# Problem statement

Operation of services in all cases, whether locally or centrally deployed and operated, carries **security risks for resource providers at WLCG sites**. The standard for any service operator is to uphold the security, accountability, and incident response obligations of the host institution (e.g. a WLCG center) and participating research infrastructure (e.g. WLCG or experiments). **These obligations need to be articulated in a federated trust model appropriate to operation of distributed service platforms by trusted operations teams.**

# Charter

The main challenge to be addressed is to **document a trust model** for centralized service orchestration capability across WLCG centers ( federated operations ) to enable efficient operation of WLCG computing services and innovation of new platforms in support of HL-LHC software development. This Working Group **aims to clearly articulate entities and processes** which implement such capabilities. The **methods and trust relationships will be described** in documents (both existing and to be written) such as service level agreements and security policy documents, including security incident response and traceability. The trust model enables delegation of the service operator responsibility by the resource provider.

# Timeframe

- Complete all deliverables by May 31, 2020 (original).
- Revised target date - TBD

# Contact

e-group and mailing list, wlcg-federated-operations-security-wg@cernNOSPAMPLEASE.ch.

# Group membership

The group welcomes any contribution and discussion as long as they focus on the agreed WLCG deliverables and goals stated in this document. The group recognises the value of collaborations with connected communities. Joining the group can be done (pending moderator approval to avoid spam) HERE.

*(It is possible to login directly using eduGAIN or a Google account (among others) on the CERN SSO page, without applying for a CERN account.)*

# Plan for Deliverables (last update: August 6, 2020)

1. [Q4 2019] **Survey** and organize information about security concerns that stakeholders have with the federated operations model advanced by the SLATE project and by others, including the assurances that resource providers are looking for. **Document** what those concerns are.
    - ♦ Identify survey tool
    - ♦ Formulate questions
    - ♦ Send to communities noted below
    - ♦ Collect, synthesize and summarize survey methodology and results
    - ♦ Inform communities of results
    - ♦ 2020-02-13: Survey responses: https://docs.google.com/forms/d/e/1FAIpQLSdmWOThOXkTmTYO6Qz6-BUvLBDLdo0EVlzjka3M
    - ♦ Survey Report (2020.08.06): https://docs.google.com/document/d/1hB0bz8Dx2ZfdXl6RsskTm9KGE_oZ_H2uvqgeMvoR398/edit?

2. [Q1 2020] **Document** current SLATE and related technologies, architecture, workflows and operations and how they address the **WLCG Security Policies** and **Trusted CI Framework** and identify potential gaps.
    - **Establish and confirm** the relevant topics in the context of the working group.
        - Draft list include:
        - Incident response
        - Traceability
        - SLA / Security Operations policy
        - TBC
    - **WLCG security policies**: Evaluate SLATE compliance and areas of work, for each topic, in the context of the WLCG security policies.
    - [Q2 2020?] **Trusted CI - SLATE engagement** work plan:
        - Status update on SLATE security policies (following the Trusted CI Master Information Security Policy & Procedures template)
        - Initial risk assessment of 5 core SLATE "workflows"
        - Discussion of available container image security scanning tools and their applicability to SLATE
3. **Identify further areas** that Federated Operations processes and policies should address, together with any constraints or other concerns associated with each area.
    - Produce a **document** with these additional areas.
    - Audiences for this documentation are:
        - WLCG resource providers and cybersecurity responsibles
        - Federated operations platform developers, e.g. the software and computing teams of the experiments (e.g. ATLAS Distributed Computing) and R&D teams (e.g. HSF related development, IRIS-HEP, etc.)
        - SLATE and other federated operation project teams
4. Integrate the outcomes of 1-3 and document the complete set of policies, procedures, and security controls and produce the new **Federated Operations trust model document**.
5. Evaluate the new trust model in the context of the existing WLCG Security Policies (http://wlcg.web.cern.ch/security/computer-security). Determine if the new federated trust model can respect these policies and recommend updates as necessary.
6. Apply the Trusted CI Framework (https://trustedci.org/framework) to the new federated operations model and provide feedback to the Trusted CI organization.
7. Report concerns, progress, etc at appropriate places:
    - NSF Cybersecurity Summit
    - WLCG Grid Deployment Board meetings
    - Experiment software and computing meetings
    - Relevant conferences such as WLCG Collaboration meetings, HSF, OSG meetings, CHEP, GridPP, PEARC20, etc.

