Earth System Grid Federation (ESGF)

Software Security Plan

Issue Date: 10-Feb-2016
Effective Date: 13-Apr-2016

Verify that this is the correct revision before use.

THIS PAGE INTENTIONALLY LEFT BLANK

ESGF Software Security Plan – Review and Approval

This Security Plan for the Earth System Grid Federation was prepared for the exclusive use of ESGF and in particular its sites and developers.

I have reviewed and concur with the contents of this plan.

Approved by/Date: _____13April2016_____
Dean N. Williams, DOE
ESGF Chair

Approved by/Date: _____13April2016_____
Michael Lautenschlager, DKRZ
ESGF Co-Chair

Approved by/Date: _____13April2016_____
Sebastien Denvil, IPSL
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
Martin Juckes, STFC
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
Luca Cinquini, NASA/NOAA
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
Robert Ferraro, NASA
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
Daniel Q. Duffy, NASA
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
Cecilia DeLuca, NOAA
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
V. Balaji, NOAA
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
Ben Evans, NCI
ESGF Executive Committee Member

Approved by/Date: _____13April2016_____
Claire Trenham, NCI
ESGF Executive Committee Member

Revision History

Date (MM/DD/YYYY)	Identifier (YYYY.revision#)	Author (Name/ID)	Change Description	Document Owner (Name/email)
01/30/2016	2016.01.20	George Rumney/NASA	Initial document draft.	George Rumney george.rumney@nasa.gov
02/10/2016	Draft Version 14	NASA NCCS	Updated draft.	George Rumney george.rumney@nasa.gov
04/13/2016	Version 1.0	George Rumney/NASA	XC approval of final draft.	George Rumney george.rumney@nasa.gov

Table of Contents

Background

The primary purpose of this security plan is to prepare for both major and minor Earth System Grid Federation (ESGF) software releases within the context of the ESGF Software Development Life Cycle (SDLC). This plan's emphasis is on the "release" phase of a typical SDLC and its pre-requisites but depends upon development and maintenance (design and build) aspects of the SDLC as well.

SDLC phases prior to a software release:

- Requirements definition;
- Design (including secure coding practices and threat modeling);
- Implementation; and
- Verification (including security testing).

The release phase of the ESGF SDLC shall include the following:

- Inventory update;
- Change documentation;
- Security Review (minor | major);
- Issue resolution; and
- Certification of release.

In order to implement effective IT security for ESGF the ESGF Executive Committee shall charter and oversee a Software Security Working Team (SSWT) whose duties shall emphasize the release procedures as well as helping to guide ESGF along a continuous improvement path to a more secure "to-be" methodology and architecture.

Federal Information Security Management Act (FISMA) Controls: SA-3, SA-8.

Roles and Responsibilities

ESGF Executive Committee

- Ensure that the ESGF software security plan is agreed upon, signed, and followed by all sites.
- Charter and oversee the ESGF Software Security Working Team (SSWT)
- Define an ESGF Risk Executive function as an adjunct to the ESGF Executive Committee
    - Reference: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
    - The ESGF Risk Executive shall be independent of the SSWT and have signatory authority over the formal submissions made by the SSWT

(e.g., risk assessment, "to-be" architecture, plans of actions and milestones, etc.)

ESGF Software Development Team led by Lawrence Livermore National Laboratory (LLNL)

Governance:

- Define roles and responsibilities at the federation level
  - FISMA Control SA-2
- Ensure ESGF Points of Contact (PoC) are identified for all sites:
  - Site ESGF Manager PoC
  - Site ESGF Security PoC
- Ensure PoC information is maintained and kept current
  - FISMA Controls CP-3, IR-2, SA-3
- Ensure ALL PoCs have PGP keys and that those keys are managed appropriately. (https://en.wikipedia.org/wiki/Pretty_Good_Privacy)
  - FISMA Controls SC-12, SC-13

