Operationalizing Sirtfi… Going Beyond the Technical

Linking Two Teams

Cultivating "Security Mindedness" in IAM Teams

Cultivating "Federation Mindedness" in Security Teams

Operationalizing Sirtfi

This presentation iterates and integrates the following concepts:

- Sirtfi – What is it?
- Practical Considerations
- Process-based Approach
- Potential Scenarios requiring Sirtfi
- Practice and Learning Opportunities

TLP:CLEAR

REFEDS Sirtfi – What is it?

- Security Incident Response Trust Framework for Federated Identity (Sirtfi)
  - Enables federation members to coordinate cybersecurity incident response
  - Builds information security trust between federation members
  - Sirtfi (v1) is part of InCommon Baseline Expectations (not yet Sirtfi2)

https://refeds.org/sirtfi

TLP:CLEAR

Guide for Federation Participants

https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants

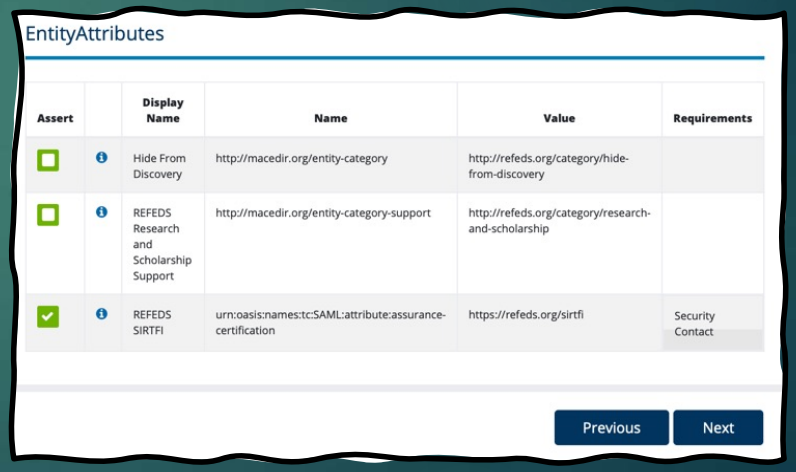
- Self Assessment
  16 Normative Assertions

- Add Security Contact Details

An example of a ContactPerson element can be seen below:

REFEDS security contact

```
<ContactPerson xmlns:remd="http://refeds.org/metadata"
    contactType="other"
    remd:contactType="http://refeds.org/metadata/contactType/security">
<GivenName>Security Response Team</GivenName>
<EmailAddress>mailto:security@xxxxxxxxxxxxxxx</EmailAddress>
</ContactPerson>
```



- Agree to use Traffic Light Protocol
- Assert Sirtfi Compliance (to your federation)

TLP:CLEAR

Trust Questions for Self Reflection

- If you reach out to my security point of contact and share a firewall log marked "TLP RED", can you trust that my team knows we can't share that even with my other team members?
- If I have a user account who accesses your systems, and that account becomes compromised … can you trust my security team knows how to look up your security team's contact info in the federation metadata, and reach out to let you know?
- Am I comfortable trying to figure out the Sirtfi expectations on the fly during a real world incident … or can you trust whether I incorporated the expectations into my procedures, and have practiced them?

Light Towers: Process and Procedures

- When is Sirtfi "activated"?
- Who is prompted to activate it?
- Two perspectives: internally initiated and externally initiated
- Modify your procedures

Normative Assertions– Operational Security

- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.
- [OS3] Means are implemented to detect and act on possible intrusions using threat intelligence information in a timely manner.
- [OS4] A user's access rights can be suspended, modified or terminated in a timely manner.
- [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.
- [OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

Managing access to information resources, maintaining their availability and integrity, and maintaining confidentiality of sensitive information

These likely (hopefully) exist even before considering Sirtfi or Federation

TLP:CLEAR

Normative Assertions– Incident Response

Incident response interactions with other organizations participating in the Sirtfi trust framework

- [IR1] Provide security incident response contact information as may be requested by any federation to which your organisation belongs.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in Sirtfi in a timely manner.
- [IR3]* Notify security contacts of entities participating in Sirtfi when a security incident investigation suggests that those entities are involved in the incident. Notification should also follow the security procedures of any federations to which your organisation belongs.
- [IR4] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in Sirtfi.
- [IR5] Respect user privacy as determined by the organisation's policies or legal counsel.
- [IR6] Respect the Traffic Light Protocol [TLP] information disclosure policy and use it during incident response communications with federation participants.

By definition, these assertions do not exist before considering Sirtfi or Federation.
These require some work (hold on to this idea; we'll revisit).

* Added requirement for Sirtfi2

TLP:CLEAR

Normative Assertions – Traceability

Able to answer the basic questions "who, what, where, and when" concerning a security incident requires retaining relevant system generated logs, including accurate timestamps and identifiers of system components and actors, for a period of time

- [TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.
- [TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices.

These likely (hopefully) exist even before considering Sirtfi based on already being in the Federation.

TLP:CLEAR

Normative Assertions – Participant Responsibilities

- [UR1] The participant has defined rules and conditions of use.
- [UR2] There is a process to notify all users of these rules and conditions of use.

