Sirtfi Exercise Planning Working Group

InCommon's 2022 Cybersecurity Cooperation Exercise

Kyle Lewis

TechEX/CAMP Week 2022

Certifiably
Sirtfiable

10,211

Agenda

- Lightning Refresher on Sirtfi
- The brief and illustrious history of the SEPWG
- Exercise Objectives
- Exercise Structure
- Exercise Feedback
- Way Ahead

Sirtfi Refresher

Why is Sirtfi important to us?

REFEDS Sirtfi -- Part of the InCommon Baseline Expectations for Members

But why is it important?

- Service Provider (SP) perspective: What if one of your user's accounts is trying to elevate privileges on my service?
- Identity Provider (IdP) perspective: what if one of my user's accounts becomes compromised?
  - What did that account access?
  - What other Service Providers (SPs)

We are in a trust federation. Trust involves risk.

How do we talk to each other when bad things happen?

REFEDS Sirtfi – What is it?

- REFEDS (the Research and Education FEDerations group) provides various common specifications for federations across the world to use to meet mutual needs, one of which is Sirtfi (Security Incident Response Trust Framework for Federated Identity)
  - Enables federation members to coordinate cybersecurity incident response
  - Builds information security trust between federation members

https://refeds.org/sirtfi

Asserting Sirtfi means three things

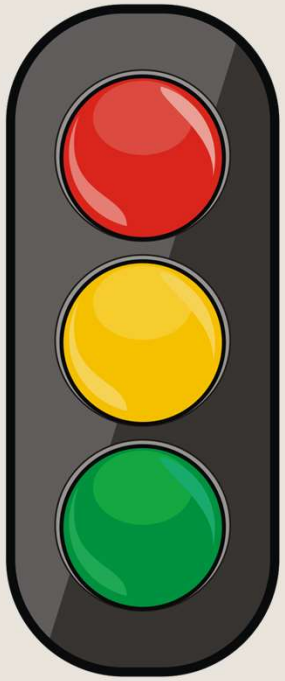
When you (as an entity) adds the Sirtfi attribute to the entity's metadata:

- You affirm "Yes" to normative assertions in the Sirtfi Framework
- You publish a Security Contact in your federation metadata
- You agree to use and honor the Traffic Light Protocol (TLP) [with other Sirtfi compliant organizations] for marking and handling shared incident response information

Traffic Light Protocol (TLP)

- 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/WHITE*** = **Disclosure is not limited.**

- Note: To keep trust, ensuring your own team knows how to HONOR this is as important as knowing how to mark your own information.



https://www.first.org/tlp

* Note TLP v2 vs v1 terminology

Why should we want to practice Sirtfi?

- Preparedness is as much about process and people as it is about technical skills and tools
  - Do the right people get notified? Do the right teams become engaged?
  - Did the right information get to the right person at the right time?

- Sirtfi is our federation framework for security response coordination

- People need to practice crisis response rather than assuming they will know what to do

- It's about checklists and procedures, especially for larger organizations.
  - It’s not just about having good security controls (those are important, but preemptive measures)
  - Not only about the technical skills of the staff to investigate and take action on the network (if the right staff is not energized, the right things won’t happen)

In the beginning… (of 2022) SEPWG was formed

- How to design a communication and coordination scenario for cybersecurity cooperation for:
  - Unknown amount of organizations
  - Unknown architectures for organizations who might volunteer to participate

- How prepare working group team to:
  - Discover/scope objectives
  - Land on an agreed approach to running exercise
  - Design, practice, and run a scripted scenario

Exercise learning objectives
Communication and Coordination

- InCommon's Goals - Federation Mindedness
  - Practice cross-organization coordination on cybersecurity scenario response using the Sirtfi Framework
  - Practice identifying need and knowing how to get another organization's security contact

- Participating Organization Opportunities
  - Practice responding to external notifications on cybersecurity events
  - Practice identifying and acting on situations that should prompt using the Sirtfi framework

What This Was Not

- Not a cybersecurity penetration test
- No actual network activity
- Not a test of technical abilities to do forensics or check audit logs

Roadmap to a Mult-Organizational Sirtfi Tabletop Exercise (TTX)

SEPWG Planning

Call for Participants, Summer 2022

Email to InCommon Participants Newsletter Article

24 May 2022

Phase 0
Practice Walkthrough

- SEPWG-internal 'mock' tabletop exercise
- Practice Exercise Control Center (ECC) roles