# Work timeline and meetings

*(ISO 8601 format: YYYY-MM-DD)*

- 2020-09-01: Federated Operations Security Birds of Feather at OSG All Hands Meeting: https://docs.google.com/document/d/1yWJ6lkdHGFETuDQaAWZAawH3k4tnBPlUD6RfHPqYrt8/edit?usp=s
- 2020-08-06: WLCG Federated Operations Security Survey document released, https://docs.google.com/document/d/1hB0bz8Dx2ZfdXl6RsskTm9KGE_oZ_H2uvqgeMvoR398/edit?usp=sha
- 2020-03-11: GDB Meeting: *WLCG Federated Operations Security Survey*, Slides
- 2020-02-26: Meeting to discuss survey results, https://indico.cern.ch/event/892058/
- 2020-02-13: Survey responses: https://docs.google.com/forms/d/e/1FAIpQLSdmWOThOXkTmTYO6Qz6-BUvLBDLdo0EVlzjka3Mzj0lRoR
- 2020-01-23: Survey sent to the community: https://forms.gle/efcShH2DoXxLspFp8 (SurveyEmailText)

- 2019-11-05 : CHEP2019: https://indico.cern.ch/event/773049/contributions/3473807/
  - "Towards a NoOps Model for WLCG" -- SLATE presentation and status update
- 2019-10-15: NSF Cybersecurity Summit: https://trustedci.org/2019-nsf-cybersecurity-summit/
  - Report out during proposed WISE workshop
  - Chris and Rob submitted proposal for plenary talk
  - Have a side meeting to review draft of deliverables 1&2 and highlighted content
- 2019-09-10 Kick off meeting to define charter and deliverable: https://indico.fnal.gov/event/21485/
  - Attendees: Jim Basney, Rob Gardner, Kay Avila, John Hover, Romain Wartel, Jeny Teheran, Shawn McKee, Mike Stanfield, Irwin Gaines, Dave Kelsey, Frank W, Lincoln Bryant, Andrew Adams, Stephane Jezequel, Joe Breen, David Crooks, Vlad Grigorescu, Vincent Brillault, Brian Bockelman, Chris Weaver
- 2019-07-16 Initial discussion:  We need a WG  : https://indico.cern.ch/event/834872/
  - Attendees: Chris Weaver, Dave Kelsey, Frank Wuerthwein, Igor Sfiligoi, Jim Basney, Johannes Elmsheuser, Lincoln Bryant, Nikolai Hartmann, Paul Millar, Robert Gardner, Romain Wartel, Petr Vokac, Tom Barton, Stephane Jezequel, Shawn McKee, Vincent Brillault, Brian Bockelman, Xavier Espinal, Elizabeth Sexton-Kennedy

# WG Documents

- A number of policy documents, conformant with the WISE Community SCIv2 framework have been developed for the SLATE federation: https://slateci.io/docs/security-and-policies/index.html

# Related Presentations and Publications

- 2020.09.01: Chris Weaver, *Status of Security Policies for SLATE*, OSG All Hands Meeting: https://docs.google.com/presentation/d/1-4Ep-g2SITwbnaU-3kVaHdByrCeXVlBh0fu29C-bXBU/edit?usp=sha
- Applying the SCI Trust Framework to SLATE, C. Weaver, WISE meeting, April 21, 2019: https://docs.google.com/presentation/d/1h97qIHxFIzxGjdJIA9_FJW-qtMqwKD-f7QcII1BeoHE/edit?usp=shar
- Presentations at https://wiki.geant.org/display/WISE/WISE+@+NSF+Cybersecurity+Summit+2019
- Managing Privilege and Access on Federated Edge Platforms, https://dl.acm.org/doi/10.1145/3332186.3332234

# References

- SCIv2: A Trust Framework for Security Collaboration among Infrastructures: https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf
- https://slateci.io/docs/security-and-policies/
- https://trustedci.org/slate

---

This topic: LCG > WLCGFederatedOperationsSecurityWG
Topic revision: r8 - 2020-10-14 - RobertGardner