

**Technology Services Committee
IPTel Workgroup Meeting Notes
January 23, 2007**

Attendees: Alan Friedman, Mary Hanson, Cal Rogers, Bob Raetz, Christopher Flores, Terri Bollinger

Action Items:

- **Christopher Flores present, at the March 28 IPTel Meeting, DOI IPTel-related Hardware Information to the Team**

Project Update:

Christopher Flores, Delegata, walked through a PowerPoint presentation which outlined Department of Insurance's (DOI) Telecommunications Infrastructure Replacement Project (TIRP) progress since the last IPTel meeting. Mr. Flores reported that the RDD Phase has been delayed due to a need to strengthen the Business and Technical Requirements defined earlier in the project. He walked the Workgroup Attendees through the Timeline and Project Accomplishments/Next Steps. Mr. Flores stated after the Provisioning and Installation Phase, DOI has planned a three month pilot. A question arose about the network and routers/switches. Mr. Flores reported that DOI is working on upgrading the network as a separate project and routers/switches are the joint responsibility of DOI and DTS, not the vendor. During pilot, if network deficiencies create performance issues, DOI will work with Cisco and DTS to resolve. Mr. Flores further stated that during pilot the full existing system will remain operational. During transition DOI will have interoperability between old and new system. Questions regarding the hardware arose. Mr. Flores said he would present at the next meeting information regarding hardware. Mr. Flores proceeded to present the Testing Methodology and ended with a discussion on an article from Homeland Security on VoIP Service.

Mr. Flores reported that the Homeland Security article, "VoIP Service: Fraught with Vulnerabilities and Susceptible to Fraud" is unduly alarmist and highlights a pathological situation. He went on to state the fraud involved unauthorized access to VoIP Service Provider media gateways to convert VoIP calls into PSTN traffic. It involved 4 independent vulnerabilities identified as A, B, C, D. These vulnerabilities ranged from unprotected routers to VoIP Service Providers (VSPs) without any security measures. These vulnerabilities are highly unlikely in current deployments. He concluded by reporting the CDI TIRP deployment is protected against this type of fraud for two reasons:

1. The TIRP deployment does not send VOIP traffic over the Internet. VoIP traffic is limited to CDI LAN and WAN. All external calls are through the PSTN.
2. CDI maintains extensive security measures (firewall, anti-virus, IDS, IPS etc) that meet all the DHS/FBI recommendations.

Round Table:

The attendees further discussed VOIP being utilized in other departments.

Next Meeting:

March 28, 2007, 10:30-12:00. 2525 Natomas Park Drive, Suite 100, Conference Room 1.