All participants (IdPs and SPs) in the federations rely on each others users practicing knowing what is expected as authorized, appropriate and responsible network behavior

These likely (hopefully) exist even before considering Sirtfi or Federation

TLP:CLEAR

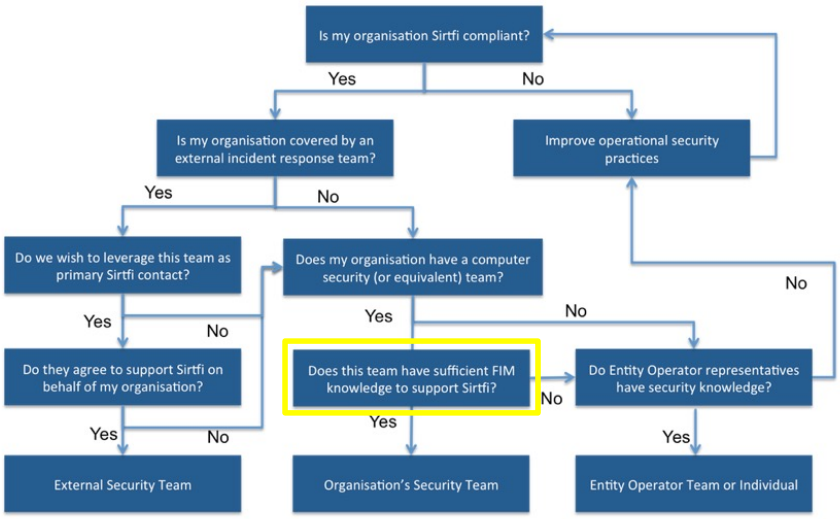
Self-Evaluation of Normative Assertions

- Review all normative assertions and assess yes/no
- Note:
  - *"How thoroughly each asserted capability should be implemented […], is not specified.*
  - *Care should be focused on […] elements that directly handle federated transactions;*
  - *however, the investment in mitigating a risk should be commensurate with the degree of its potential [risk], and this determination can only be made within each organisation." (https://refeds.org/sirtfi)*
- If any "no", must not assert Sirtfi
- Compliance with this self-assessment is self-asserted (trust federation)

TLP:CLEAR

Publishing the Security Contact

A flow chart has been provided to describe the thought process for choosing a Sirtfi contact.

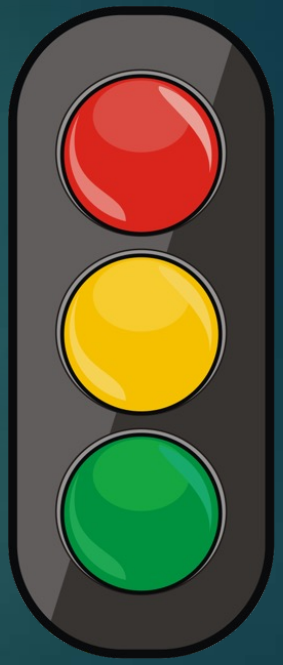


https://wiki.refeds.org/display/SIRTFI/Choosing+a+Sirtfi+Contact

- How Integrated are your IAM and Security Teams?
- Even if you publish a dedicated security contact for Federation, that only "solves" incoming requests. What about internal security incidents handled by your "normal" Security Team?
- Will your security team be responsive to your IAM team if the IAM team is the published security contact?

Traffic Light Protocol (TLP)

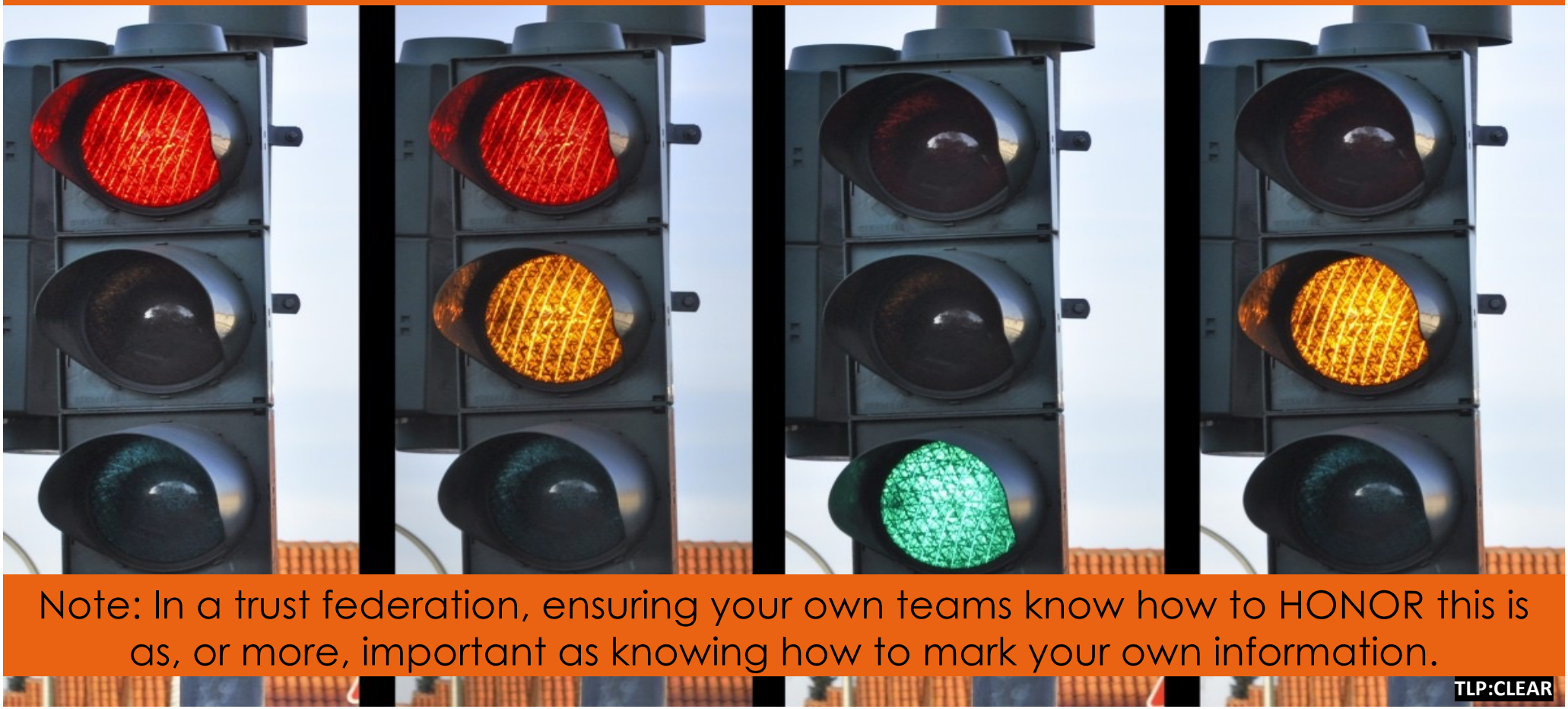
- Traffic Light Protocol (TLP) is a way of marking information so others know if and how wide they can share it.
  - **TLP:RED = Not for disclosure, restricted to participants only**
  - **TLP:AMBER = Limited disclosure, restricted to participants' organizations.**
  - **TLP:GREEN = Limited disclosure, restricted to the community.**
  - **TLP:CLEAR or TLP:WHITE = Disclosure is not limited.**



