IT Program Assessment
FEMA- Federal Emergency Management Agency
Infrastructure Program

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) conducted a program health review of the Federal Emergency Management Agency (FEMA) Infrastructure program. This assessment represents the program's status through March 2012.

Description and Background:

The FEMA Infrastructure program supports implementing IT solutions, managing, directing, and supporting the daily operations support of the FEMA telecommunications and computing network. A full range of telecommunications and computing network services, including cyber security and network infrastructure management and monitoring, are required for day-to-day operations within FEMA and throughout the life of a disaster or emergency.

FEMA Infrastructure has nine services essential to the daily operations of the organization. These services include Network, Email, Help Desk, Data Center, Desktop, Site, Video, Voice, and Wireless.

In its current state, the Network Managed Services (NMS) system does not meet all of the Fault, Configuration, Accounting, Performance, Security (FCAPS) model criteria as described in the International Organization for Standardization (ISO) Telecommunications Management Network model. The program has completed an analysis of network field operations to upgrade the infrastructure. This analysis will be used to present a business case to the FEMA IT Governance Board for an estimated amount of $26.7M as stated in last year's slide submission.

Risks and Issues:

- If the component does not invest in Network Infrastructure Life Cycle Refresh then the viability of the FEMA NMS remains at significant risk
- If the impact on the help desk function is not carefully managed and prioritized, activities such as email migration, disaster activity, and the addition of new customer support areas is at risk.
- If the agency does not provide for equipment refresh, desktop support will be hampered and have limited value.
- If IT Infrastructure in the buildings within the National Capital Region (NCR) is not upgraded, the network may be at risk.
- If aging and end-of-life audio/video (A/V) and network enterprise equipment is not replaced, frequent system outages will continue to occur. This also applies to our Network and Security Operations Centers (NOC/SOC) as all internal and enterprise network, security-related hardware and systems which also supports

demilitarized zones (DMZs) are at end of life or in an aging status. They are included below.

- The Network and Private Internet eXchange (PIX) firewalls are at End of Life and will cost $400 to replace.
- The Intrusion Detection Systems (IDS) and Defense Center Console are aging equipment and will cost 65 thousand dollars to replace.
- The Cisco Network Admission Control (NAC), which enforces access privileges rights when a device is attempting to connect to the network, is not a part of the FEMA enterprise network and its absence is considered a major risk. It will cost $3 million.

- If staff levels are not adjusted for day-to-day operations and contingencies, the program may not be able to continue normal service when staff are deployed to contingency sites.

Mitigation Strategy:

Here are the program's mitigation strategies for each of the risks presented.

- Network Infrastructure Life Cycle Refresh remains at significant risk**.** The program will use a Routed Access Local Area Network (RLAN) architecture. A business plan has been written and provided; currently awaiting approval and funding of $26.7 million.
- Email migration was completed and the last email account was migrated to DC2 September 9, 2011.
- The program is currently waiting to obtain additional life cycle funds to address this upgrade.
- The program is currently waiting to obtain additional life cycle funds to address upgrade for the IT Infrastructure within the NCR building.
- The program is currently waiting to obtain additional life cycle funds to address upgrade for end-of-life A/V and network enterprise equipment.
- IT-Operations (Service Delivery and Site Support) have initiatives to convert contractors to Permanent Full Time Employees. This will ensure that the Infrastructure has the required skilled manpower and funding to effectively and efficiently mitigate risks for day-to-day and contingency operations.

Assessment:

The FEMA Infrastructure program is responsible for the essential daily operations to the organization which are Network, Email, Help Desk, Data Center, Desktop, Site, Video, Voice, and Wireless. The program is in need of funding for critical equipment refreshes for customer support and desktop support. Its' network is at risk unless the IT infrastructure in the buildings within the NCR are upgraded. A top down analysis was completed on the Infrastructure Operations by the Engineering Branch and an estimated $26.7M is needed to continue network support and upgrade. The FEMA Infrastructure program continues to manage current resources well in order to meet the

requirements of day-to-day operations. The program will present its Business Case to the FEMA IT Governance Board to request additional funding for planned upgrades to the Infrastructure. The CIO assesses the FEMA Infrastructure program as a **Medium Risk** investment.

Score: 3