Cybersecurity Policy Road Ahead

Please see the attached Cybersecurity Policy. The Policy lays the foundation for City and County of San Francisco departments (CCSF) to protect and defend information resources (infrastructure and data) against compromise.

The Cybersecurity program focuses current resources and funding toward providing services dedicated to fundamental security concerns:

1) Better inventory of hardware and software operating on the network.
2) Document the types of data we possess and systems they reside on within our perimeter and in the cloud.
3) Conduct risk assessments on systems and data stores we rely upon to provide critical services to the residents of CCSF and/or we have a legal responsibility to protect.
4) Patching, Vulnerability Scanning, Hardening Systems, Reporting Incidents and remediating them.
5) Improve knowledge level of our employees in the areas of Cybersecurity threat and risk mitigation.

The City Cybersecurity Team is implementing services and standards to help your department comply with the policy:

- Our Tenable Security Center Vulnerability Management platform will give your department a non-intrusive look into the vulnerabilities currently on your portion of the network.
- We are implementing an incident response and reporting platform to assist departments in reporting compromises and to track mitigation efforts.
- We are developing a patching solution which will significantly reduce residual risk across the City. The service is available to departments participating in City-wide AD.

We understand that there will be questions on aspects of compliance with this policy. It is the intent of the policy and program to set the course, understand where we must improve, and iteratively improve our capabilities.

Please review the policy, our staff will work with your department to implement the services described above.