

UK TOP SECRET

The maximum [classification](#) allowed on GCWiki is **TOP SECRET STRAP1 COMINT**.

# VoIP NSA alias

From GCWiki

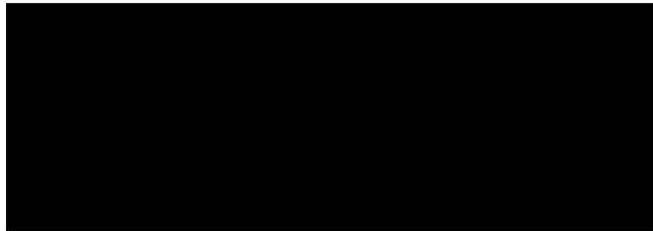
Jump to: [navigation](#), [search](#)

SAMESHEET is a group for discussing media over packet in the SIGINT community. It initially dealt with just VOIP, but has expanded its scope. These notes get mailed out after each monthly meeting (usually held the third Wednesday of every month.) Look for reminders, calls for Agenda items, and notes on the voip@nsa alias. This alias can be joined at: [\[1\]](#)

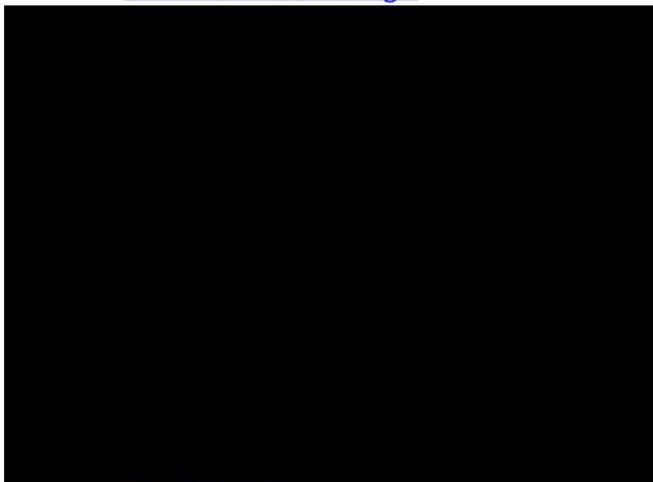
**This GCHQ record of SAMESHEET meetings is ended in favour of NSA's version** at: [\[2\]](#).

I encourage all those who have an interest to join NSA's alias directly.

