



IT Program Assessment

NPPD- Critical Infrastructure Warning Information Network (CWIN)

Review

The DHS Chief Information Officer (CIO) conducted a comprehensive review of the NPPD- Critical Infrastructure Warning Information Network (CWIN) program on May 14, 2010. The CWIN is the Department's stand-alone, independent network that connects the government and critical Information Technology and Communications, sector owners and operators to coordinate recovery and reconstitution following disruption (primarily due to a cyber attack) of the public switched network (PSN) and internet for voice and data services. It is a contingent "insurance policy" for a low probability, high consequence event. CWIN does not connect to the public internet, the public switched network (PSN), or any other public or private network due to its purpose of avoiding disruption through a cyber attack.

CWIN was established in 2001 at the direction of the National Security Council, by the National Communications System. In 2004, DHS leveraged CWIN to extend connectivity to 51 state Emergency Operations Centers (EOCs). Currently, the CWIN system is in operations and maintenance lifecycle stage, serves 163 members in federal and state government Emergency Operations Centers (EOCs), Information Sharing and Analysis Centers (ISACs), and the private sector, with client terminals and/or VoIP phones deployed at about 160 sites.

Findings during the review are as follows:

- CWIN is managed by NPPD and supports the I&A and OPS components of DHS.
- CWIN is not funded past the end of FY2010. Current NPPD funding sustains baseline (connections to CWIN partners such as Federal and State EOCs).
- I&A provided funding, through June 2009, for classified circuits to EOCs and Fusion Centers to classified I&A laptops.
- The DHS OPS component desires the Secure Video Tele-Conference (VTC) capability offered by the program, yet does not have the available funding to support this requirement.
- CWIN currently has no operational Continuity of Operations (COOP) site.

Assessment

From a program management perspective, CWIN appears to be well-managed and is operating effectively, given the resources applied to the program. CWIN provides a critical capability that ensures network connectivity and security in the event of a cyber attack. As a result of the review, the DHS CIO recommended that the OneDHS Emergency Communications Committee (ECC) conduct a comprehensive analysis to determine the future of the program given the funding shortfall and supposed mission criticality.

Score: 4