

**DRTS meeting** - Security coordination, trust and policy

~~Cybersecurity for  
Science Research in EU Europe~~

(Trusted CI Virtual Institute, 25 June 2019) **1 Dec 2020**

**David Kelsey, RAL PPD**

STFC, UK Research and Innovation



# Security Coordination – DavidK & STFC roles - HISTORY

- Various roles in *Security, Trust and Identity* since year 2000
  - In UK GridPP, WLCG and EU-funded projects (EU DataGrid, EGEE, EGI-Inspire, EGI-Engage, AARC/AARC2, EOSC-hub, EGI-ACE, EOSC Future)
  - 2000: **DaveK** EU CA Coordination Group -> X.509 EUGridPMA (2004) & TAGPMA & IGTF (2005)
    - **AndrewS** ran the first UK CA. **Jens** joined soon after
  - 2001: EU DataGrid WP7 Security Group started – **Linda** worked on Security Requirements (D7.5)
  - 2003: Security policies for GridPP (UK) & Worldwide Large Hadron Collider Computing Grid (WLCG) - **IanN**
  - 2004: EGEE starts. WLCG/EGEE/OSG Joint Security Policy Group (JSPG)
  - 2005: EGEE OSCT/CSIRT and Software Vulnerability Group (SVG) - **IanN & Linda**
  - 2010: EGI Foundation created – EGI CSIRT, SVG and SPG
  - 2011: FIM4R.org (Research Community Federated IdM requirements) – founding partner
  - 2013: Security for Collaborating Infrastructures (SCI) - version 1 published
  - 2015: WISE & SCI version 2 (published 2017)
  - 2018: EOSC-hub starts and then -
  - Threat Intelligence - WLCG SOC Working Group - **DavidC**
  - UK IRIS – Policy/Trust Asset development and Operational Security – **DavidC**
  - 2020: Join GEANT GN4-3 WP5 Enabling Collaboration (EnCo) policy group
  - 2021: EGI-ACE and EOSC-Future start

Ian Bird  
CERN

EGI Conference  
Amsterdam, 6<sup>th</sup> May 2019

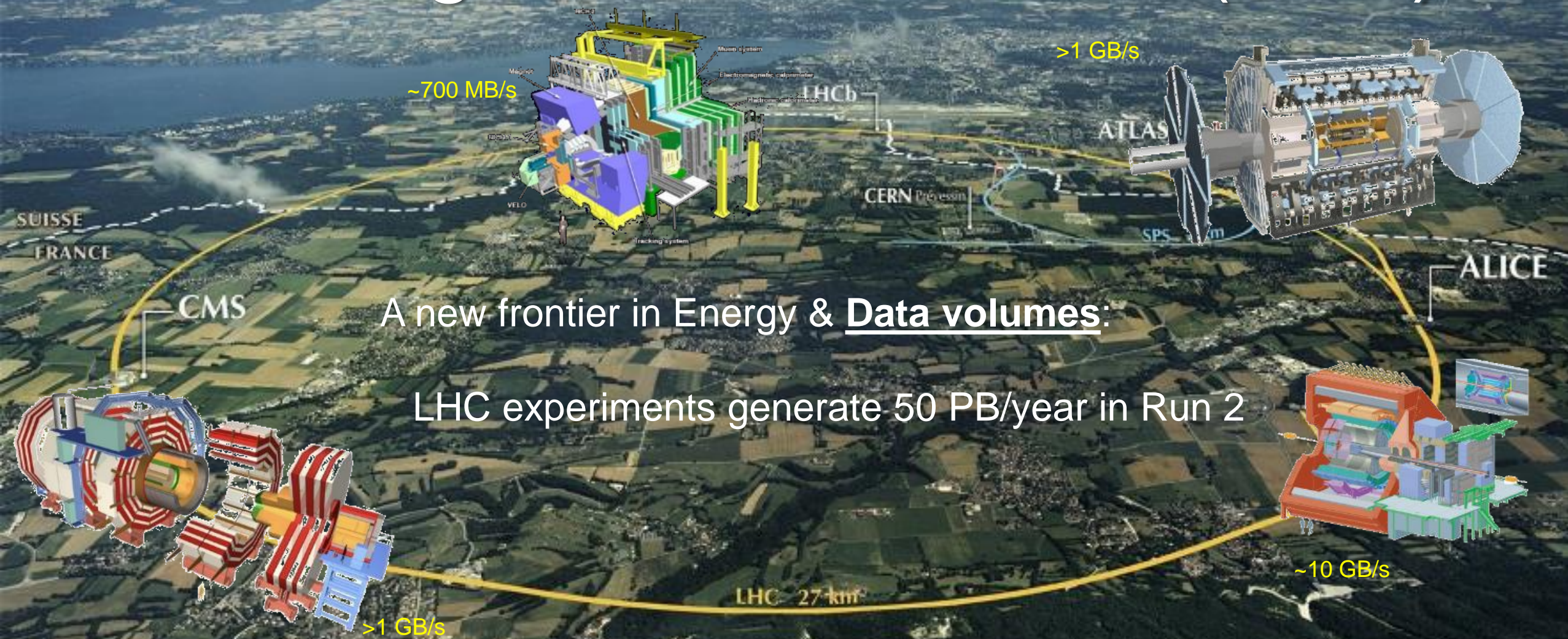
CMS Experiment at the LHC, CERN  
Sat 2012-12-09 22:34 CEST  
Run 194050 Event 111946235  
C O M Energy 8.0TeV  
H>Gamma Gamma candidate