https://www.cisa.gov/tlp

TLP:CLEAR

Who's "answering the phone?"
Is my security team trained on TLP?



Note: In a trust federation, ensuring your own teams know how to HONOR this is as, or more, important as knowing how to mark your own information.

TLP:CLEAR

Requires an Organizational Culture/Procedures Change

- Build "federation mindedness" in your Security Response Team (i.e., who is answering the published security contact mail?)
  - Do this by updating checklists, SOPs, and practicing!
- Build "security mindedness" in your IAM team
- How integrated are your IAM and Security Teams?

TLP:CLEAR

Process and Procedures

- When is Sirtfi "activated"?
- Who is prompted to activate it?
  - Do they know how to look up security contacts based on IdP logs and using the REFEDS Metadata Explorer Tool?
- Two perspectives:
  - Initiator – Security Team which uncovers a security incident
  - Receiver – Security Contact notified by external team
- Build, document and train on updates to your procedures

Resource: eduGain Security Incident Response Handbook

Federation Participants

1. Follow all security incident response procedures established for your organisation and your federation.
2. Initial incident response:
   a. Contain the security incident to avoid further propagation to other entities, while preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
   b. Report on all suspected ongoing security incidents posing a risk to any Federation Participants within or outside your own federation to your Federation Operator as soon as possible, but within one local working day of becoming aware of the suspected incident.
3. In collaboration with your Federation Operator, ensure that all affected Federation Participants are notified, including those belonging to other federations. Include relevant information, when possible, to allow them to take action.
4. Investigate and coordinate the resolution of suspected security incidents within your domain of operation and keep the Federation Operator and other involved parties updated appropriately.
5. Announce suspension of service (if applicable) to your Federation Operator, in accordance with federation practices.
6. Perform appropriate investigation, system analysis and forensics and strive to understand the cause of the security incident and its full extent.
7. Share additional information as often as necessary to keep all affected parties up-to-date with the status of the security incident and enable them to investigate and take action should new information appear. It is strongly encouraged for such updates to occur at regular intervals, to include the time of the next update within each update and to issue a new update sooner if significant new information is available.
8. Respond to requests for assistance from others involved in the security incident within one local working day (in case of limited trust or doubt regarding the party behind a given request, involve your Federation Operator and the eduGAIN Security Team).
9. Take corrective action, restore legitimate access to service (if applicable).
10. In collaboration with your Federation Operator, produce and share a report, including lessons learned and actions taken, of the incident with all Sirtfi-compliant organisations in all affected federations within one month of its resolution. This report should be labelled TLP AMBER or higher.
11. Review and update your own organisation's documentation and procedures as necessary to prevent recurrence of the incident in the future.

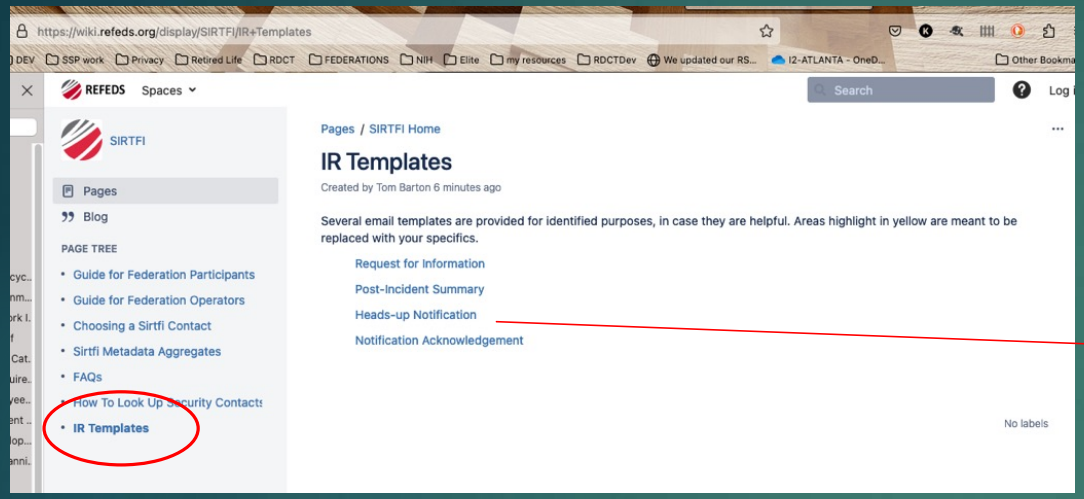
The Federation Participant's Federation Operator or the eduGAIN Security Team may be contacted and involved at any time for security advice, recommendations, technical support and expertise, regardless of the severity of the suspected incident, at the discretion of and based on the needs of the Federation Participant.

