2023-07-27 GSWG Meeting Notes

Meeting Date

27 Jul 2023 The GSWG meets bi-weekly on Thursdays at 11:00-12:00 PT / 18:00-19:00 UTC. Check the ToIP Calendar for meeting dates.

Zoom Meeting Link / Recording

Zoom Recording

Attendees

- Scott Perry
- Daniel Bachenheimer
- Neil Thomson
- Carly Huitema
- Keerthi Thomas
- Steven Milstein
- @Michael Parisi
- Kabir Maiga

Main Goal of this Meeting

Understand the opportunity to create a governance framework for dual-stack interoperability.

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
5 min	• Start recording • Welcome & antitrust notice • Introduction of new members • Agenda review	Chairs	• **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* • Suggestion by Neil Thomson about educating Governance Stack Working Group on mature governance, compliance and accreditation models in the marketplace to help adopt new standards for ecosystems to adopt • New Members: Ashley Rhéaume, part of the government of Quebec's team for digital identity, adopting the Trust over IP model
5 mins	Review of action items from previous meeting	Chairs	☐ Scott Perry : ☐ Talk to Judith Fleenorabout schedule changes but will maintain current time slot & Zoom link ☐ Ask Darrell O'Donnell & Antti Kettunen for feedback on Trust Registry Presentation Governance ☐ Ask Velocity Network Foundation architect of the registrar to also review ☐ Daniel Bachenheimer ☐ Ask Drummond Reed to reviewTrust Registry Presentation Governance and then ask Stephen Curran
5 mins	Announcements		1. Scott Perry a. Will be presenting at The State of Global Crypto Assets Regulation - Friday August 4 1PM ET (10AM PT). Registration b. Why Private Certification Authorities Need WebTrust Assessments
30 mins	Presentation from Michael Parisi (Schellman)	Scott Perry	Michael Parisi (Schellman) will speak about the governance process employed at HITRUST

5 mins	Any other business		
5 mins	- Review decisions /action items - Planning for next meeting	Chairs	Next Plenary meeting Thursday August 24, 2023 11:00PT

AI-Generated Meeting Notes

Courtesy of a Langchain conversation with ChatGPT after loading the transcript, presentation and chat messages.

Prompt: Find and define all acronyms and technical terms as accurately as you can. For example: What is CSF and AS?

CSF stands for Control Security Framework. It is a framework that focuses on control security and privacy controls. It is designed to be a compliance controls-based framework with prescriptive security and privacy controls. The CSF is certifiable and maps to over 46 authoritative sources. It is industry agnostic and can scale to any size organization. It is governed, managed, maintained, and regularly updated by HITRUST, the standards organization.

AS stands for Authoritative Sources. In the context of the HITRUST CSF, authoritative sources refer to the various frameworks, regulations, and guidelines that are included within the CSF. These sources provide the basis for the controls and requirements outlined in the CSF. Examples of authoritative sources mentioned in the context include ISO/IEC 27001:2013, EU GDPR, OCR Guidance for Unsecured PHI, and OECD Privacy Framework.

Please summarize Michael Parisi's presentation in 300 to 500 words. Always use the full name of acronyms like "Acronym Name (AN)"

The purpose of the Control Security Framework (CSF) is to provide a certifiable, risk- and compliance controls-based framework with prescriptive security and privacy controls. It is designed to help organizations manage risk and ensure compliance with various authoritative sources.

The CSF is developed, governed, managed, maintained, and updated regularly by the HITRUST standards organization. HITRUST is responsible for maintaining the CSF framework and its mappings to over 46 authoritative sources. They also qualify and oversee HITRUST Authorized External Assessors, ensure the assessment methodology is followed, and produce the HITRUST Validated Assessment/Certification Report. In summary, HITRUST is the organization that oversees and maintains the CSF framework and ensures its effectiveness and relevance in the industry.

Please summarize Michael Parisi's presentation in 300 to 500 words. Always use the full name of acronyms like "Acronym Name (AN)"

Michael Parisi's presentation focused on the organization I Trust and its role as a standards organization and certifying body. I Trust was founded in 2007 and aims to provide a standardized set of prescriptive criteria for information security and privacy programs.

Parisi explained that one of the key concepts in I Trust's framework is the idea of relying parties. Relying parties can be individuals within an organization or different organizations and institutions. These relying parties are the ones who require and accept high trust certifications.

Replace "I Trust" with HITRUST and summarize the presentation

Michael Parisi, a consultant and expert in cybersecurity, gave a presentation on HITRUST, a certification and standards organization. He explained that HITRUST was founded in 2007 and is focused on creating a standardized set of criteria for information security and privacy programs. The organization aims to consolidate various authoritative sources into one comprehensive framework.

Parisi mentioned that HITRUST offers a certification called the high trust certification, which is the only certification that satisfies federal requirements and enables organizations to reduce cybersecurity insurance premiums. Parisi also emphasized the importance of threat intelligence in the HITRUST framework and its role in helping institutions gain visibility with underwriters. He mentioned the wide acceptance of HITRUST by organizations like Zurich, Chubb, and AIG. Parisi's personal involvement with HITRUST further adds credibility to his insights and recommendations.

Elaborate further

Threat intelligence plays a crucial role in the HITRUST framework by providing organizations with valuable information about current and emerging threats. HITRUST incorporates regular reviews of threat intelligence data, including indicators of compromise (IoCs) and indicators of attack (IoAs). This allows organizations to stay updated on the latest threat landscape and ensure that their control requirements are evolving to address these threats.

By leveraging threat intelligence, HITRUST enables organizations to implement cyber threat-adaptive controls. These controls are designed to continuously address emerging threats and are regularly updated in each HITRUST assessment. This ensures that organizations are taking a proactive approach to cybersecurity and risk mitigation.

In terms of cybersecurity insurance premiums, the visibility provided by the HITRUST framework is valuable to underwriters. By demonstrating that they have implemented the appropriate controls based on threat intelligence, organizations can reduce the likelihood of a data breach and the associated costs. This can lead to a reduction in cybersecurity insurance premiums or allow organizations to negotiate higher levels of coverage.

It's important to note that the specific impact on insurance premiums may vary depending on the insurance provider and the organization's overall risk profile. However, having a HITRUST certification can provide stronger assurances to stakeholders, including insurance underwriters, that the organization has taken proactive measures to protect sensitive information and mitigate cyber risks.

What was the most popular topic of conversation?

The topic that dominated the conversation was the adoption and governance of the High Trust certification framework in the healthcare industry.

Slides

Trust Over IP HI...ST Overview.pptx

Screenshots/Diagrams (numbered for reference in notes above

Action Items