom application | |  | |  | |
|  |  | | Upgrade/bug fix of existing application | |  | |  | |
|  |  | | New database (e.g. Microsoft SQL Server or Oracle) | |  | |  | |
|  |  | | Upgrade of existing database (e.g. Oracle 11g to 12c) | |  | |  | |
|  |  | | Addition of new database instance | |  | |  | |
|  |  | | Modification of an existing database instance (e.g., changes to a table) | |  | | **Updating Morpheus DB to add proper monitoring flag for instances created via Morpheus UI.** | |
|  |  | | New or upgraded middleware application or service | |  | |  | |
|  |  | | Modifications to ports, protocols, and services used or provided by the system | |  | |  | |
|  |  | | Changes intended to address security requirements or improve/modify the security of the system (e.g., cryptographic modules, security patch, authentication, authorization, role changes) | |  | |  | |
|  |  | | New information type processed, stored, or transmitted on the system | |  | |  | |
|  |  | | Interface changes (addition/removal) | |  | |  | |
|  |  | | Change of location | |  | |  | |
|  |  | | Other Change | |  | |  | |
| Have changes to the components (software, hardware, firmware and application changes) been appropriately authorized, tested, validated, approved, and documented? | | | | | | | | |
|  | |  | | Yes | | | | |
|  | |  | | No | | | | |
|  | | We are currently waiting for Security and Client to approve this change | | | | | | |
| Purpose Specification and Minimization of Personally Identifiable Information | | | | | | | | |
|  | | Describe the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices as part of this implementation.  No PII involved with this change. | | | | | | |
|  | | Identify the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection.  No PII involved with this change. | | | | | | |
|  | | How will the collection and retention of PII be limited to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent as part of this implementation?  No PII involved with this change. | | | | | | |
| Access Control for Sensitive and Financially Sensitive Information | | | | | | | | |
|  | | Describe how PII, sensitive, and financially sensitive information is limited to only those who are authorized to view the information.  No PII involved with this change. | | | | | | |
|  | |  | |  | | | | |

# Security Control Documentation Impact

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Have the following documents been reviewed and updated as part of this implementation?** | | | | |
| 4.1 | Yes | No |  | Configuration Management Plan (CMP)  [Add comments here] |
| 4.2 | Yes | No |  | Baseline Configuration  [Add comments here] |
| 4.3 | Yes | No |  | Information System Contingency Plan (ISCP)  [Add comments here] |
| 4.4 | Yes | No |  | System Security Plan (SSP)  [Add comments here] |
| 4.5 | Yes | No |  | Risk Assessment (RA)  [Add comments here] |
| 4.6 | Yes | No |  | Privacy Impact Assessment (PIA)  [Add comments here] |
| 4.7 | Yes | No |  | e-Authentication Plan (eAuth)  [Add comments here] |
| 4.8 | Yes | No |  | Federal Information Processing Standards (FIPS 199)  [Add comments here] |
| 4.9 | Yes | No |  | Business Requirements Definition Document  [Add comments here] |
| 4.10 | Yes | No |  | Requirements Traceability Matrix  [Add comments here] |
| 4.11 | Yes | No |  | Solution Architecture Design  [Update L3/L4 diagrams to reflect the change request] |
| 4.12 | Yes | No |  | Technical Design Document  [Update L3/L4 diagrams to reflect the change request] |
| 4.13 | Yes | No |  | Interface Control Document  [Add comments here] |
| 4.14 | Yes | No |  | Capacity Plan  [Add comments here] |
| 4.15 | Yes | No |  | Data Conversion Plan  [Add comments here] |
| 4.16 | Yes | No |  | Release Plan  [Add comments here] |
| 4.17 | Yes | No |  | Implementation Plan  [Add comments here] |
| 4.18 | Yes | No |  | Test Plan  [Add comments here] |
| 4.19 | Yes | No |  | Data Management Plan  [Add comments here] |

# Security Controls Impact

In NIST SP 800-37 Rev. 1 RMF Task 6.1, organizations are advised that “assessing the potential impact [that] changes may have on the security state of the system or the organization is an important aspect of security control monitoring.”

For each of the impacted NIST SP 800-53 Rev. 4 controls and control categories, provide the NIST Control ID, the name, and a description of the manner by which each pertinent control is impacted by change(s) proposed in this document.