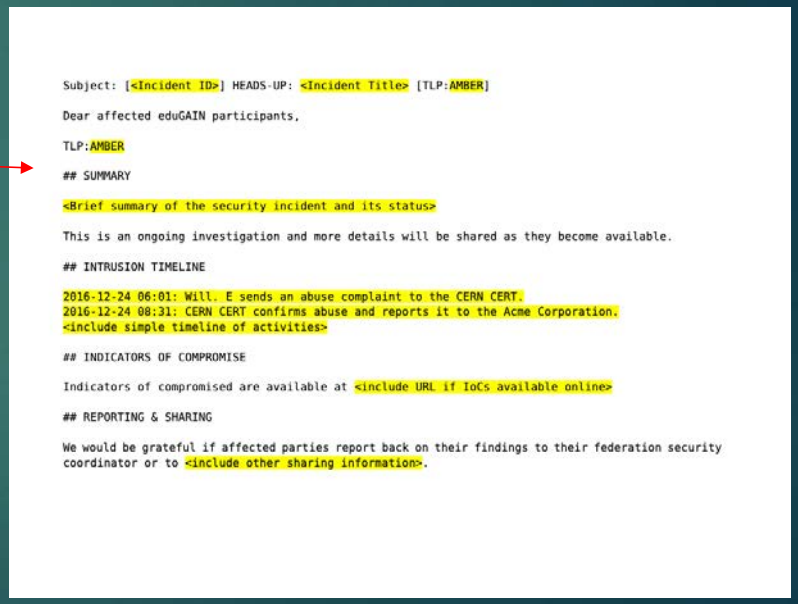
Linked from https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants

TLP:CLEAR

Resource:
Sirtfi WG's Incident Response Templates

https://wiki.refeds.org/display/SIRTFI





```
Subject: [<Incident ID>] HEADS-UP: <Incident Title> [TLP:AMBER]

Dear affected eduGAIN participants,

TLP:AMBER

## SUMMARY

<Brief summary of the security incident and its status>

This is an ongoing investigation and more details will be shared as they become available.

## INTRUSION TIMELINE

2016-12-24 06:01: Will. E sends an abuse complaint to the CERN CERT.
2016-12-24 08:31: CERN CERT confirms abuse and reports it to the Acme Corporation.
<include simple timeline of activities>

## INDICATORS OF COMPROMISE

Indicators of compromised are available at <include URL if IoCs available online>

## REPORTING & SHARING

We would be grateful if affected parties report back on their findings to their federation security
coordinator or to <include other sharing information>.
```

- Not "mandatory"
- Available to use/supplement local procedures

TLP:CLEAR

Resource:
REFEDS Metadata Explorer Tool (MET)

https://wiki.refeds.org/display/SIRTFI and https://met.refeds.org

REFEDS Spaces Search Log in

SIRTFI

Pages
Blog

PAGE TREE
- Guide for Federation Participants
- Guide for Federation Operators
- Choosing a Sirtfi Contact
- Sirtfi Metadata Aggregates
- FAQs
- How To Look Up Security Contac
- IR Templates

Pages / SIRTFI Home

How To Look Up Security Contacts

Created by Tom Barton on Sep 20, 2022

When you need to reach out to another Sirtfi compliant entity, how should you grab their security contact info from the entity's federation metadata? Below are details of a good method for doing so.

Use the REFEDS Metadata Explorer Tool (MET)

The REFEDS organisation collects the complete metadata registered by every R&E federation in the world and provides the MET tool to search it:

https://met.refeds.org/

Click the Search Entities button on that page to bring up the search interface.

If you have the complete entity ID of the entity you wish to contact in hand, enter it in the "Search entity ID" field and click Submit.

Otherwise, you can choose an Entity Type, usually either IdP or SP, to narrow the result set. You might also choose the Entity Category of "https://refeds.org/sirtfi" if you wish to only attempt to contact a Sirtfi compliant site. Beyond that, use the Organization Name or Organization Display Name fields to narrow the result set. For example, to look up the IdP for a university in Chicago without being certain exactly how it is named, enter just "chicago" in either of those fields. The result list shows the complete entity ID and Organization Display Name of all matching entities.

Click on the entity ID of the one you think you're looking for. This brings up some details of the entity's metadata that can help you confirm whether you've got the right one. If it is, scroll down to the Contacts area. The security contact, if there is one, will be of type "other". You can mouse over its displayed name to have your browser show the actual contact.

You can also click on the "view xml" button at the top right and search the displayed metadata for "security". If you find

remd:contactType="http://refeds.org/metadata/contactType/security

within a ContactPerson element you've found the right one. The security contact address is usually given in an associated md:EmailAddress element.