Software Design

- Define goals for future enhancements of the ESGF software design principles that include measures to enhance configuration management
- Site ESGF Security PoC should be consulted before adding new protocols or services
- Formalize a secure coding standard for ESGF
  - Reference Appendix 2
  - FISMA Control SA-11
- Define ESGF developer roles and responsibilities; at a minimum they shall include:
  - Ensure developers maintain a basic awareness of security principles (e.g., training)
  - Implement an ESGF process for pre-screening 3rd party libraries/components
  - Define and formalize an ESGF change process that includes enhancing configuration management (e.g. use of Puppet)
  - Implement a formalized peer review process of the ESGF Suite and incorporate that into the ESGF change process
  - Conduct threat modeling exercises during road-mapping/long range planning
  - Include security testing as part of functional testing as an integral aspect of the release process
  - Ensure the ESGF software stack can run under the supervision of mechanisms supporting access control security policies at the operating system level (such as SELinux)
  - FISMA Control SA-11
- Define flaw remediation procedures
  - Document ESGF software flaws (bug tracking, e.g., Bugzilla, Mantis,

Trac, etc.)
- Document ESGF software flaws with security implications
- Create a tracking database of flaws, accessible to all federation sites (authorization required)
- Disseminate flaw remediation status to the federation
- FISMA Controls SI-2, SA-11

Software Release

- Declaration and justification of minor versus major software release.
- Define/coordinate all release procedures (each site likely to customize this)
  - Ensure independence from the developer team
  - FISMA Control SI-2
- Ensure that the releases are assessed appropriately and that the appropriate Security Review (see below for details) is conducted
- Coordinate all releases and ensure that all releases include:
  - Current complete software component inventory (this is extremely important)
  - Release notes of changes
  - Current complete source code
  - Configuration and install scripts
  - FISMA Controls CM-2, CM-3, CM-6, CM-9, SA-10, SA-11
- Certify release for distribution. This is solely the responsibility of the LLNL ESGF Team.

Certificates

- Manage and coordinate ESGF certificates
  - Create ESGF certificates
  - Distribute ESGF certificates
  - Maintain ESGF certificates
  - FISMA Controls IA-5, SC-12

Incidents

- Define incident response procedures (to follow local Agency/site requirements) and include, at a minimum, the following:
  - Document incidents
  - Create a tracking database of ESGF incidents, accessible to all Federation sites (authorization required)
  - Disseminate incident status to the federation
  - Define an incident/security call-tree and distribute to all ESGF sites
  - FISMA Controls IR-4, IR-5, IR-6, IR-8

Contingency and Continuity of Operations Plans

- Define contingency plan and Continuity of Operations Plan (COOP) to manage outages, denial of service attacks and the like
  - Exercise contingency and COOP plans regularly

        - Partial exercise annually at a minimum
        - Full exercise every 2 years at a minimum
    - FISMA Controls CP-2, CP-4

Best Practices

- Define, collect, document and distribute best practices to sites
    - Reference Appendix 4
    - Areas that are of particular importance: access control, patching, configuration management, account management, incident response, security planning, system development and testing, system and information protection, and monitoring and integrity.
    - Maintain the repository of best practice documentation and distribute updates to all sites
    - Ensure sites adhere to best practices
    - Ensure sites contribute to best practices
- FISMA Controls AC-3, AC-5, AC-6, AC-14, AC-17, AC-22, CM-3, CM-4, CM-6, CM-7, CM-8, IA-8, IR-5, IR-6, PL-2, PL-8, SA-3, SA-8, SA-10, SA-11, SC-2, SC-5, SC-12, SC-13, SC-32, SI-4, SI-7

ESGF Software Security Working Team (SSWT)

Governance

- The ESGF SSWT shall be chartered and overseen by the ESGF Executive Committee
- The ESGF SSWT shall provide continuous improvement across ESGF by having membership and at least one representative from all ESGF sites and working teams
- The ESGF SSWT shall collaborate with all ESGF sites and working teams to provide procedures and guidance
- The ESGF SSWT shall seek to achieve commitment from all ESGF sites and working teams for its procedures and guidance
- The ESGF SSWT shall define and maintain the *major release Security Review procedure* (Appendix 3)
- The ESGF SSWT shall distribute the *major release Security Review procedure* to ESGF for review and approval by the Executive Committee
- The ESGF SSWT shall provide guidance to sites for the *minor release Security Review procedure* (Appendix 3) to ensure best practices are maintained
- The ESGF SSWT shall contribute to the transition from the "as-is" to the "to-be" architectures with respect to IT security
- Membership
    - NASA NCCS (chair)
    - Outside the NASA organization (secondary or co-chair)
    - All security PoCs from all ESGF sites
- Representation

