# CNCF Core Infrastructure Initiative

This document normatively details tremor project best-practices which is founded on the Cloud Native Compute Foundation’s Core Infrastructure Initiative’s Best Practices.

## Basics

### Identification

**What is the human-readable name of the project?**

Tremor Event Processing System

**What is a brief description of the project?**

Tremor

**What is the URL for the project (as a whole)?**

https://github.com/wayfair-incubator/tremor-runtime

**What is the URL for the version control repository (it may be the same as the project URL)?**

https://github.com/wayfair-incubator/tremor

**What programming language(s) are used to implement the project?**

Rust Erlang Python

**What is the Common Platform Enumeration (CPE) name for the project (if it has one)?**

N/A TBD We should follow the CPE process at NIST – https://nvd.nist.gov/products/cpe

### Basic project website content

**The project website MUST succinctly describe what the software does (what problem does it solve?).**

Met

**The project website MUST provide information on how to: obtain, provide feedback (as bug reports or enhancements), and contribute to the software.**

Met. https://github.com/wayfair-incubator/tremor-runtime/issues

**The information on how to contribute MUST explain the contribution process (e.g., are pull requests used?) (URL required)**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/contributions.md

**The information on how to contribute SHOULD include the requirements for acceptable contributions (e.g., a reference to any required coding standard). (URL required)**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/patches.md

### FLOSS license

**What license(s) is the project released under?**

ASL-2.0

**The software produced by the project MUST be released as FLOSS.**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/LICENSE

**It is SUGGESTED that any required license(s) for the software produced by the project be approved by the Open Source Initiative (OSI).**

Met. The ASL-2.0 license is approved by the Open Source Initiative (OSI).

**The project MUST post the license(s) of its results in a standard location in their source repository. (URL required)**

Met. The license (ASL-2.0) in in the file LICENSE, see https://github.com/wayfair-incubator/tremor-runtime/tree/master/LICENSE

### Documentation

**The project MUST provide basic documentation for the software produced by the project.**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs

**The project MUST provide reference documentation that describes the external interface (both input and output) of the software produced by the project.**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/api

### Other

**The project sites (website, repository, and download URLs) MUST support HTTPS using TLS.**

Met.

**The project MUST have one or more mechanisms for discussion (including proposed changes and issues) that are searchable, allow messages and topics to be addressed by URL, enable new people to participate in some of the discussions, and do not require client-side installation of proprietary software.**

Met.

**The project SHOULD provide documentation in English and be able to accept bug reports and comments about code in English.**

Met.

## Change Control

### Public version-controlled source repository

**The project MUST have a version-controlled source repository that is publicly readable and has a URL.**

Met. https://github.com/wayfair-incubator/tremor-runtime.git

**The project’s source repository MUST track what changes were made, who made the changes, and when the changes were made.**

Met. https://github.com/wayfair-incubator/tremor-runtime.git

**To enable collaborative review, the project’s source repository MUST include interim versions for review between releases; it MUST NOT include only final releases.**

Met. https://github.com/wayfair-incubator/tremor-runtime.git

**It is SUGGESTED that common distributed version control software be used (e.g., git) for the project’s source repository.**

Met. https://github.com/wayfair-incubator/tremor-runtime.git

### Unique version numbering

**The project results MUST have a unique version identifier for each release intended to be used by users.**

Met. The project follows [Semantic Versioning](https://semver.org/) (SemVer) format

**It is SUGGESTED that projects identify each release within their version control system. For example, it is SUGGESTED that those using git identify each release using git tags.**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/release.md

**The project MUST provide, in each release, release notes that are a human-readable summary of major changes in that release to help users determine if they should upgrade and what the upgrade impact will be. The release notes MUST NOT be the raw output of a version control log (e.g., the “git log” command results are not release notes). Projects whose results are not intended for reuse in multiple locations (such as the software for a single website or service) AND employ continuous delivery MAY select “N/A”. (URL required)**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/CHANGELOG.md

**The release notes MUST identify every publicly known vulnerability with a CVE assignment or similar that is fixed in each new release, unless users typically cannot practically update the software themselves. If there are no release notes or there have been no publicly known vulnerabilities, choose “not applicable” (N/A).**

Met.

