TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 06/30/2023 | 1.0 | All | Initial publication. | FedRAMP PMO |
|  |  |  |  |  |

**How to contact us**

For questions about FedRAMP, or for questions about this document including how to use it, contact [info@FedRAMP.gov.](mailto:info@FedRAMP.gov)

For more information about FedRAMP, see [www.FedRAMP.gov](http://www.fedramp.gov).

Delete this Template Revision History page and all other instructional text from your final version of this document.

## Appendix Q <CSO Name> Encryption Implementation Status

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Data in Transit (DIT) | | | | | | | | | | |
|  | Source | | | | Destination | | | | |  |
| **Ref #** | **Areas of DIT[[1]](#footnote-1)** | **CMVP #[[2]](#footnote-2)** | **CM Vendr** | **Module Name** | **Areas of DIT** | **CMVP #[[3]](#footnote-3)** | **CM Vendor** | **Module Name** | **Usage** | **Notes[[4]](#footnote-4)** |
| 1 | NGINX Server  <Use Case Example - Please Delete> | **#4271**    Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Red Hat, Inc. | RHEL 8 OpenSSL | All Application Servers | **#3980**    Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Canonical Ltd. | Ubuntu 18.04 OpenSSH Server | Load Balancer TLS to Application Server  TLS 1.1 or earlier  TLS 1.2  TLS 1.3  Other \_\_\_\_\_\_\_\_ |  |
| 2 | All Application Servers  <Use Case Example - Please Delete> | None    Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | CentOS 7.9 | OpenSSL 1.0.1 | PostgreSQL | **#3980**    Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Canonical Ltd. | Ubuntu 18.04 OpenSSH Server | Application servers to common DB  TLS 1.1 or earlier  TLS 1.2  TLS 1.3  Other \_\_\_\_\_\_\_\_ | Plans to move to RHEL 8. See POA&M ID 111. |
| 3 | Container traffic  <Use Case Example - Please Delete> | **#3678**    Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Google | BoringCrypto | Container traffic | **#3678**    Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Google | BoringCrypto | Istio Tetrate service mesh  TLS 1.1 or earlier  TLS 1.2  TLS 1.3  Other \_\_\_\_\_\_\_\_ |  |
| # | *<Fill In>*  *<Copy and Paste this Row to Complete>* | *<Fill In and Select Below>*  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | *<Fill In>* | *<Fill In>* | *<Fill In>* | *<Fill In and Select Below>*  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | *<Fill In>* | *<Fill In>* | *<Fill In and Select Below>*  TLS 1.1 or earlier  TLS 1.2  TLS 1.3  Other \_\_\_\_\_\_\_\_ |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Data at Rest (DAR) | | | | | | | |
| **Ref #** | **Areas of DAR[[5]](#footnote-5)** | **CMVP # [[6]](#footnote-6)** | **CM Vendor Name** | **Module Name** | **Usage** | **Encryption Type** | **Notes[[7]](#footnote-7)** |
| 1 | PostgreSQL database  <Use Case Example - Please Delete> | **#3980**  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Canonical Ltd. | Ubuntu 18.04 OpenSSL Cryptographic Module | Volume encryption | Full disk  File  Record  None  Other \_\_\_\_\_\_\_\_ |  |
| 2 | App server local storage  <Use Case Example - Please Delete> | **#2931**  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Microsoft | Windows Server 2016 | OS and application binaries | Full disk  File  Record  None  Other \_\_\_\_\_\_\_\_ | CM is Historical, per NIST CMVP. Plans to move to Windows 2019 upon Active FIPS-140-validation achieved. See POA&M ID 123. |
| 3 | S3 buckets  <Use Case Example - Please Delete> | **#4177**  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | AWS | Key Management Service (KMS) HSM | Server-side encryption with KMS keys (SSE-KMS) used to encrypt bucket | Full disk  File  Record  None  Other \_\_\_\_\_\_\_\_ |  |
| 4 | [**Hashicorp Vault Enterprise**](https://developer.hashicorp.com/vault/docs/enterprise/fips/fips1402) credential storage  <Use Case Example - Please Delete> | **#3678**  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Google | BoringCrypto | Storing customer and system keys and passwords | Full disk  File  Record  None  Other \_\_\_\_\_\_\_\_ |  |
| 5 | *<Fill In>*  *<Copy and Paste this Row to Complete>* | *<Fill In and Select Below>*  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | *<Fill In>* | *<Fill In>* | *<Fill In>* | *<Select Below>*  Full disk  File  Record  None  Other \_\_\_\_\_\_\_\_ | *<Fill In>* |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Other (Hashes, Digital Signatures, MFA, etc.) | | | | | | | |
| **Ref #** | **Areas of Use[[8]](#footnote-8)** | **CMVP #[[9]](#footnote-9)** | **CM Vendor Name** | **Module Name** | **Usage** | **Encryption Type** | **Notes[[10]](#footnote-10)** |
| 1 | MFA  *<Use Case Example - Please Delete>* | **#3907**    Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Yubico | Yubikey | Hard token TOTP code generations |  |  |
| # | *<Fill In>*  *<Use Case Example - Please Delete>* | *<Fill In and Select Below>*  Embedded CM  Third-party CM  Uses OS CM  In FIPS Mode  Other  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | *<Fill In>* | *<Fill In>* | *<Fill In>* | *<Fill In>* | *<Fill In>* |

1. Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located. [↑](#footnote-ref-1)
2. If using cryptography that lacks FIPS validation, state “No FIPS”. If unencrypted, state “Unencrypted”. [↑](#footnote-ref-2)
3. If using cryptography that lacks FIPS validation, state “No FIPS”. If unencrypted, state “Unencrypted”. [↑](#footnote-ref-3)
4. For example, specify if the historical CM is used or the store lacks encryption entirely. Include the related POA&M ID, remediation plans, etc. [↑](#footnote-ref-4)
5. Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located. [↑](#footnote-ref-5)
6. If using cryptography that lacks FIPS validation, state “No FIPS”. If unencrypted, state “Unencrypted”. [↑](#footnote-ref-6)
7. For example, specify if the historical CM is used or the store lacks encryption entirely. Include the related POA&M ID, remediation plans, etc. [↑](#footnote-ref-7)
8. Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located. [↑](#footnote-ref-8)
9. If using cryptography that lacks FIPS validation, state “No FIPS”. If there is no cryptography, state “No Crypto”. [↑](#footnote-ref-9)
10. For example, specify if the historical CM is used or it lacks cryptography entirely. Include the related POA&M ID, remediation plans, etc. [↑](#footnote-ref-10)