    - All other working teams will define a primary and secondary PoC to represent themselves to the SSWT. These members will be invited to all discussions, have access to all notes, and be responsible for disseminating information to and from the SSWT to all other working teams.
- The ESGF SSWT shall collaborate with the developer team with respect to incorporating security into the design and build phases of the SDLC
- The ESGF SSWT shall ensure independence from the developer team with respect to implementation of security audits and code reviews and the definition of audit requirements and auditing functions
    - FISMA Control AC-5 (separation of duties)

The ESFG SSWT shall conduct the following activities:

- Provide a forum for coordination and discussion of all IT security related topics for ESGF.
- Coordinate forums and schedules of activities to support the ESGF SDLC
- Draft, maintain, and distribute the following:
    - Major release software review procedures
    - Guidance for the minor release software review procedures
    - Guidance for secure software design
    - Guidance for secure software build
    - Requirements for auditing/logging functions
    - Guidance for auditing/logging review
    - Guidance for secure baseline configurations
    - Guidance for best practices and lessons learned
- Ensure continuous improvement to the release procedures, best practices and other IT security aspects of the SDLC
- Ensure collaboration with the ESGF sites in order to obtain input for improving all aspects of the ESGF SDLC
- Ensure collaboration with the ESGF sites to factor in both individual site and collective security in all aspects of the ESGF SDLC
- Secure communications
    - Make sure all members of the team (including the site and working team PoCs), have a secure communication channel
    - Test this regularly

Create an “as-is” description of the current design and build processes.

- Draft in Appendix 5

Define “to-be” design, build and release processes:

- Apply a risk-based approach to the creation of the “to-be” design, build and release procedures
    - Perform a risk assessment of the “as-is” design, build and release procedures

    - Seek approval of the risk assessment recommendations and plans of action and milestones from the ESGF Risk Executive
- Provide guidance for secure software development practices (Appendix 2), informed by the risk assessment
- Apply secure software build and release practices (Appendix 2)

Effect a transition from the current "as-is" design, build and release processes to the agreed-upon "to-be" design, build and release procedures.

Software Review for Release

- Apply the major release procedure when requested and as per agreed-upon schedule.
- Communicate results of the Security Review to ESGF and iterate on results as necessary.
- Contribute to minor release Security Review activities as needed.

Baseline Configurations

- Coordinate the creation of a baselines for recommended configuration of the following:
    - Firewall
    - Servers
    - Administration accounts
    - Monitoring
    - Logging
    - Auditing
- Ensure baselines are provided back to ESGF for consideration/dissemination as best practice

ESGF Sites

All ESGF sites shall conduct the following activities:

Governance

- Shall be overseen by the ESGF Executive Committee
- Ensure ESGF PoC contact info is provided to the federation
- Ensure ESGF PoCs create and maintain PGP keys including the signing of PoC keys by trusted parties (web of trust) and the uploading of those signed keys to a PGP keyserver (e.g., https://pgp.mit.edu) for distribution and availability, see Appendix 2

Incident Response

- Define site-specific incident response procedures and ensure coordination with the federation

Contingency and Continuity of Operations Plan

- Define a site-specific contingency plan as well as continuity of operations (COOP) procedures and ensure coordination with the federation, including participation in exercises

Best Practices

- Follow the best practices as documented by the ESGF community.
- Reference Appendix

Appendix 1: Acronym List

Acronyms	Description
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Certification, Accreditation and Security Assessments
CM	Configuration Management
COOP	Continuity of Operations Plan
CP	Contingency Planning
CVE	Common Vulnerabilities and Exposures
ESGF	Earth System Grid Federation (aka "federation")
FISMA	Federal Information Security Management Act
GPG	Gnu Privacy Guard
IA	Identification and Authentication
IR	Incident Response
ISSO	Information System Security Officer
JPL	Jet Propulsion Laboratory
LLNL	Lawrence Livermore National Laboratory
MA	Maintenance
MP	Media Protection
NCCS	NASA Center for Climate Simulation
PE	Physical and Environmental Protection
PGP	Pretty Good Privacy (see also Gnu Privacy Guard – GPG)
PL	Planning
PM	Program Management
PoC	Point of Contact
PS	Personal Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SDLC	Software Development Life Cycle
SI	System and Information Security
SSWT	ESGF's Software Security Working Team
WASP	Web Application Security Project

