Goal 3: Strengthen Security & Disaster Preparedness

San Francisco considers the protection of our City business systems and services a primary objective. A major component of this effort is the safeguarding of confidential and sensitive data through increased security initiatives and policies. The second component of this effort is the City's work to reduce the recovery time of the City business systems and services in the event of a disruption, whether from a natural or unnatural event. San Francisco's IT Security program incorporates both components into a holistic approach to protecting City government services and providing secure, reliable technology solutions for our constituents and visitors.

STRATEGIES

- Protect sensitive and confidential data through strong security and privacy standards;
- Develop and implement a comprehensive disaster recovery plan; and
- Ensure technology and public safety communication infrastructures have robust disaster recovery capabilities.

OVERVIEW

Over the next five years, there are $21.6 million in project requests that support security and disaster preparedness as their primary goal. These projects make up 4.0 percent of the total IT project requests citywide. These 13 projects from eight departments build on the existing security efforts that are occurring citywide to further safeguard our IT infrastructure. Of the requests, there is an even distribution of infrastructure and software application projects.

The City currently has a number of completed and on-going projects that support this goal. As the City looks to the future, this Plan serves to highlight a few projects that are representative of the investments the City has recently made, and those it is poised to make in the years ahead.

STATUS OF CURRENT PROJECTS

These selected projects highlight progress to date on efforts that align with the goal of improving security and disaster preparedness.

- ✓ **Citywide Security Task Force (On-going)**
  In FY 2011-12, the City established its first IT Security Task force. This cross functional taskforce includes members from all major service areas in the City. This group is tasked with developing, training and helping the City to prepare for potential cyber incidents in order to minimize any disruptions to City services. This group increases public awareness around cyber security and the City's efforts to protect its IT infrastructure and technology-reliant services.

- ✓ **Citywide IT Security Training Program (On-going)**
  Since its inception in 2011, this security training program has provided comprehensive, straight forward training for all City employees around cyber security. This program was created to increase awareness among City staff that cyber security is a responsibility of every City employee. This program aligns the City with federal and State agencies to create greater public awareness surrounding the importance of protecting the City's IT infrastructure through education and awareness of cyber security issues.

- ✓ **Server Virtualization & Relocation (On-going)**
  The Department of Technology, in conjunction with various City departments, has been working to relocate servers that are currently located in various data closets and data centers to approved Tier 2 facilities. These Tier 2 facilities have redundant site infrastructure capacity components that will run in parallel with the City's current systems. This will be important in the event of a local disaster. Currently, the City has leased space at a data center located at 200 Paul Street. Additionally, there is a new Tier 2 facility being constructed at the Airport.

- ✓ **Citywide IT Disaster Readiness Planning – Phase 1 (Complete)**
  The Department of Technology is coordinating citywide IT disaster readiness planning and is working with the Controller's Office and other agencies to protect data and vital information in the event of an emergency. The City is finalizing an agreement with the State to lease space at its data center located in Rancho Cordova. Once this site is ready, the City will begin to replicate its critical financial systems, eMerge, and other services covered under a current SunGard contract.

MAJOR PROJECTS & INITIATIVES

Of the total requests received under this goal, 77.4 percent are identified as enhancement projects and 22.6 percent as replacements. This $21.6 million project category may seem relatively small in comparison to project requests under other goals; however, many security projects and initiatives are infrastructure related and, therefore, are included in the fourth goal of the Plan.

The following projects grouped by functional category are highlighted in this section as representative of the kinds of investments the City could make in the next five years. More detail on each of the featured projects is located in the appendix. The projects that are ultimately funded must be recommended by COIT and approved through the annual budget process by the Mayor's Office and the Board of Supervisors.

NEW / ENHANCEMENT

- Radio Security Enhancement Project
  Sponsoring Department: Technology
  Timeline: FY 2013-14 through FY 2014-15
  Project Budget: $1,500,000
  Project Summary: This project will enhance the security 9-1-1 public safety radio sites to ensure reliable radio communication. The Department of Technology maintains the City's public safety and non-public safety voice and data wireless communication systems in facilities scattered across the City and County of San Francisco. This project is to enhance the security of the areas surrounding the radio sites. As a result of continuous acts of vandalism and attempted break-ins, the Department has conducted site inventory and security assessments. This project will implement the recommendations of a consulting report that identified security weaknesses.

- Security Visibility and Intelligence

  Sponsoring Department: Technology
  Timeline: FY 2012-13 through FY 2017-18
  Project Budget: $3,459,203
  Project Summary: The Visibility and Intelligence program will cost-effectively leverage leading-edge IT Security monitoring and analytic tools to gain visibility and gather intelligence from multiple sources into a consolidated threat management system. To achieve this goal, the Department of Technology has implemented Security Event Management, Intrusion Protection, and Web Filtering technologies. In FY 2012-13, the Department is implementing other technologies that fit into its five-year technology road map for IT Security Visibility. The Department's Security staff will begin to feed these backend systems into a consolidated analytic and dash boarding platform to correlate and analyze the activity on the Department's networks. Furthermore, the Department will work with the Department of Homeland Security's MS-ISAC group to create a partnership that allows MS-ISAC to monitor the City's external perimeter and alert the Department of Technology to any threats external to our networks.

- Systems Recovery Project

  Sponsoring Department: Controller's Office and Technology
  Timeline: FY 2012-13 through FY 2013-14
  Project Budget: $2,614,709
  Project Summary: This second phase of Citywide IT Disaster Readiness Planning will establish disaster recovery capabilities for the City's integrated Human Resources, Benefits Administration, and Payroll system (eMerge), and the City's financial system (FAMIS) by creating a redundant parallel infrastructure in a data center and a back-up system in order to provide business continuity for eMerge. The City is currently negotiating with the State to lease space in its Tier 2 data center in Rancho Cordova.