# WLCG: Evolving Distributed Computing for the LHC



# The Large Hadron Collider (LHC)



A new frontier in Energy & Data volumes:

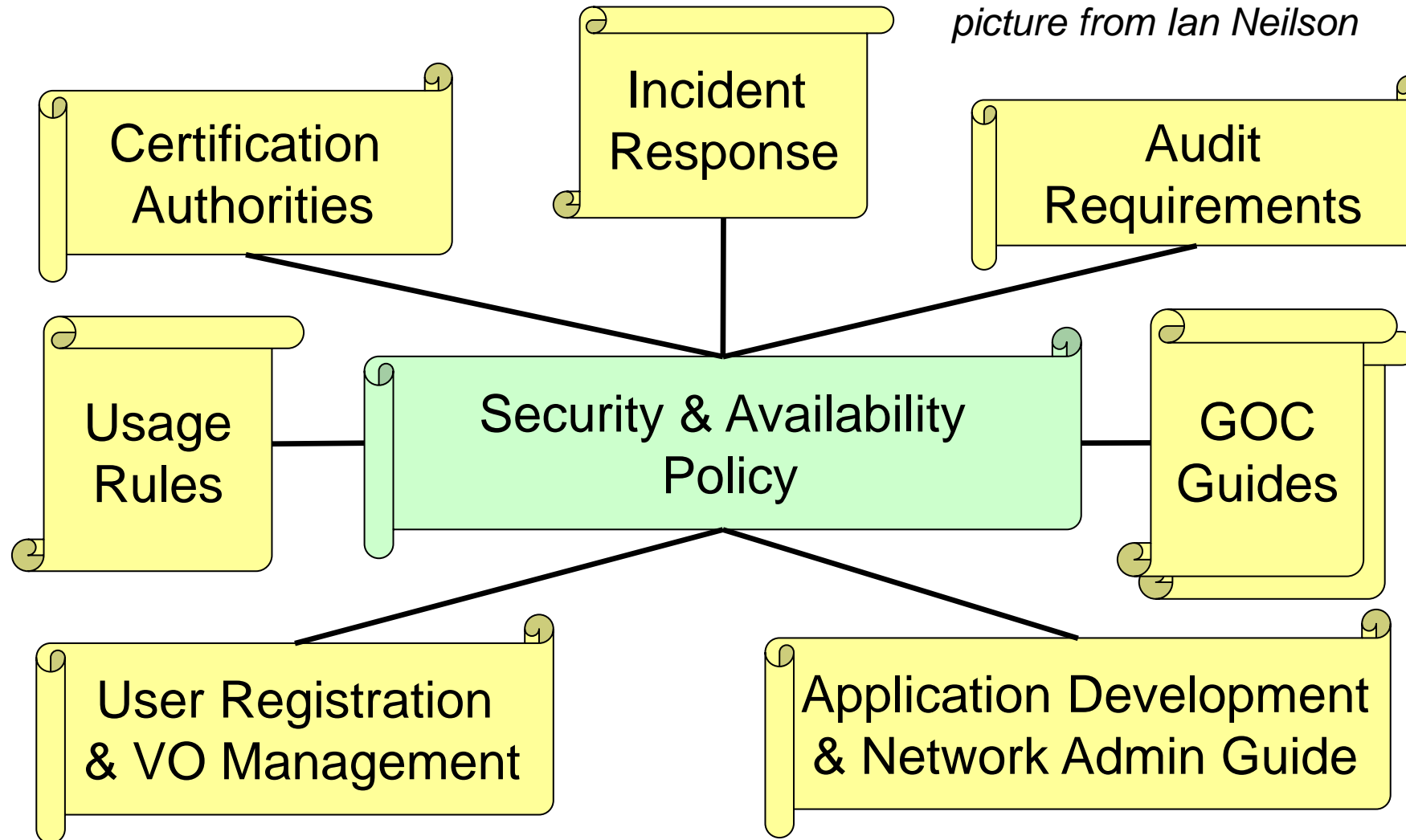
LHC experiments generate 50 PB/year in Run 2