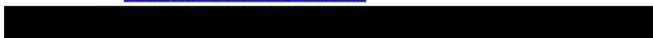
## Contents



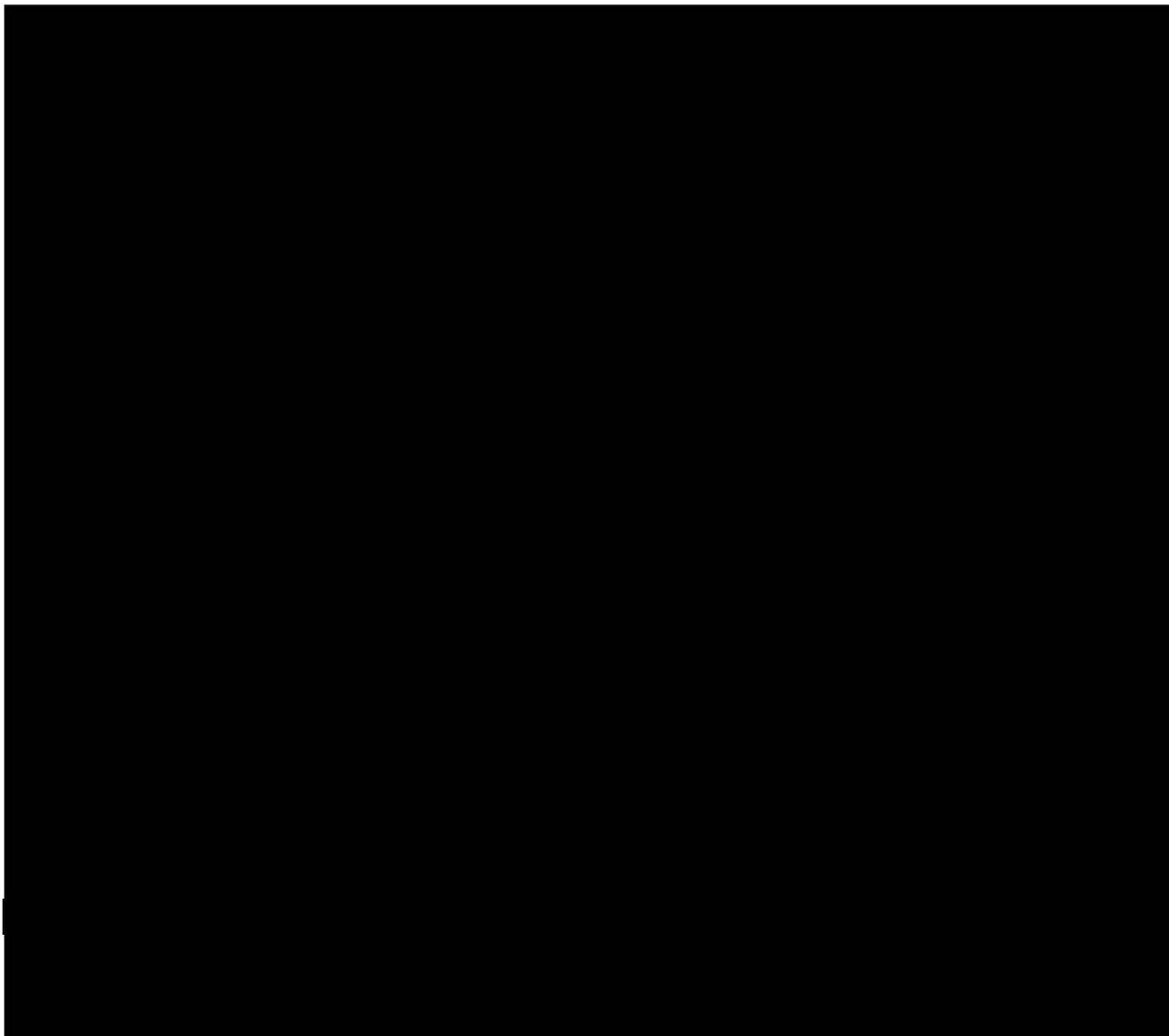
- [4.3 IETF San Diego](#)



- [7.5 VON Boston](#)



- [8 IETF SIP, Trip Report](#)



