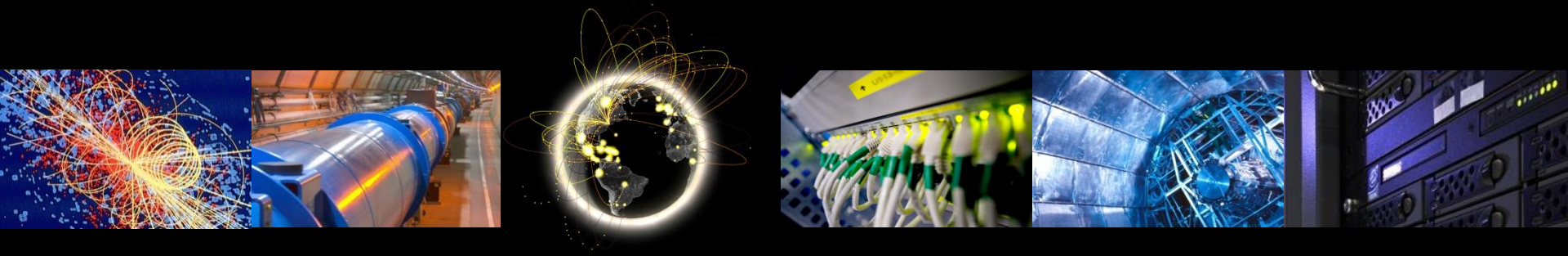
Traceability & Isolation WG Policy Recommendations

Vincent BRILLAULT, CERN/EGI-CSIRT

WLCG Management Board, July 2019



WLCG Worldwide LHC Computing Grid

CERN

Traceability policies

- Security Traceability and Logging Policy
  - High Level policy, still valid* and used
- e-Infrastructure Multi-User Pilot Jobs
  - Requires gLExec or very similar functionality
  - Not followed by any VO any more…
- Working group proposal (GDB): new policies
  - Agreed by all WLCG VOs
  - Still ensuring full traceability of user payloads

Policy recommendations (simplified)

- User payloads must be isolated (processes, files)
  - Via namespaces (e.g. Singularity), gLExec, …
- Traceability responsibility can be split
  - Sites track job activity as before, but not users
  - VOs track job-user mapping
- VOs have an operation role in incident response
  - VOs have to maintain security contacts and procedures
  - Sites can suspend VOs (no availability penalty)

Consequences / Main changes

- Full traceability of user payload maintained
  - But slightly more complex to obtain (split)
- Sites can no longer suspend end-user
  - VOs can do it. Sites suspend VOs otherwise
  - Already the case in practice
- User certificates not needed at site for isolation
  - Unprivileged credential still required for storage

Going Forward: MB approval

- Documents finalized within WG
  - Agreed by all participants (all WLCG VOs, few sites)
  - Accepted by the policy group as input

- Request to Management Board:
  Approve the attached "Recommendations"
  - Allow VOs to go forward with their implementation
    - Knowing that the policies won't change drastically in the near future
  - Allow policy group to start working on the policy
    - Knowing that the resulting policy is likely to be validated