# Some lessons and comments

- A federated infrastructure is of tremendous value and importance
  - This is the **\*key\* feature** that identifies our collaborative distributed infrastructure
  - Even though the X.509 model was difficult to use and manage
  - **Security coordination; policies, incident response, vulnerability & threat intelligence is of huge value**
- The network is a fundamental resource and opportunity, not a problem to be solved
  - Redundancy and distribution of services as originally foreseen was unnecessary, complex, and expensive
  - Today service model is much simplified and streamlined
- Today's operational structure is very simple – coordination at a high level, no need for the heavyweight operations centres
  - Integrated global ticketing system was essential
- Ubiquitous use of “pilot” jobs rather than resource brokering – far more efficient for using available resources
  - In future the potential specialization of resources may affect this
- Distributed data management and storage is expensive – hardware and operations
  - Data pre-placement is not an optimal strategy (it is a complex problem)
- Hardware and cost evolution is becoming a serious concern –
  - “Moore’s law” as we assumed it is broken
  - Future of storage technology is a concern – tape and disk
  - The future computational resources are very heterogenous

# LCG Policy

*picture from Ian Neilson*



<http://cern.ch/proj-lcg-security/documents.html>

- Prevention of security incidents
  - Risk assessment & mitigation
  - Security Monitoring
  - Vulnerability Handling
- Incident Response
  - Support Infrastructure, community & service security teams
  - Digital forensics
  - Mitigation
- Security Drills & communication challenges
- Training and dissemination
- Security Policy Group

# More details published in

<https://www.egi.eu/wp-content/uploads/2017/07/EGI-CSIRT-report-July-2017.pdf>







# SCI Version 2 - published 31 May 2017



## **A Trust Framework for Security Collaboration among Infrastructures**

*SCI version 2.0, 31 May 2017*

L Florio<sup>1</sup>, S Gabriel<sup>2</sup>, F Gagadis<sup>3</sup>, D Groep<sup>2</sup>, W de Jong<sup>4</sup>, U Kaila<sup>5</sup>, D Kelsey<sup>6</sup>, A Moens<sup>7</sup>,  
I Neilson<sup>6</sup>, R Niederberger<sup>8</sup>, R Quick<sup>9</sup>, W Raquel<sup>10</sup>, V Ribaillier<sup>11</sup>, M Sallé<sup>2</sup>,  
A Scicchitano<sup>12</sup>, H Short<sup>13</sup>, A Slagell<sup>10</sup>, U Stevanovic<sup>14</sup>, G Venekamp<sup>4</sup> and R Wartel<sup>13</sup>

The WISE SCIv2 Working Group - e-mail: [david.kelsey@stfc.ac.uk](mailto:david.kelsey@stfc.ac.uk), [sci@lists.wise-community.org](mailto:sci@lists.wise-community.org)