## [\[edit\]](#) IETF San Diego

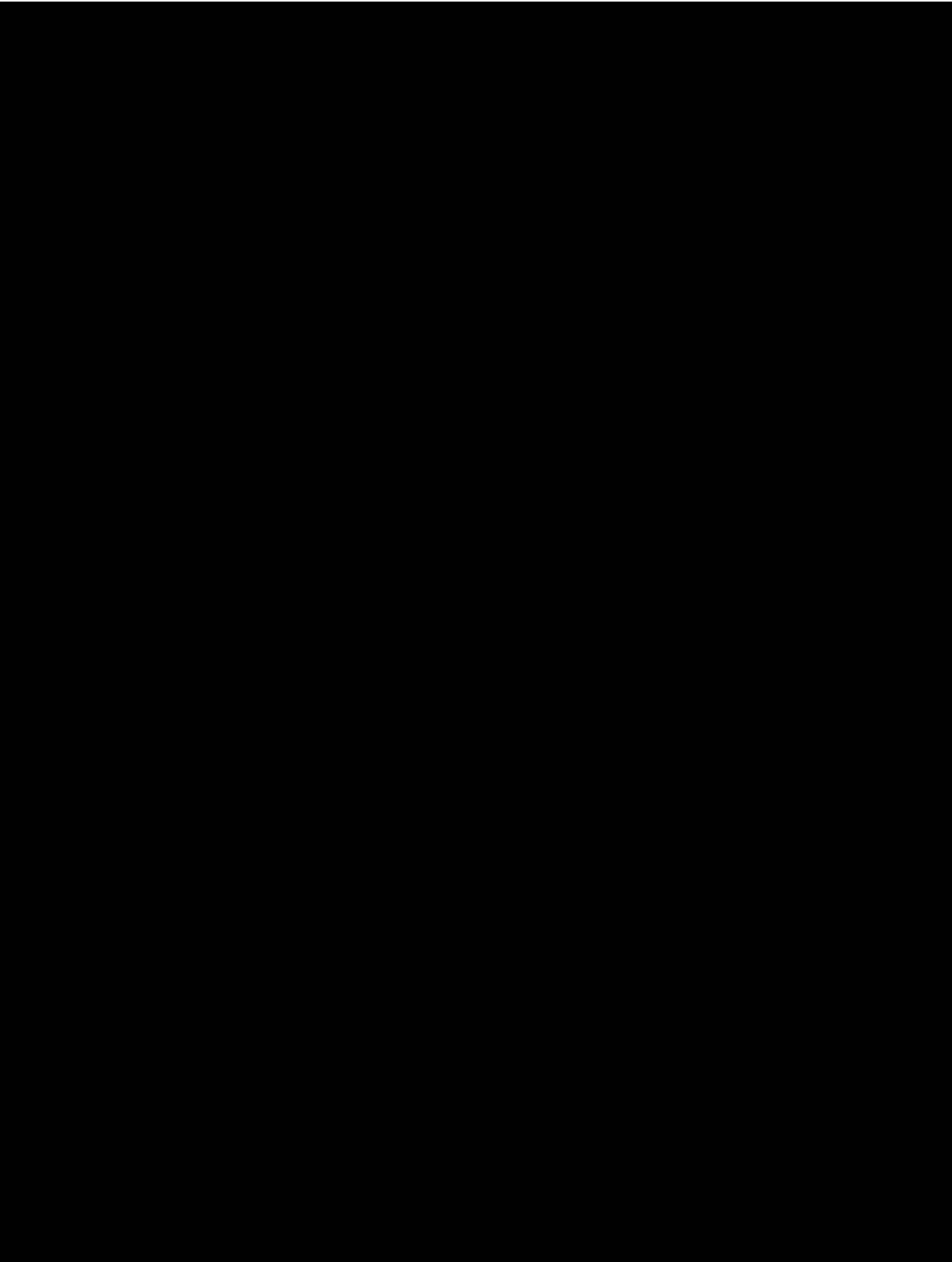
(S//CCO) ██████████ opened the meeting with a synopsis of the highlights from this past months IETF meeting in San Diego. The IETF has been at the forefront of Internet standards development over the last few decades and is responsible for the SIP standard and future extensions. Of Sigint significance, ██████ passed on a few items such as the Globally Routable User-agent URI (GRUU) which is intended to represent a specific piece of hardware or software instance for selection.

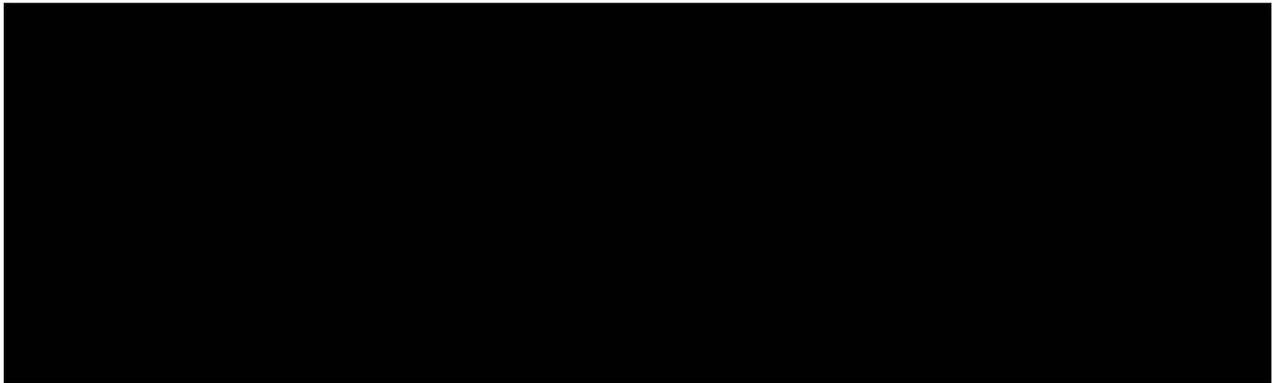
Implementations of the GRUU have been slowed due to privacy concerns.