No labels

Powered by a free **Atlassian Confluence Community License** granted to TERENA. Evaluate Confluence today.

Powered by Atlassian Confluence 7.13.7 · Report a bug · Atlassian News

ATLASSIAN

https://met.refeds.org

Metadata Explorer Tool

Access through your institution

Search service ID

Entities summary

ENTITIES	IDP	SP	AA
22472	8039	14425	8

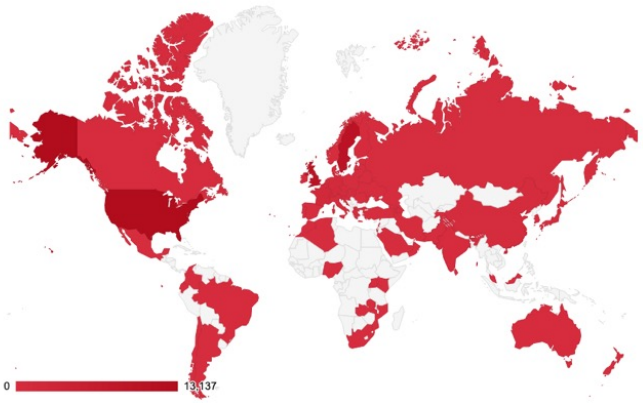
Most Federated Entities | Search Entities

Interfederations summary

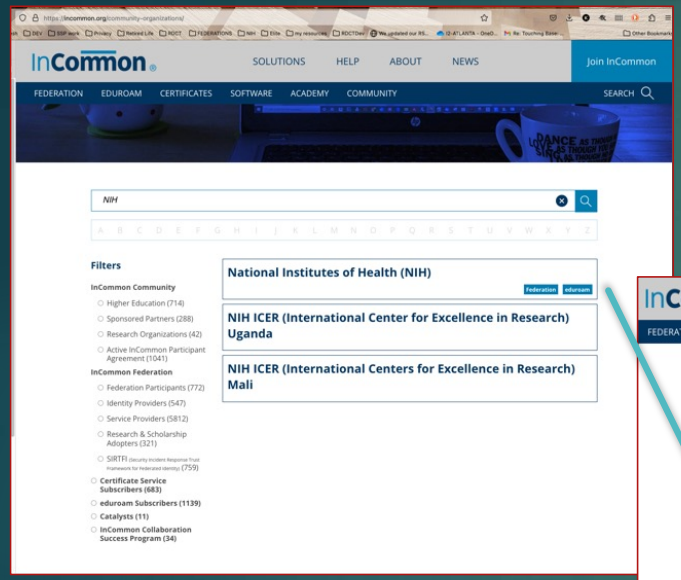
NAME	ENTITIES	IDP	SP	AA
eduGAIN	9290	5485	3825	2

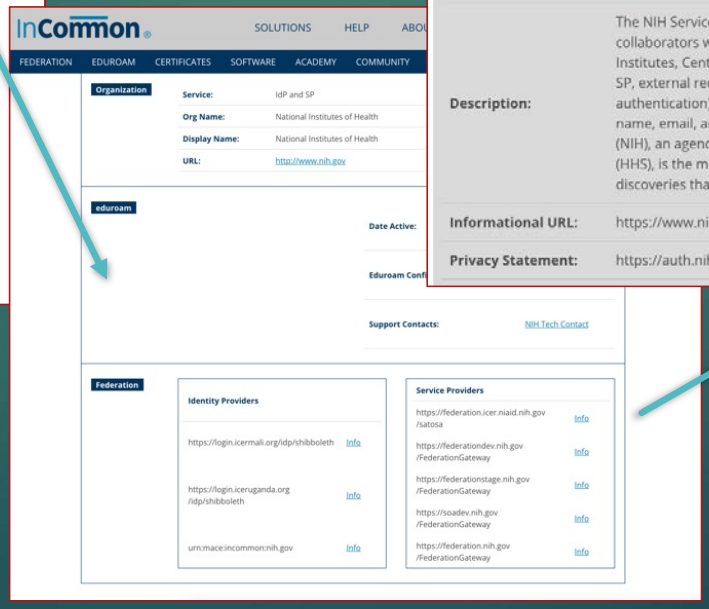
Total: 1 Export

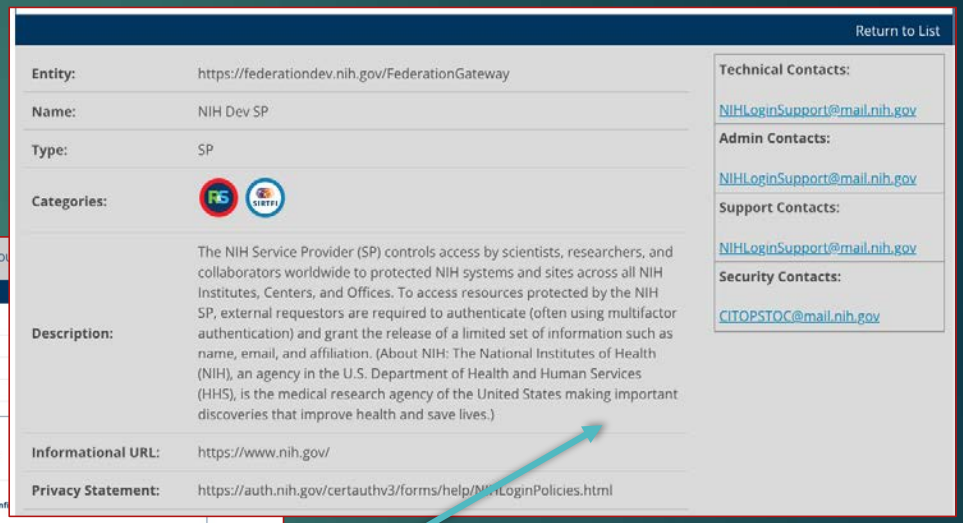
Federations map



Resource: InCommon Community Organizations
https://incommon.org/community-organizations/