Appendix 2: Secure Software Development Resources

- https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet
- https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices
- https://github.com/ESGF/esgf-installer.git

Encryption

- https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- https://www.gnupg.org/
- https://pgp.mit.edu - keyserver for key distribution (example, there is a world-wide network of these)

Security Controls, assessment case descriptions and downloads:

- http://dx.doi.org/10.6028/NIST.SP.800-53r4
    - Reference Table H-1: Mapping NIST SP 800-53 to ISO/IEC 27001
    - Reference Table H-2: Mapping ISO/IEC 27001 to NIST SP 800-53
- http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_dcussatt_dod-rmf-transition-brief.pdf
- http://csrc.nist.gov/groups/SMA/fisma/assessment-cases.html
- https://www.stigviewer.com/stigs

Appendix 3: Major and minor release Security Review procedures

ESGF Major Release Security Review Procedure:

- Responsibility: NASA NCCS Information System Security Officer (ISSO)
- To be performed by NASA NCCS, NASA JPL and others as needed.
- **Important: must have independence from developer team**

Prepare for Audit

- Install release candidate in a test environment – ESGF System Administrator
- Verify inventory and software package – ESGF System Administrator and ESGF Security Analyst
- Review release notes and updated documentation to assess changes – ESGF System Administrator and ESGF Security Analyst
- Develop a plan and schedule for Security Review, including the use of external resources (e.g., CS Gov "AppSec on Demand", JPL Dynamic scan, NASA WASP (web application security project) dynamic scan, etc.) – NCCS Security Lead, ESGF System Administrator and ESGF Security Analyst

Audit Release Candidate

- Schedule static code scan (e.g., Hewlett Packard (HP) Fortify) of ESGF release – NCCS Security Lead
- Perform the Common Vulnerabilities and Exposures (CVE) check (e.g., of "jar" files) of ESGF release – ESGF System Administrator
- Manual test and scan using local tools (adjust as needed for changes) – ESGF Security Analyst
- Review and code analysis of changed source code – ESGF Security Analyst
- Review of updated configurations (e.g., Apache, Tomcat, etc.) – ESGF System Administrator
- Schedule NASA WASP dynamic scan (e.g., Hailstorm, Nessus scanners) or NASA JPL dynamic scan as available of installed new version – NCCS Security Lead
- Activate external resources (e.g., CS Gov "Appsec on Demand") as necessary, should the assessments, static or dynamic scans be deemed insufficient – NCCS Security Lead

Maintenance of Audit Tools

- Perform maintenance of local scanning tools – ESGF System Administrator
- Maintain NCCS local assessment tools – ESGF Security Analyst
- Maintain access to external scanning resources (e.g., licenses for HP Fortify) – NCCS Security Lead

- Update resources and tools in response to ESGF technological changes and requests – NCCS Security Lead, ESGF System Administrator, and ESGF Security Analyst

Document Audit Results

- Document all high and moderate impact issues for tracking, add to ESGF Flaw Tracking Database – NCCS Security Lead, ESGF System Administrator, and ESGF Security Analyst
- Coordinate the resolution of all high and moderate impact issues – NCCS Security Lead
- Document for ESGF both the resolved and unresolved issues, recommendations, impacts and possible risk acceptance for ESGF sites – ESGF System Administrator and ESGF Security Analyst
- *IMPORTANT: Note that during this process feedback to the developer team is crucial for continuous improvement of pre-screening, peer-review, threat-modeling, and security testing as well as best practices*
- Document findings – NCCS Security Lead, ESGF System Administrator, and ESGF Security Analyst
- NCCS ISSO to issue final report to ESGF Executive Committee
    - ESGF Executive Committee certifies for release

ESGF Minor Release Security Review Procedure:

- Responsibility: individual ESGF sites
- **Important: must have independence from developer team**

Prepare for Audit

- Verify inventory and software package
- Review release notes
- Assess changes, define target for CVE check, testing and code review

Audit Minor Release Candidate

- Perform targeted CVE check (e.g., of "jar" files)
- Perform targeted manual testing and local scan tools
- Perform targeted source code review and code analysis
- Perform targeted configuration review (e.g., Apache, Tomcat, etc.)