| ID # | Control Reference | Impact Level | Impact Description | Responsible Party | | Components Affected (i.e. Hardware, Software, System, Subsystem, Module) | Recommended Corrective Action to be Taken |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Example** | | | | | | | |
| *RFS-1* | *NIST SP 800-53 AC-2: Account Management* | *Mod* | *Lack of standardized account management process increases the probability that users will be given more access than necessary.* | | *O&M Team* | *Software, System, Subsystem/Module* | *Create standardized account management process.* |
| **Access Control** | | | | | | | |
| Will change(s) to system affect how the system limits: (i) information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems); and (ii) the types of transactions and functions that authorized users are permitted to exercise? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Awareness and Training** | | | | | | | |
| Will change(s) affect required system training to ensure that personnel are adequately trained to carry out their assigned information security related duties and responsibilities? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Audit and Accountability** | | | | | | | |
| Will change(s) affect how system audit requirements to (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Security Assessment and Authorization** | | | | | | | |
| Will change(s) affect the system boundary or require a security assessment? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Change Management** | | | | | | | |
| Will change(s) to the system impact the (i) baseline configuration and inventory of organizational information systems; (ii) establishment and enforcement of security configuration settings; and (iii) ability to monitor and control changes to the baseline configurations and to the constituent components of the systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycle? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Contingency Planning** | | | | | | | |
| Will change(s) affect contingency planning efforts? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Identification and Authentication** | | | | | | | |
| Will change(s) to the system impact how it (i) identifies users, processes acting on behalf of users, or devices; and (ii) authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Maintenance** | | | | | | | |
| Will change(s) to the system impact how (i) periodic and timely maintenance is performed; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Media Protection** | | | | | | | |
| Will change(s) to the system impact how (i) information contained in the system in printed form or on digital media is protected; (ii) access to information in printed form or on digital media removed from the system is limited to authorized users; and (iii) how digital media is sanitized or destroyed before disposal or release for reuse? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Physical and Environmental Protection** | | | | | | | |
| Will change(s) to the system/system environment change how (i) physical access to information systems, equipment, and the respective operating environments is limited to authorized individuals; (ii) the physical plant and support infrastructure for information systems is protected; (iii) supporting utilities for information systems are provided; (iv) and (v) appropriate environmental controls in facilities are provided? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Risk Assessment** | | | | | | | |
| Will change(s) affect the risk level? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Systems and Communications Protection** | | | | | | | |
| Will change(s) to the system affect how: (i) communications (i.e., information transmitted or received by organizational information systems) are monitored, controlled, and protected at the external boundaries and key internal boundaries of the information systems; and (ii) architectural designs, software development techniques, and systems engineering principles that promote effective information security are implemented? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Systems and Information Integrity** | | | | | | | |
| Will change(s) to the system affect how (i) system flaws are identified, reported, and corrected in a timely manner; (ii) malicious code protection is employed; (iii) system events are monitored and detected; (iv) the correct operation of security functions is verified; and (v) information is checked for accuracy, completeness, validity, and authenticity? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **Privacy** | | | | | | | |
| Will change(s) affect sensitive data, including PII? | | | | | | | |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |

# Potential Impacts

In the following table, indicate the potential impact for each item as High, Medium, or Low. Please check the suitable cell for each possible impact. Do not skip or delete any existing entries in the table. Each item requires a rating. Preparers may add additional possible impacts at the end of the table if required.

|  |  |  |  |
| --- | --- | --- | --- |
| **Description of Possible Impacts On Service or System** | **Probability** | | |
| **High** | **Medium** | **Low** |
| May cause one or more outages exceeding contractual obligations. |  |  |  |
| May cause an abnormal recovery process and recovery timeframe. |  |  |  |
| May require an increase in staff or other resources for an ongoing period of time. |  |  |  |
| May require additional user support. |  |  |  |
| Other (additional rows provided for use if necessary). |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Authorization Actions

In the following table, indicate the authorization action(s) required for the actual or proposed change(s) to this service or system.

Please check the suitable cell for “Required” or “Not Required.” Do not skip or delete any existing entries. Each item requires a response. Preparers may add additional possible authorization actions at the end of the table if required.

|  |  |  |
| --- | --- | --- |
| Action | Required | Not Required |
| New security authorization. |  |  |
| New network vulnerability assessment(s) (NVA). |  |  |
| New remote/onsite application security assessment(s) (R/OASA). |  |  |
| Update plan of action and milestones (POA&Ms). |  |  |
| Conduct new site or facility assessment. |  |  |
| Prepare decommissioning plan and documents. |  |  |
| Provide new assessment artifacts. |  |  |
| Other (additional rows provided for use if necessary). |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# SIA Determination

|  |
| --- |
| I have carefully assessed the Security Impact Assessment (SIA) for [Insert Name of system/project here]. Based on my authority and judgment, the data captured in this document is current and accurate. |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | MANAGEMENT DECISION - Please check the appropriate statement.   |  |  |  | | --- | --- | --- | |  |  | The document is accepted. | |  |  | The document is accepted pending the changes noted. | |  |  | The document is not accepted. |  |  |  |  | | --- | --- | --- | | Troy Icenhour |  | Date | | Technology Management Division Director  Office of Enterprise Data & Technology Solutions |  |  | |  |  |  | | Daniel L. Boling, Technology Management Director |  | Date | | Office of Enterprise Data and Technology Solutions  Infrastructure and System Owner | | | |  |  |  | | John E. Crump  Chief Information Security Officer  Office of Enterprise Risk |  | Date | |  |  |  | |  |  |  | | | |