

## **Solution Innovation Case Study: Implementing the World's Only Privatized Virtual Sensitive Compartmented Information Facility (SCIF) for Sensitive Information Conference Calls**

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved to help security practitioners expedite choosing a trustworthy risk mitigation vendor with confidence given the myriad of viable options in the marketplace. Proven Solution Innovation Case Studies help to evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This case study demonstrates Hercules Secure Inc.'s innovative capabilities to deliver the most secure video conference platform for this global pharmaceutical end user. This was validated by the Security Executive Council and the client end-user.

### **Risk Issues and Mitigation Opportunities:**

- Currently not using a secure online meeting tool for sensitive calls/meetings
- Concerns over video conference communications security and exposure to unauthorized access by internal/external individuals and adverse foreign actors (e.g. for “ghost call” attacks by adversaries or antagonists <https://cybersecuritynews.com/ghost-calls-attack>)
- Legal risk and compliance concerns given the sheer volume of the end user’s video conference communications. The American Bar Association (ABA) demands lawyers “make reasonable efforts to prevent the inadvertent unauthorized disclosure of or unauthorized access to information relating to the representation of the client.” (ABA Model 1.6c). Further, as articulated in ABA Formal Opinion 477R, the opinion discusses the ethical obligation to “understand and use reasonable electronic security measures that would prevent unauthorized access to client information”. Further, under (Rule 1.6a), the ABA has implemented a variety of changes enfoldng the attorney’s obligation to maintain client confidentiality with respect to the use of technology and to maintain “the requisite knowledge and skill” in keeping abreast of changes in the law and its practices to include the benefits and risks associated with relevant technology.
- Health Insurance Portability and Accountability Act (HIPAA) risk and compliance concerns. HIPAA Security Rule, 45 CFR §164.312(e)(1) mandates technical safeguards to protect electronic protected health information while it is transmitted. Additionally, HIPAA requires strict access controls and identity verification for any system that accesses ePHI. Under 45 CFR §164.312(a)(1) and §164.312(d) it requires covered entities to implement access controls and verify user identity to ensure only authorized individuals can access protected health information. Further, HIPAA requires confidentiality and limits disclosure of ePHI across electronic communications. Under HIPAA Privacy and Security Rules at 45 CFR §164.306(a) and §164.502(a), requires covered entities to protect the confidentiality and integrity of ePHI and limit unauthorized use or disclosure. Unauthorized disclosure of HIPAA-protected health information (PHI) can trigger significant federal civil and criminal penalties, and—depending on the state—additional fines, damages, and even criminal charges.

**Solution Innovation Case Study:  
Implementing the World's Only Privatized Virtual Sensitive  
Compartmented Information Facility (SCIF) for Sensitive Information  
Conference Calls**

**Solution Requirements:**

- Easy to create a meeting invitation and use the video conference platform for all users.
- Complete control over access to meetings. Only meeting organizers can permit user access to individual meetings.
- Relinquishing control of the server to the client once onboarding is complete.
- Clear identification of identity of platform attendees on each online meeting.
- Government grade encrypted meetings
- Void of AI/machine learning, recording, data mining, voice replication solutions

**Delivered:**

- Meetings take seconds to create and send out invitations.
- Hercules reduces HIPAA risk and improves HIPPA compliance by:
  - Providing a closed, private communication platform that prevents forwarding, resharing, or unauthorized entry, significantly reducing the risk of interception or exposure during electronic delivery of medical records.
  - Enforcing locked, identity-verified access, explicit approval of participants, and isolated client environments, directly supporting HIPAA's technical safeguard requirements.
  - Not recording, storing, transcribing, or processing communication content, helping ensure electronic medical information is not retained or inadvertently disclosed beyond its intended purpose.
- Provided a virtual Sensitive Compartmented Information Facility (SCIF)
- Improved ABA compliance.
- The only meeting record, to include attendees, is in the calendar entry which can be manually deleted as deemed necessary.
- Provides alerts if a conference call breach is attempted to include name, email address, and physical location (Latitude/Longitude) of the subject.
- Easy access from all devices and search engines.
- Communication security is unaffected by the location of the participants (airport, hotel, open Wi-Fi etc.)

**Outcome and Benefits of Service:**

- Hercules delivers ROI by preventing the financial, legal, operational, and reputational losses that occur when sensitive communications are compromised. Avoiding even one data breach involving confidential discussions can save millions to hundreds of millions.
- Provides complete assurance of online meeting privacy and confidentiality.

**Solution Innovation Case Study:  
 Implementing the World’s Only Privatized Virtual Sensitive  
 Compartmented Information Facility (SCIF) for Sensitive Information  
 Conference Calls**

- The end user’s online meeting brand protection/privacy confidence was 1 out of 10 before and 9.5 out of 10 after implementing Hercules.
- Quantitative benefits (dollars, deals closed due to increased meeting confidence, near misses with bad actors trying to get into the meeting, etc.) are measured by the depth of a company’s exposure to breach (litigation, brand damage, stock drop etc.).

*“As a former FBI Senior Executive and Vice President of Global Security for a global pharmaceutical organization, I’ve seen firsthand that secure and confidential communication is foundational to effective risk management and operational resilience. As one of Hercules’ initial test users, I found its video and audio performance to be exceptional—but more importantly, I had complete confidence that every conversation was fully protected. Hercules establishes a new standard in secure video conferencing and is essential for corporate legal, security programs and GSOCs. It enables protected collaboration across legal and compliance matters, mergers and acquisitions, strategic and financial planning, insider-risk management, crisis and incident response, investigations, executive protection operations, product development, customer engagement, and board-level deliberations.” – Vice President of Global Security*

**SIP Case Study Authentication Process**

This process was overseen by a Security Executive Council subject matter expert with 20+ years of experience in developing and leading people and asset protection programs as a trusted security advisor for global, multinational organizations. **Client end-user authenticated by the SEC January 2026.**

Note: The Security Executive Council's Solution Innovation case study represents a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.

**A General Comparison of Competition**

<b>Client Service/Resource Attributes or Capabilities</b>	<b>Hercules YES/NO</b>	<b>Company A YES/NO</b>	<b>Company B YES/NO</b>	<b>Company C YES/NO</b>	<b>Company D YES/NO</b>
Dedicated Private Server	YES	NO	NO	NO	NO
No Recording/No AI/No Transcription	YES	NO	NO	NO	NO
Guest approval + Identity Verification	YES	NO	NO	NO	NO

**Solution Innovation Case Study:  
 Implementing the World's Only Privatized Virtual Sensitive  
 Compartmented Information Facility (SCIF) for Sensitive Information  
 Conference Calls**

OS-Hardened & Monitored Services	YES	NO	NO	NO	NO
True Environment Isolation	YES	NO	NO	NO	NO
ZERO Data Retention	YES	NO	NO	NO	NO
Ultra-Sensitive Use Ready	YES	NO	NO	NO	NO
Broad Ecosystem/Integrations	NO	YES	YES	YES	YES
Scale/Meeting Flexibility	NO	YES	YES	YES	YES

See other case studies and learn more about the SIP Program here:  
<https://www.securityexecutivecouncil.com/solutions/vendor-innovations>