## Reporting

### Bug-reporting process

**The project MUST provide a process for users to submit bug reports (e.g., using an issue tracker or a mailing list). (URL required)**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/reporting-bugs.md

**The project SHOULD use an issue tracker for tracking individual issues.**

Met. https://github.com/wayfair-incubator/tremor-runtime/issues

**The project MUST acknowledge a majority of bug reports submitted in the last 2-12 months (inclusive); the response need not include a fix.**

Met.

**The project SHOULD respond to a majority (>50%) of enhancement requests in the last 2-12 months (inclusive).**

Met. It is up to contributors to submit enhancement requests via the RFP process. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/rfp.md

**The project MUST have a publicly available archive for reports and responses for later searching.**

Met. All requests, reports and responses are gated via the issue tracking system. https://github.com/wayfair-incubator/tremor-runtime/issues

### Vulnerability report process

**The project MUST publish the process for reporting vulnerabilities on the project site. (URL required)**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/reporting-bugs.md and https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/security-bugs.md

**If private vulnerability reports are supported, the project MUST include how to send the information in a way that is kept private. (URL required)**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/reporting-bugs.md and https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/security-bugs.md

**The project’s initial response time for any vulnerability report received in the last 6 months MUST be less than or equal to 14 days.**

Met.

## Quality

### Working build system?

**If the software produced by the project requires building for use, the project MUST provide a working build system that can automatically rebuild the software from source code.**

Met.

**It is SUGGESTED that common tools be used for building the software.**

Met.

**The project SHOULD be buildable using only FLOSS tools.**

Met. The project primarily uses FLOSS tooling with the exception of EQC which we used for random stochastic property based testing.

### Automated test suite

**The project MUST use at least one automated test suite that is publicly released as FLOSS (this test suite may be maintained as a separate FLOSS project).**

Met. https://github.com/wayfair-incubator/tremor-runtime/actions

**A test suite SHOULD be invocable in a standard way for that language.**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/running-tests.md

**It is SUGGESTED that the test suite cover most (or ideally all) the code branches, input fields, and functionality.**

Met. The project uses a combination of unit, functional, benchmark, integration and specialized ( EQC ) tests

**It is SUGGESTED that the project implement continuous integration (where new or changed code is frequently integrated into a central code repository and automated tests are run on the result).**

Met. https://github.com/wayfair-incubator/tremor-runtime/actions and TBD-eqc-runner-public-url

### New functionality testing

**The project MUST have a general policy (formal or not) that as major new functionality is added to the software produced by the project, tests of that functionality should be added to an automated test suite.**

Met. https://github.com/wayfair-incubator/tremor-runtime/tree/master/docs/development/process/rfp.md

**The project MUST have evidence that the test policy for adding tests has been adhered to in the most recent major changes to the software produced by the project.**

Met.

**It is SUGGESTED that this policy on adding tests (see test policy) be documented in the instructions for change proposals.**

Met.

### Warning flags

**The project MUST enable one or more compiler warning flags, a “safe” language mode, or use a separate “linter” tool to look for code quality errors or common simple mistakes, if there is at least one FLOSS tool that can implement this criterion in the selected language.**

Met. The project enables all warnings and enforces strict / pendantic checks on code style, format. These are constraints and limitations are enforced by the build and continuous integration systems.

**The project MUST address warnings.**

Met.

**It is SUGGESTED that projects be maximally strict with warnings in the software produced by the project, where practical.**

Met.

### Security

**The project MUST have at least one primary developer who knows how to design secure software. (See ‘details’ for the exact requirements.)**

Met.

**At least one of the project’s primary developers MUST know of common kinds of errors that lead to vulnerabilities in this kind of software, as well as at least one method to counter or mitigate each of them.**

Met.

### Use basic good cryptographic practices

**The software produced by the project MUST use, by default, only cryptographic protocols and algorithms that are publicly published and reviewed by experts (if cryptographic protocols and algorithms are used).**

Met. The project does not provide bespoke cryptographic protocols, algorithms or methods of its own. The project calls on specifically designed externally provided cryptographic methods.

