

CTS Advisory Council

April 4, 2012
1500 Jefferson Street
Olympia, Washington

Welcome/Introductions

Dan Mercer, Consolidated Technology Services (CTS), provided an overview of the agenda.

Attendees: Grant Rodeheaver, Co-Chair (WSDOT), Ron Seymour (DFI), Doug Hoffer (DOC), Sue Langen (DSHS), Marcus Bailey (DOL), Richard Campbell (HCA), Rob St. John (OCIO), Mike McVicker (ESD), Mike Ricchio (CTS), Debbie Stewart (ECY), and Frank Westrum (DOH).

Security Operations Center (SOC)

David Morris (CTS) provided an overview of the Security Operations Center (SOC). The mission of the CTS SOC is to provide centralized information sharing, monitoring, and analysis of Washington State security posture. The SOC was created in October 2011 and their tactical plan includes the following:

- 1) Establish the SOC within CTS (complete);
- 2) Improve Situational Awareness by adding IPS and SIEM (in process);
- 3) Centralize Security Incident Management; and
- 4) Centralized Risk Analysis.

The SOC provides:

- Near-Real-Time Alerting;
- Risk Analysis;
- Security Incident Response;
- Vulnerability Management; and
- Education (includes developing materials and training).

Training courses are sponsored as part of the education SOC provides. The next training opportunity is scheduled for April 25-26 on *Digital Evidence Seizure and Forensic Tools for Everyday Forensics*.

The SOC will produce a twice-monthly Cyber Health Report covering the 1st – 15th and 16 – end of each month. The report includes an Executive Summary capturing interesting events for the period of the reporting cycle, as well as short snapshot briefings on different security topics.

SDC Update

Dan Mercer (CTS) reviewed the SDC Re-Scoped projects with an emphasis on reducing the load on the cooling systems in OB2.

April activities include:

- Restart SDC Project:

- Re-scope Projects;
 - Update Charters;
 - Severity & Risk Assessments; and
 - Update the investment plans for Network, Security, and Storage.
- Focus on Facilities project (critical path).
 - Initiate “Reduce Heat” project.

An equipment template was sent to the OB2 tenant agencies asking to identify the following and return the template to CTS by April 22:

- Equipment already planned for shutdown in near future as result of ongoing virtualization;
- Documentation of least critical equipment that can be shutdown in an emergency, in order to protect mission-critical systems from heat damage; and
- Agency coordinator name.

Any OB2 tenant agencies that did not receive an equipment template should contact Dan Mercer.

SDC – Data Hall 1 will be ready to accept customer equipment by year-end 2012.

Action Items

Send an electronic copy of the most recent Cyber Health Report to the Advisory Council members and the Agency CIO’s.

Dan Mercer will follow up on questions regarding background checks for staff for Data Hall 1. This topic will also be a future agenda item.

Next Meeting

May 2, 2011
Conference Center Room 2331
1500 Jefferson Street
Olympia, WA