19-23 September

Phase 1
Communications Test

- Multi-organizational "communications exercise"

14– 22 Oct (5 sessions)

Phase 2
Exercise POC Orientation

- Orientation Sessions for Exercise POCs

Nov 14-18

Phase 3
Distributed TTX

- Multi-organizational multi-day scripted exercise

Roster

1. CA Poly State University-San Luis Obispo
2. CILogon
3. Elsevier
4. Laser Interferometer Gravitational-Wave Observatory (LIGO)
5. National Institute of Allergy and Infectious Diseases (NIAID) International Team
6. National Institutes of Health (NIH)
7. North Dakota State University (NDSU)
8. Online Computer Library Center Inc (OCLC)
9. Rice University
10. University of Illinois*

Exercise schedule – November 14-18

(times are in EST)

Mon 14 Nov (non play day)	Tue 15 Nov	Wed 16 Nov	Thu 17 Nov	Fri 18 Nov (non play day)
(1000): Orientation Zoom call: ALL participants welcome	EX day 1 ECC Open 0700 STARTEX . . ECC Closed 1700	EX day 2 ECC Open 0700 . . . ECC Closed 1700	EX day 3 ECC Open 0700 . . ENDEX	(1000): Closing Zoom call to share observations: ALL participants welcome

- Most organizations only had action/response in a single day; they did not know which day.
- Three days allotted for time differences; no expectation for after-hours actions.
- If an organization took too long to respond that it jeopardized others' participation later in the script, ECC "narrated the story" forward as required.

Three roles

- Exercise Control Center (ECC)
  - Volunteers from SEPWG
  - Provides scenario injects
  - Tracks script progress
  - Acts as ‘referees’/scenario narrators
- Exercise POCs
  - Appointed by volunteer organizations
  - Trusted Agent for ECCs
  - Facilitates/leads own organization’s participation
  - Liaison between ECC and Participants
- Exercise Participants
  - Determined by participating organization
  - Responds to scenario situations

Two teams

- 10 Organizations grouped into two teams
- Each group participated in their own self-contained exercised

Participating Organizations: 2 exercise roles

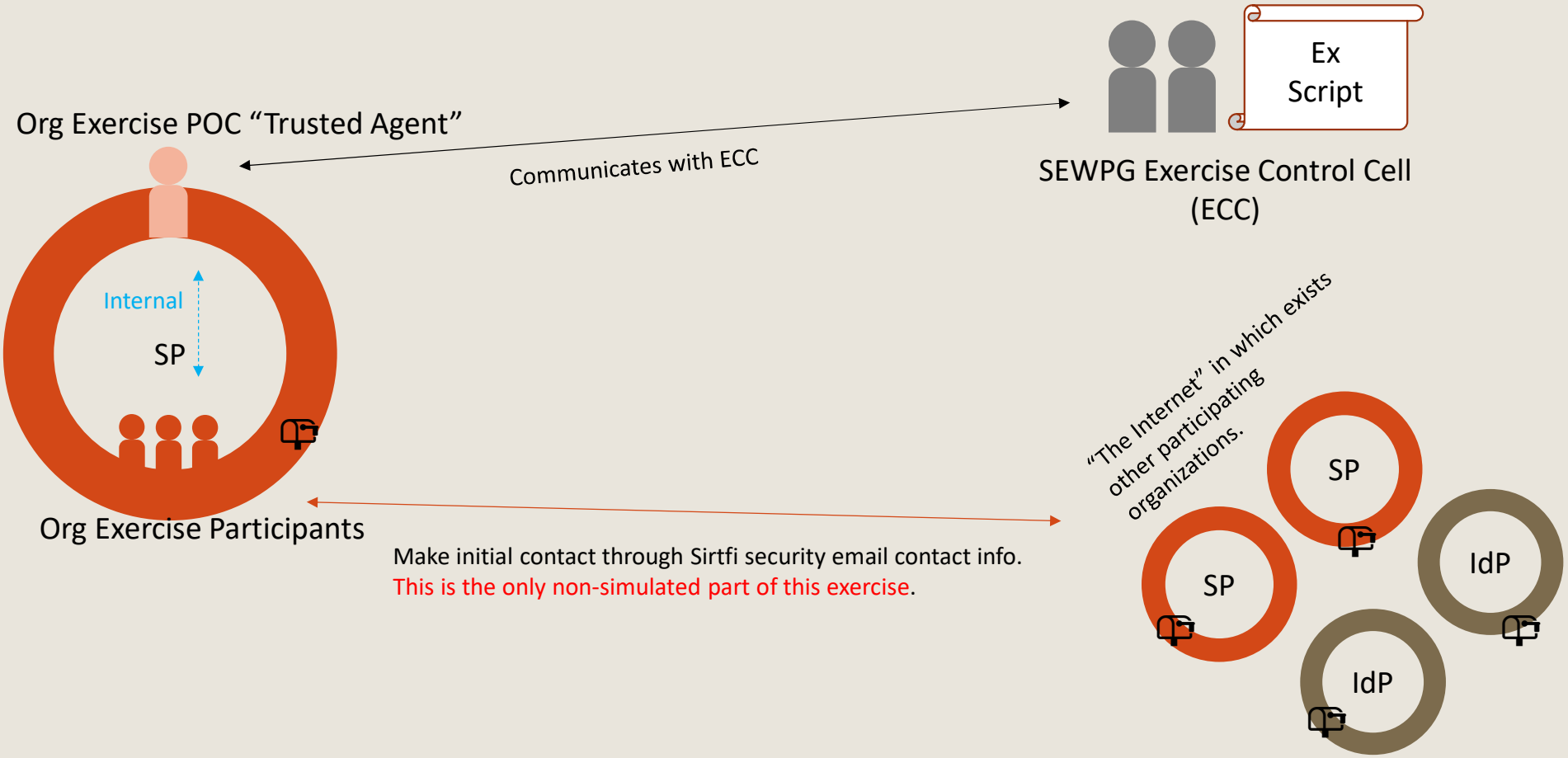
Org Exercise POC "Trusted Agent" = Local Facilitators to help ECC