**If the software produced by the project is an application or library, and its primary purpose is not to implement cryptography, then it SHOULD only call on software specifically designed to implement cryptographic functions; it SHOULD NOT re-implement its own.**

Met. The project does not provide bespoke cryptographic protocols, algorithms or methods of its own. The project calls o specifically designed externally provided cryptographic methods.

**All functionality in the software produced by the project that depends on cryptography MUST be implementable using FLOSS.**

Met.

**The security mechanisms within the software produced by the project MUST use default keylengths that at least meet the NIST minimum requirements through the year 2030 (as stated in 2012). It MUST be possible to configure the software so that smaller keylengths are completely disabled.**

Met.

**The default security mechanisms within the software produced by the project MUST NOT depend on broken cryptographic algorithms (e.g., MD4, MD5, single DES, RC4, Dual\_EC\_DRBG), or use cipher modes that are inappropriate to the context, unless they are necessary to implement an interoperable protocol (where the protocol implemented is the most recent version of that standard broadly supported by the network ecosystem, that ecosystem requires the use of such an algorithm or mode, and that ecosystem does not offer any more secure alternative). The documentation MUST describe any relevant security risks and any known mitigations if these broken algorithms or modes are necessary for an interoperable protocol.**

Met.

**The security mechanisms within the software produced by the project SHOULD implement perfect forward secrecy for key agreement protocols so a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.**

Met.

**If the software produced by the project causes the storing of passwords for authentication of external users, the passwords MUST be stored as iterated hashes with a per-user salt by using a key stretching (iterated) algorithm (e.g., PBKDF2, Bcrypt or Scrypt).**

Met.

**The security mechanisms within the software produced by the project MUST generate all cryptographic keys and nonces using a cryptographically secure random number generator, and MUST NOT do so using generators that are cryptographically insecure.**

### Secured delivery against min-in-the-middle (MITM) attacks

**The project MUST use a delivery mechanism that counters MITM attacks. Using https or ssh+scp is acceptable.**

Met.

**A cryptographic hash (e.g., a sha1sum) MUST NOT be retrieved over http and used without checking for a cryptographic signature.**

Met.

### Publicly known vulnerabilities fixed

**There MUST be no unpatched vulnerabilities of medium or higher severity that have been publicly known for more than 60 days.**

Met.

**Projects SHOULD fix all critical vulnerabilities rapidly after they are reported.**

Met.

### Other security issues

**The public repositories MUST NOT leak a valid private credential (e.g., a working password or private key) that is intended to limit public access.**

Met.

## Analysis

### Static code analysis

**At least one static code analysis tool (beyond compiler warnings and “safe” language modes) MUST be applied to any proposed major production release of the software before its release, if there is at least one FLOSS tool that implements this criterion in the selected language.**

Met.

**It is SUGGESTED that at least one of the static analysis tools used for the static\_analysis criterion include rules or approaches to look for common vulnerabilities in the analyzed language or environment.**

Met.

**All medium and higher severity exploitable vulnerabilities discovered with static code analysis MUST be fixed in a timely way after they are confirmed.**

Met.

**It is SUGGESTED that static source code analysis occur on every commit or at least daily.**

Met.

### Dynamic code analysis

**It is SUGGESTED that at least one dynamic analysis tool be applied to any proposed major production release of the software before its release.**

Met.

**It is SUGGESTED that if the software produced by the project includes software written using a memory-unsafe language (e.g., C or C++), then at least one dynamic tool (e.g., a fuzzer or web application scanner) be routinely used in combination with a mechanism to detect memory safety problems such as buffer overwrites. If the project does not produce software written in a memory-unsafe language, choose “not applicable” (N/A).**

Met.

**It is SUGGESTED that the software produced by the project include many run-time assertions that are checked during dynamic analysis.**

Met.

**All medium and higher severity exploitable vulnerabilities discovered with dynamic code analysis MUST be fixed in a timely way after they are confirmed.**

Met.