Document Audit Results

- Document all high and moderate impact issues in ESGF Flaw Tracking Database
- Coordinate the resolution of all high and moderate impact issues with ESGF Team
- Document findings and each site issues report to ESGF (as necessary)
- ESGF Executive Committee certifies for release (NOT individual ESGF site)

Appendix 4: ESGF Site Best Practices

All Sites

- Shall adhere, as applicable, to ESGF site Best Practices
- Shall contribute recommendations to the ESGF site Best Practices for consideration and distribution
- FISMA Controls AC-3, AC-5, AC-6, AC-14, AC-17, AC-22, CM-3, CM-4, CM-6, CM-7, CM-8, IA-8, IR-5, IR-6, PL-2, PL-8, SA-3, SA-8, SA-10, SA-11, SC-2, SC-5, SC-12, SC-13, SC-32, SI-4, SI-7

Installation

- Verification of software packages using appropriate methods, such as checksums
- Create and maintain sufficient segregation/isolation of the local ESGF site environment - where feasible, ESGF published datasets should be separate from other data, preferably on storage hardware dedicated to ESGF nodes; least privilege shall be used, in regard to permissions on the ESGF datasets, i.e., if ESGF only requires read access, then only read is granted
- Implement recommended ESGF site firewall rules, to include:
    - Default deny posture, with exceptions allowed for access to the ESGF application;
    - Administrative access to the servers hosting the application; and
    - Other support functions.
- Ensure that the default password is changed after the ESGF Installer completes
- Ensure the ESGF software and supporting server operating system environment and supporting elements (e.g., Apache) are maintained and patched
    - Note/reminder: kernel updates typically require a reboot to take effect

Monitoring

- Highly recommended: implement central logging (loghost) of the ESGF environment, including Apache HTTPD and Apache Tomcat logs (ryslog imfile or similar means)
- Highly recommended: implement the use of the Linux audit capability and auditd daemon to monitor access attempts (NOTE: a baseline shall be developed for this), with audit logs also forwarded to a central loghost
- Highly recommended: implement monitoring (e.g., Nagios) of the ESGF environment and services upon which the ESGF local environment depends
- Highly recommended: implement mechanisms supporting access control security policies at the operating system level (e.g., SELinux)

Specific and Actionable Guidance shall also be developed in the following areas:

- Access control;
- Patching;
- Configuration management;
- Account management;
- Incident response;
- Security planning;
- System development and testing;
- System and information protection; and
- Integrity.

Appendix 5: ESGF "As-Is" Build Process

ESGF Installer Code Changes

- Done on ESGF mirror servers
- Tested on ESGF mirror servers
- Commited on ESGF mirror servers
- Synced to GitHub

Rationale for the above: the ESGF Installer is tied to specific contents mirrored by the project (tarballs of 3rd-party code, configuration templates, and other files including a copy of the main ESGF Installer scripts).

Note: the version that is uploaded to GitHub *deliberately* has an invalid version string, and if used unmodified will result in a broken build. This is because the release management software was written by an earlier ESGF developer and relies on search/replacing the invalid string during the release process when it copies the ESGF Installer script into its final location where users are instructed to retrieve it.

Note: the release process includes a checksum in the script, but since it relies on the script to verify itself, it has NO value in preventing a malicious replacement.

- At install/upgrade time, the script configures the system to accept additional third-party RPM repositories (the ESGF mirror and the Globus repos) for the RPMs it installs (the Globus RPMs are signed).

Note: it is unclear if the ESGF mirror signs its RPMs. This needs to be determined.

- The script downloads additional components including third-party tar-balls from the ESGF mirror to a "workbench" area. Those tar-balls are NOT signed.
- Configuration files and templates are also downloaded from the ESGF mirror. These configuration files and templates are NOT signed.

Note: Checksumming alone will not help unless ESGF can store the checksums in a more secure way.

- The ESGF Installer unpacks these files and runs code inside them as root during the install process

Note: there is significant value in preventing an attack on the ESGF mirrors. Git-Annex may be a way to mitigate this risk.