- ONLY point of communication with ECC
- Relays exercise actions to ECC for tracking
- Makes Requests for Information (RFIs) to ECC on behalf of Participants
- Reads or sends exercise injects or response from ECC to Participants
- May role-play own organizations' internal roles not participating, if/as needed, to help own Participants

Org Exercise Participants

- Invisible to SEPWG ECC during the exercise
- How Participants and POC communicate is up to the organization
- How many Participants or few Participants is up to the organization
- At least one Participant must be able to receive non-simulated communications sent to actual Sirtfi Security Contact address

Each participating entity had two external lanes of communication



Simple Scenario Rotated Through SPs to IdPs

Team A - Inject 01 to SP1(LIGO)'s Exercise POC

To: [Warren A.]

Subject: EXERCISE - Inject 1 - STARTEX

Body:

EXERCISE EXERCISE EXERCISE

Your team reports that your monitoring tool alerts on activity from 104.219.236.100, a TOR exit node belonging to Datawagon LLC. Monitoring tool alerted because it indicated a successful connection/login. Initial investigation shows that the login was using a known, federated user: simu.lated@icermali.org, logging in from entity ID: https://login.icermali.org/idp/shibboleth

Further investigation reveals that the user was downloading unusually large volumes of data to that IP.

Exercise POC: Please reply to acknowledge response to ECC so we know the exercise is under way.

Team A – Inject 2 to IdP1 (NIAID IBRSP) (based on POC's request for information to ECC)

EXERCISE EXERCISE EXERCISE

Your own internal investigation confirms that the account for simu.lated@icermali.org is compromised. Your IdP's login logs for that user show logins from two IPs: an internal one that is yours and you recognize, and 104.219.236.100. An investigation into that user's laptop reveals they must have clicked on a link they shouldn't have, and a keylogger was detected when you forced a malware scan.

(In a real situation, your boundary detection system may have alerted on logins from that IP even before LIGO informed you of the activity; for the sake of the exercise narrative, assume it did not.)