Additionally, new session policy extensions may improve our ability to passively target two sided communications by the incorporation of detailed call information being included with XML imbedded in SIP messages. On the security front, SRTP has been slow in the uptake due to key management limitations. At the meeting however there was a significant amount of discussion surrounding Zimmerman's (of PGP fame) ZRTP showing an easier to implement solution. SPEERMINT has been very active as well discussing standards for multi and unilateral peering as well as initial interest in standardization of the Session Border Controller services. Finally, peer-to-peer SIP is heating up which may lead to the formation of a new IETF

working group. This meetings full minutes as well as previous meetings will be posted to: [REDACTED]

<< [REDACTED] >> In addition to [REDACTED]  
[REDACTED] also attended





## [\[edit\]](#) VON Boston

(U//FOUO) Three attendees of this months meeting, [REDACTED] and [REDACTED] were able to attend this years Fall VON in Boston. [REDACTED] notes can be found at:

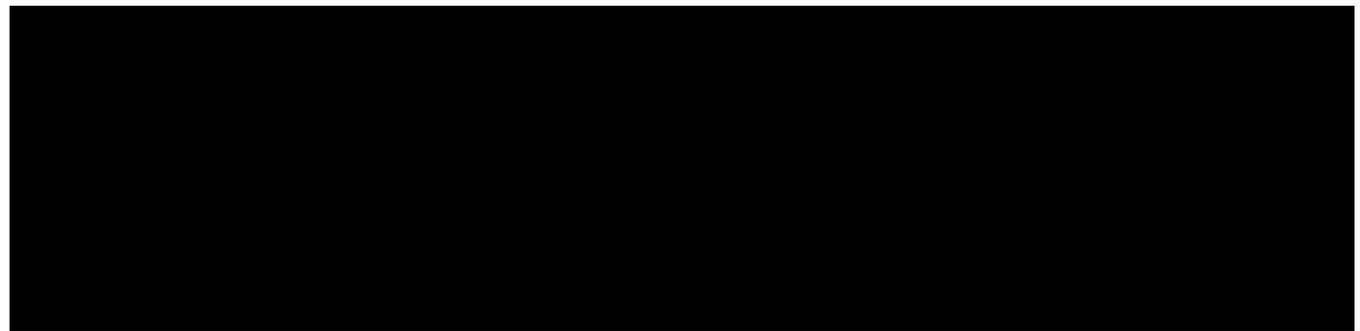


### Next Meetings

October 18th - Room 3W083-2 (tentative) - 1:00pm - 3:00pm Featured topic - IAD VoIP Vulnerability Analysis

November 15th - Room 2W037-2 - 2:00pm - 4:00pm Featured topic - TBD - Please send suggestions/requests!

## [\[edit\]](#) Attendees:



Thanks, [REDACTED]

## [\[edit\]](#) IETF SIP, Trip Report

18/09/06 (S//SI) X71's Network convergence project has posted a trip report from July's Internet Engineering Task Force, by [REDACTED]. This report describes developments at the IETF in SIP and SIP-related protocols. This report includes observations on SIP-based location conveyance (p. 6 and 10), new media types (p. 11), migration of communication services to SIP (p. 9), plans/issues for

media encryption (p. 12-14), and information on pace of service provider adoption of SIP for presence and instant messaging (p.15-16). Sprinkled throughout are observations on how user identifiers may be changing (p.5,7,8). The executive summary gives thumbnail sketches of each of these.

(U) The report is available on the "trip reports" section of our web site:

[REDACTED]

[REDACTED]

[REDACTED]