<https://wise-community.org/sci/>



# Endorsement of SCI Version 2 at TNC17 (Linz)



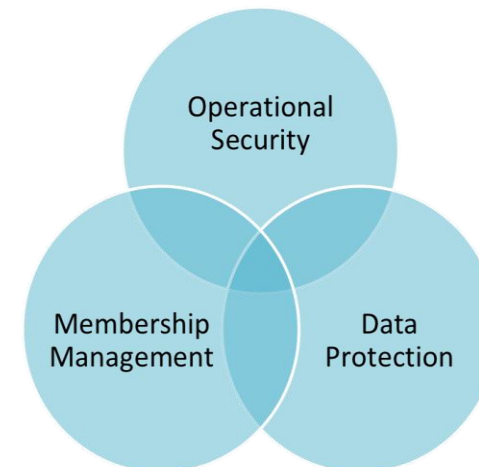
- 1<sup>st</sup> June 2017
- *Infrastructures endorse the governing principles and approach of SCI, as produced by WISE, as a medium of building trust between infrastructures, to facilitate the exchange of security information in the event of a cross-infrastructure incident, and the collaboration of e-Infrastructures to support the process. These Infrastructures welcome the development of an information security community for the Infrastructures, and underline that the present activities by the research and e-Infrastructures should be continued and reinforced*
- Endorsements have been received from the following infrastructures; EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE, HBP
- [https://www.geant.org/News\\_and\\_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx](https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx)



# AARC Policy Development Kit

---

- SCI paper (*A Trust Framework for Security Collaboration among Infrastructures*)
- SNCTFI (*Scalable Negotiator for a Community Trust Framework in Federated Infrastructures*)
  - Top level policy
    - Operational Security
    - Membership management
    - Data protection
- Consider current best practices (EGI, CERN, ELIXIR, TrustedCI, etc.)
- Policies started from EGI versions
  - And then modified
- Some other policies (Infrastructure-related) will need to be handled by WISE/EOSC-hub



# FIM4R version 2

David Kelsey (STFC UK Research and Innovation)  
at UK AAI meeting 24-25 July 2018

*With thanks to the FIM4R Authors and Contributors for their collaboration on the whitepaper and the following slides.*



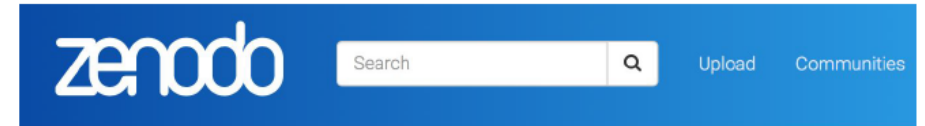
*\*\* Not all contributors' logos represented*

*“Every researcher is entitled to focus on their work and not be impeded by needless obstacles nor required to understand anything about the FIM infrastructure enabling their access to research services.”*

FIM4R version 2

# FIM4R Whitepaper


- A second version of a 2012 whitepaper
- Representatives of more than 20 research communities provided input
- Five face to face meetings in Europe and North America
  - Vienna (TIIME) x 2
  - Montreal (RDA)
  - Barcelona (RDA)
  - San Francisco (Internet2 TechEx)
- Produced a new distillation of specific requirements and a set of recommendations



June 22, 2018

Journal article Open Access

## Federated Identity Management for Research Collaborations

 Christopher John Atherton;  Thomas Barton;  Jim Basney;  Daan Broeder;  Alessandro Costa;  Mirjam van Daalen;  Stephanie Dyke;  Willem Elbers;  Carl-Fredrik Enell;  Enrico Maria Vincenzo Fasanelli;  João Fernandes;  Licia Florio;  Peter Gietz;  David L. Groep;  Matthias Bernhard Junker;  Christos Kanellopoulos;  David Kelsey;  Philip Kershaw;  Cristina Knapic;  Thorsten Kollegger;  Scott Koranda;  Mikael Linder;  Filip Marinic;  Ludek Matyska;  Tommi Henrik Nyrönen;  Stefan Paetow;  Laura A D Paglione;  Sandra Parlati;  Christopher Phillips;  Michal Prochazka;  Nicholas Rees;  Hannah Short;  Uros Stevanovic;  Michael Tartakovsky;  Gerben Venekamp;  Tom Vitez;  Romain Wartel;  Christopher Whalen;  John White;  Carlo Maria Zwölf

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

<https://doi.org/10.5281/zenodo.1296031>



Science and  
Technology  
Facilities Council

# AAI and Security

David Crooks

david.crooks@stfc.ac.uk

IRIS Collaboration Meeting

November 2020



Science and  
Technology  
Facilities Council



iris

# Distributed Research Trust and Security

- Within STFC in SCD and PPD we have people working on all areas of distributed security
  - Security Coordination
  - Identity Management
  - Trust and Policy
  - Operational Security
- Collectively many years of experience
  - National and international contacts
- Working to bring together a new team representing all these areas
  - Single point of contact to support communities in a distributed federated landscape



Science and  
Technology  
Facilities Council



iris



# Thank you for your attention.

*Questions?*



[www.esgi.eu](http://www.esgi.eu)