Your own internal investigation reveals that simu.lated@icermali.org also accessed services tagged with entity ID https://cilogon.org/shibboleth

During the exercise – ECC Perspective

- Curveballs During Execution:
  - Real-world event took one university and Team A ECC lead out of exercise
  - One org's response was slowed due to security team (exercise participants) not knowing there was an exercise (deleted other playing org's email as spam)
  - One org switched Exercise POCs after exercise kickoff … arranged just-in-time orientation for new POC minutes before the script brought the scenario to their front door
- How did we do? (aside from exercisisms)…
  - Most organizations took advantage of the learning opportunity for internal practice
  - Most organizations were responsive
- How did we do? (exercisisms)
  - Some organizations' participants weren't aware of the exercise
  - Some struggled with exercise artificiality (this is normal, especially first time through)

General Reflections from ECC/SEPWG

- Scripting pace of two entities per day seems right
- Ask organizations' exercise POCs what timezones their participants are in during script development
- Evolve narrative richness of exercise injects
  - Timestamps for simulated activity, considerations for IPv6
  - Foster more back and forth participation between participants
- Ask orgs for primary and alternate POCs
- Increase emphasis on ensuring Participants attend kickoff sessions
- If organization provides multiple entities (e.g., 1 SP and 1 IdP), pick the one that fits the script rather than impact the organization's real-world responsibilities twice in the same week vs once for the others
- Next year the scenario needs to increase TLP-related tests in script

Participant Feedback

(Collected at Wrapup Meeting Friday 18 Nov 22)

Open Feedback

- Cal Poly: agrees letting participant team know in advance; took advantage of opportunity to review documentation with SOC; communication incoming was not TLP marked; REFEDS MET does not include security tag (bottom line: worthwhile; prompted internal impetus to do internal TTXs with lessons learned from here)
- OCLC: appreciated the chance to participate; wants more TLP injects/objectives; our emails don't come from our security email (it's a distro list); more emphasis on checking message authenticity; not all organizations will send from the security contact; add need to request information across organizational boundaries in script (bottom line: overall good exercise)
- NDSU: pri and alt POCs! Our team got ahead in shaping the narrative before the RFI went to the ECC and got the actual information; include timestamps; what about including IPv6? (overall: very good exercise)
- CILogon: definitely worthwhile; agree with pros and cons of distributed; interested in an in-person TTX/workshop at something like a TechEX); give feedback to InCommon and REFEDS on difficulty of finding security contacts
- NIAID IBRSP: overall good; we've done them internally in the past, but having real external players helped break an insular mindset of not being used to reach out externally; agree to wanting more TLP practice; also: we need to do more internally; found the process uncomfortable because it was not easy; what will help is practicing more
- Rice University: participant team not sure it was worthwhile; waited until day 3 for a very simple inject; didn't have to consult response playbook; looking for more in-depth "rich" inputs, with more urgency; POC thinks the exercise was good and has been encouraging TTXs; glad to see TTXs are started; interested in CILogon's suggestion of an in-person TTX; also, mini-TTXs: overall wants to see this practice continue and mature

Conclusions/Way ahead

- Success with opportunities to improve (first time through)
- All feedback indicated increased desire for this type of event

- As a community, we need more practice

- Recommendations:
  - Renew SEWPG with new call for volunteers for the WG
  - Mature exercise script and planning
  - Consider other ways to achieve community learning goals (e.g., smaller scenario more routinely; workshop or in-person TTX at a conference, etc)

Your SEPWG Team

Chair
- Kyle Lewis

SEPWG Core Team
- Prabha Manda
- Tom Barton
- Mark Baumgartner
- Jon Vasquez
- Jim Basney
- Ercan Elibol

SEPWG Supporting Members
- Albert Wu
- David Bantz
- Romain Wartel
- Hannah Short
- Maria Edblom Tauson
- Mark Williams
- Rob Z

Backup Slides

Lessons Learned – ECC Perspective
For next year's SEPWG

- Ask organizations' exercise POCs what timezones their participants are in (not always the same) so we can make sure more westerly zones get written in as … not the first.
- Scripting at a pace of two organizations per day seems right
- Need to improve narrative richness of exercise injects (e.g., timestamps for simulated activity)
- Ask orgs for primary and alternate POCs
- Communicate with POCs the need to make their participants aware and attend the kickoff orientation (some time lost due to some players not knowing there was an exercise)
- Give time/set environment for more back and forth participation between participants
- Internal to ECC: how to involve more ECC members given the distributed environment vs 1 person running script per exercise team (in our case 1 person running both scripts due to real world events)
- ECC did not see all traffic between organizations (sometimes, were informed by POCs that message happened, but didn't get actual message; hard to get a feel for how many used TLP markings)
- If organization provides multiple entities (e.g., 1 SP and 1 IdP), pick the one that fits the script rather than impact the organization's real-world responsibilities twice in the same week vs once for the others
- Next year the scenario needs to test TLP knowledge