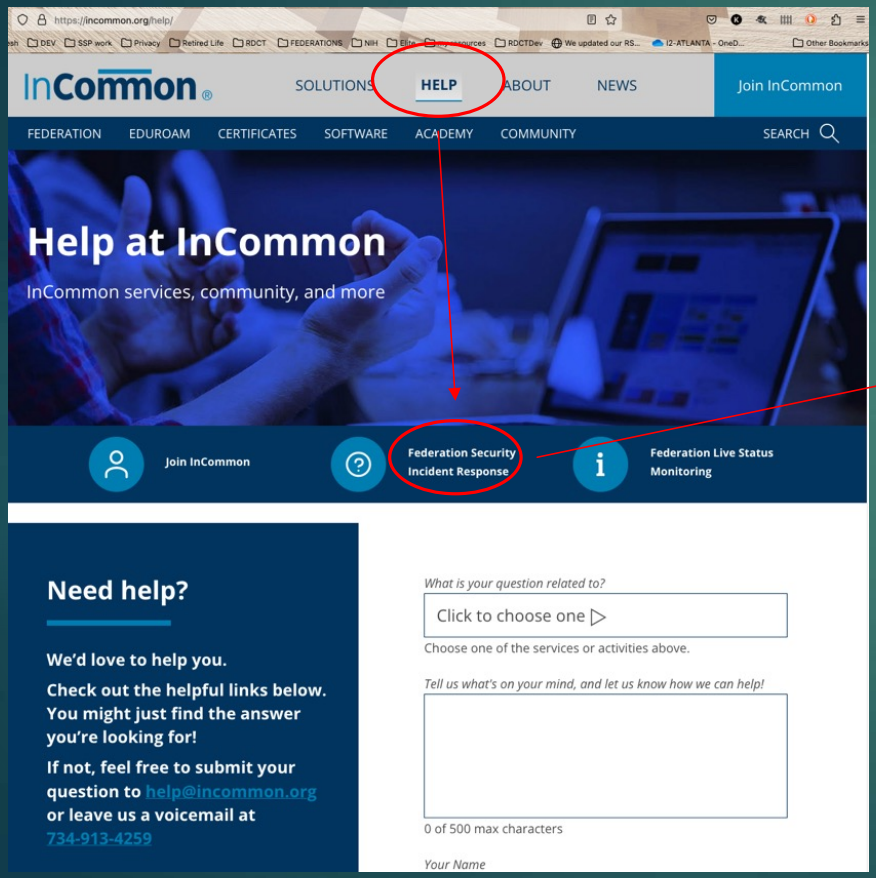


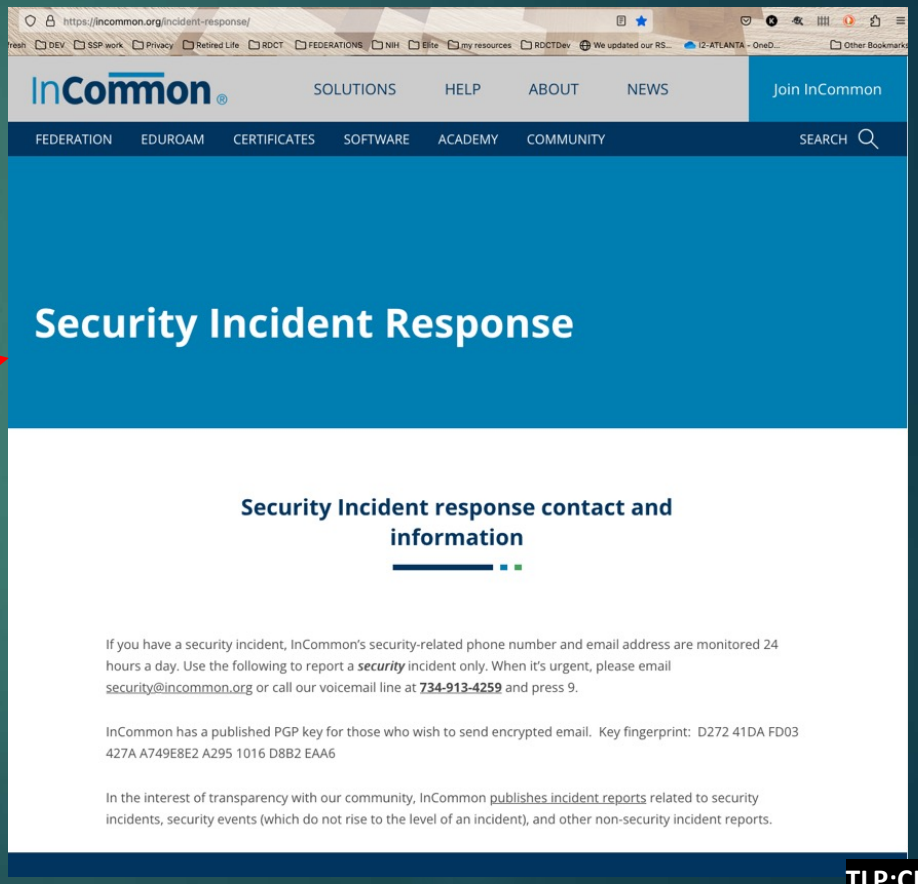




TLP:CLEAR

Federation Security Contact





TLP:CLEAR

Potential Scenarios

- Institutional server purposed as spam server from user accounts with federated access
- Phished user account discovered
- Compromised account used to scrape research library and publish to underground server
- Nation-state actor seeking national research
- A number of users' credentials compromised at a MitM attack at a conference
- Attacker uses compromised account to impersonate university leadership in attempt to deceive faculty at another university
- Insider threat
- User notified by an identity monitoring service that their credentials were found on the dark web

Every instance of a compromised account should prompt security team to ask:
"Does this account access the federation?"

TLP:CLEAR

Internal Documentation Components

- Topics to consider in local Sirtfi procedures:
  - Roles/Responsibilities
  - What is required to achieve/maintain Sirtfi
  - How to look up security contacts using the REFEDS MET tool
  - Responding to a request for help from a Sirtfi partner
  - Initiating a request for help to a Sirtfi partner
  - TLP reference readily accessible
- Security Incident Response Plan (SIRP) checklist
  - Add prompts to investigated if own accounts accessed SPs in the federation, if so, activate Sirtfi SOP

What NIAID International Team Did

- Wrote Standard Operating Procedure (SOP) on Sirtfi
  - What initiates the Sirtfi procedures
  - Engaging leadership prior to information sharing
  - Guidance on TLPs
- Created training session on SOP
- Modified existing Security Incident Response Plan checklist trigger on any activity involving federated users → directs use of the SOP
- Added required step in checklist to ascertain where federated user account has accessed (in order to accomplish Sirtfi notifications)
- Incorporated "Sirtfi" into internal security incident response plan tests and training
  - Trained on using the REFEDS MET tool to look up security contacts

Practical Recap

- Review all normative assertions and assess yes/no. If any "no", cannot assert Sirtfi
- Institutionalize Incident Response normative assertions
  - Update security incident response checklists or playbooks to identify or respond to Sirtfi events
  - Train security incident response team understands and knows how to honor TLP markings from other organizations
  - Update internal procedures to ensure your organization's interests are protected by using appropriate TLP markings when coordinating with external organizations
  - Train security incident response team on how to find security contact POC information during a security incident
- Publish security POC in metadata to the federation
- Publish the Sirtfi assertion

- Practice

InCommon CyberSecurity Cooperation Exercises 2022 Participants

CA Poly State University-San Luis Obispo

North Dakota State University

Rice University

University of Illinois

NIH National Institutes of Health

NIH National Institute of Allergy and Infectious Diseases

OCLC

CILogon

NON SOLUS
ELSEVIER

LIGO

TLP:CLEAR

InCommon Cybersecurity Cooperation Exercises

- Federation focused
  - Opportunity to practice “Sirtfi procedures”
- Participating Security Teams get to practice:
  - Narrated (simulated) scenario involving multi-organization security incident due to federated account compromises
  - Responding to exercise players from other organizations, reaching out through the published security contact
  - Looking up security contacts to affected organizations
  - Exposure to TLPs

TLP:CLEAR

2023 Exercise schedule – Nov 13-17

Mon 13 Nov (non play day)	Tue 14 Nov	Wed 15 Nov	Thu 16 Nov	Fri 17 Nov (non play day)
Orientation Zoom call: ALL participants	EX day 1 ECC Open STARTEX . . ECC Closed	EX day 2 ECC Open . . . ECC Closed	EX day 3 ECC Open . . ENDEX	Closing Zoom call to share observations: ALL participants welcome

- Most organizations have action/response in a single day → limited burden
- They won't know which day they'd get an inject → exercises responsiveness
- Three days allotted for time differences and to allow that we're not expecting after-hours actions → limited burden
- If an organization takes too long to respond such that it jeopardizes others' participation later in the week, ECC "narrates the story" forward if required → ensures all can play

TLP: CLEAR

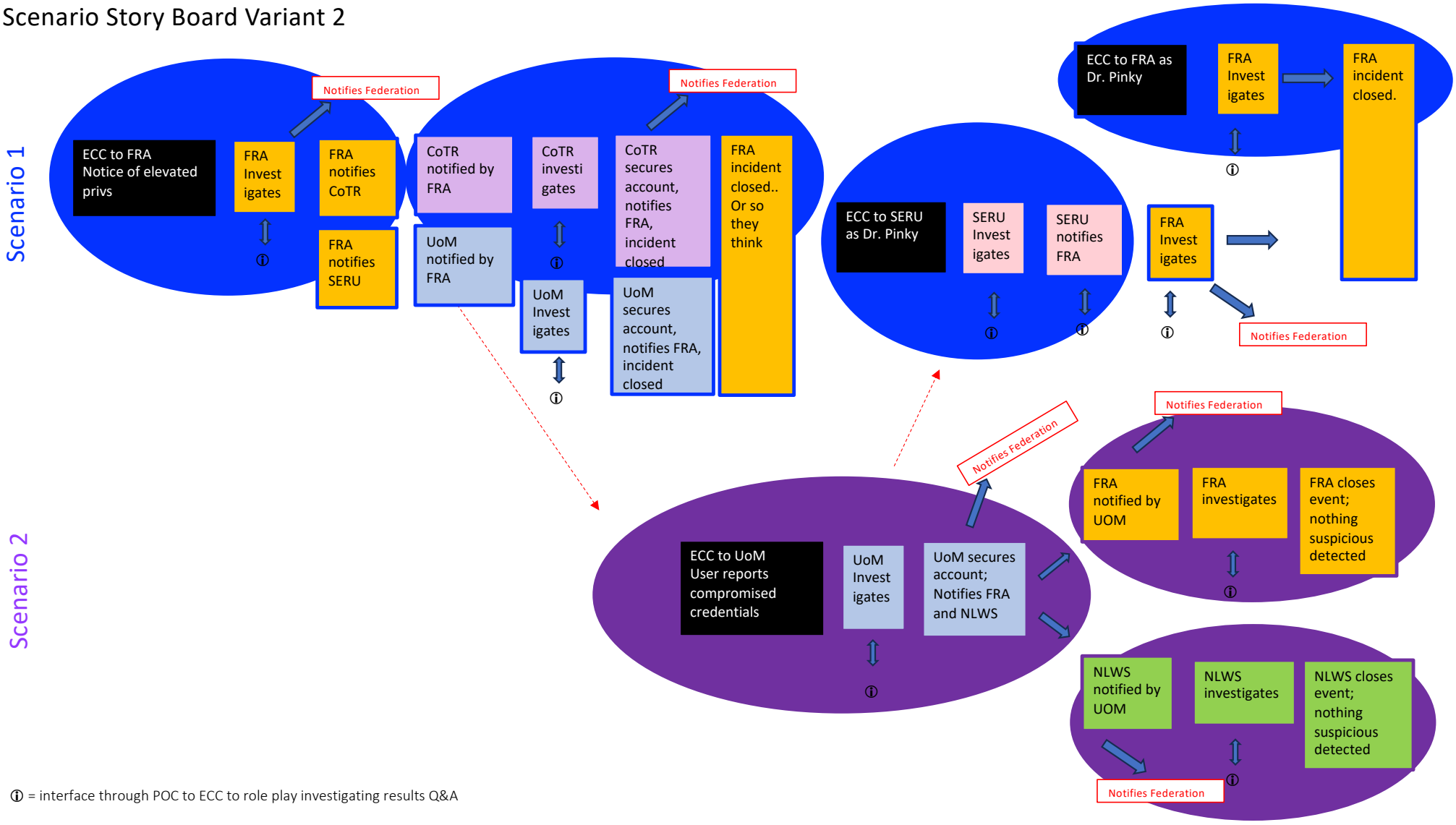
Sirtfi Exercise Planning Working Group (SEPWG) 2023 Enhancements

- Incorporated feedback from 2022:
  - This "How to Sirtfi" training
  - Open Survey to Community this Summer (closed)
  - Created practice script for 2024 SEPWG to add a traditional tabletop (in person or virtual) exercise for federation members
  - 2023 November 13-17's Distributed TTX – evolving scenario narrative, including InCommon's federation-level security contact

- Call for Participation is live until 29 Sep:
- Sign up at: https://forms.gle/aX5P3z3eNG55r4Fy5

TLP:CLEAR

Scenario Story Board Variant 2



ⓘ = interface through POC to ECC to role play investigating results Q&A

Takeaways

- Think about procedures and checklists "behind the scenes" in order to realize Sirtfi, and practice internally
- If your security team doesn't normally deal with IAM and federation, seek to increase their "federation mindedness" through awareness and training
- If your IAM team isn't routinely integrated with security, seek to increase their "security mindedness" through inclusion in internal security training

2024 SEPWG

- 2024's Sirtfi Exercise Planning Working Group (SEPWG)
- Benefits:
  - Your organization gets priority for participation
  - Learn exercise planning and conducting skills to take back to your own organization
  - Visibility and engagement with the community
  - The warm glow of contributing to community trust and preparedness

InCommon

CYBERSECURITY COOPERATION

VIRTUAL EXERCISE

THIS FALL|
NOVEMBER 13-17

SCAN THE QR CODE BELOW IF YOU WOULD LIKE TO PARTICIPATE. COMPLETE OUR EXPRESSION OF INTEREST FORM BY FRIDAY, SEPTEMBER 29, 2023

The purpose of this virtual desktop exercise is to practice using the Sirtfi framework to coordinate responses to a scripted scenario. Any Sirtfi-compliant organization (InCommon member or not) is welcome to join this exercise.

The total time commitment during the exercise week will be no more than an estimated four hours, including the time spent in the Monday orientation and Friday wrap up and slices of time participating in the scenario during the week.

https://forms.gle/aX5P3z3eNG55r4Fy5

Resources

- Sirtfi: https://refeds.org/sirtfi
- TLP: https://www.cisa.gov/tlp
- InCommon Security Incident Response Handbook
  https://spaces.at.internet2.edu/display/TI/TI.100.2
- Sirtfi's Guide for Federation Participants
  https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants
- How to Choose a Security Contact
  https://wiki.refeds.org/display/SIRTFI/Choosing+a+Sirtfi+Contact
- Sirtfi "What do you want for learning scenarios?"
  https://forms.gle/ceaKNm4oTnC3DhA98
- Sirtfi Incident Response email templates (look for IR on bottom left menu)
  https://wiki.refeds.org/display/SIRTFI
- 2023 Nov InCommon's Cybersecurity Cooperation Tabletop Exercise
  Sign up at: https://forms.gle/aX5P3z3eNG55r4Fy5

TLP:CLEAR