SFGH, JOINT CONFERENCE COMMITTEE

DEPARTMENT OF PUBLIC HEALTH, SAN FRANCISCO GENERAL HOSPITAL - SECURITY REPORT

Basil A. Price, Director of Security
basil.price@sfdph.org
## II. HOSPITAL LEADERSHIP SUPPORT

Since 2013, the hospital leadership has supported the security program through implementation of the following:

- **Protocol for timely notification of sentinel events to SFGH and SFDPH leadership.**
- **Initiated monthly meetings with the contract security provider’s leadership, including developing a plan of correction to monitor compliance with specified performance measures.**
- **Weekly meetings with hospital leadership and the contract security provider’s account management to address identified challenges/concerns in real time.**
- **Hired a Director of Security, based out of SFGH, with responsibility for managing the security program across all divisions of the Department of Public Health (DPH), developing a DPH staff training program, establishing security policies and procedures, and overseeing and maintaining security technology and equipment such as access control systems, closed circuit TV cameras, door alarms, and panic alarms.**
- **Developed an initial scope of work and commissioned an independent external review of SFGH safety and security systems.**

### KEY RECOMMENDATIONS

- **Develop a Threat Management Team to develop safeguards that cover all persons, patients, visitors, employees, and physicians, by addressing threats and aggressive behavior at the earliest stage; defining inappropriate and unacceptable workplace behavior; and establishing an effective process for responding to, managing, and reporting acts or threats of violence or aggressive behavior.**
- **Implement a security incident reporting process, where SFGH incidents are documented in a SFGH incident management program that has activity tracking capability for trending and analysis.**
- **Revise the UO System to allow for security incident reporting of all crimes against persons and facility property, in-order to track activity for trending and analysis.**

### 2015-2016 PERFORMANCE METRICS

- **Serious Incident Crime Stats as reported by SFSD and the UO Reporting system will be monitored to determine the effectiveness of the security management plan in reducing crime at SFGH.**
- **Based on the 2015 Security Risk Assessment, the campus tunnels are the hospital’s greatest security vulnerability. Security will provide month-to-month and quarterly data to demonstrate the effectiveness of a crime prevention program to minimize or eliminate unauthorized access to the campus tunnels.**

The report will include the following, as associated with the campus tunnels:

1. **Arrests** – Number of arrests conducted each month associated with the campus tunnels.
2. **Crime Analysis** – A monthly break down of criminal incidents reported, associated with the campus tunnels.
3. **Trespass Warnings** – The number of trespass warnings issued each month associated with the campus tunnels.

The results of these countermeasures will be reported quarterly in the Security EOC Report under Significant Reporting.
### II. ELECTRONIC SECURITY SYSTEM

#### Systems and Devices
- SFGH currently uses multiple access control systems, which are controlled by the Facilities Department. The system appears to be functional and most card readers are in working order. However, there are no system inspection and maintenance reports to ensure functionality. The systems reporting function does not easily identify which components are working properly, which allows for the potential of device failures without proper follow-through.

#### System Installation
- In collaboration with SFGH Rebuild (New Hospital, Building 25), a security system upgrade (Lenel OnGuard) is underway. DPH IT has assigned a Project Manager to oversee the project, who will establish the work-plan and schedule.
- Additionally, DPH has committed to a two year plan for equipment and technology enhancements – cameras, security hardware and networking for Building 5.

#### System Operational Issues
- Video surveillance is not installed in many security sensitive areas, as required by healthcare security industry standards, for the purpose of recording and digital archiving.
- Even with the completion of Lenel, there are differing types of security system design applications that have been installed over the years including push button locks, Panic Buttons, and dummy cameras, creating non-uniform security system practices.
- Video surveillance is not installed in many security sensitive areas, as required by healthcare security industry standards, for the purpose of recording and digital archiving.

#### Electronic Security System Recommendations
- Update all building security systems and devices to current healthcare security industry standards.
- Develop a security-by-design process where the Director of Security is involved in the security systems designs associated with remodel of existing buildings and construction of new facilities.
- The existing access control, alarm, and CCTV systems should be replaced with a new Lenel security management system on a phased approach in accordance with budget availability and identified useful lifespan of the existing systems. - Completed
- Security systems should be integrated between all DPH Hospitals, Clinics, Behavioral Health Facilities, and Administration Buildings to improve system management, enhance customer service, and provide operational efficiencies.
- All systems should utilize DPH local and wide-area networks as communications paths, thus reducing infrastructure costs while improving operational features and efficiencies. Provisions should be made to support future system expansions, including connection to all of the off-site buildings for local and remote monitoring and reporting.
- Develop a comprehensive program to manage the security electronic systems, including monthly testing of all systems, budget planning, administration, service, maintenance, and repair of security equipment, including periodic software upgrades.
- Develop a phased approach to add doors, gates, and/or enclosed counters to inner lobby access areas and reception desks that are currently open to provide securable entry points for employees only.

#### 2015-2016 PERFORMANCE METRICS
- The functionality of the electronic security system will be monitored in the 2015-2016 EOC Security Report. The monthly target is for 100% of the system to be inspected, and result in 98% functionality.
- The hospital’s response to Code Green will be monitored in the 2015-2016 EOC Security Report. On at least a quarterly basis, the hospital will conduct a Code Green drill to determine the effectiveness of “At Risk” patient response. The hospital will be measured on its ability to prevent/return an “At Risk” patient:
  - Prevent/Return-rate Threshold – 90%
  - Prevent/Return-rate Target – 98%
  - Prevent/Return-rate Stretch – 100%
- The hospital will also be measured on its ability to respond to a hospital-wide activation and search:
  - Response-rate Threshold – 80%
  - Response-rate Target – 90%
  - Response-rate Stretch – 100%
- Infant Abduction Response drills will be monitored to...
SECURITY ASSESSMENT KEY FINDINGS

• The medical office buildings do not comply with healthcare security system standards. There are inactive intruder alarm systems with motion detection installed that are no longer being monitored.

• Emergency Security Phones are installed on each level of the parking garage that are not operational.

Access Control

• Exterior doors throughout the hospital campus are easily defeated, unsecured, and are not currently viewed by exterior cameras. Many stairwell doors can be opened from the exterior of the buildings, and several allow unrestricted access into patientcare areas.

• The lack of after-hour access control devices in the ED waiting area, and public elevators allows for unauthorized access to the hospital, security sensitive, and administrative areas, which is a daily occurrence.

• The hospital’s loading dock does not restrict access. Access to the hospital, Materials Management storeroom, and Nutritional Services can be accomplished through the loading dock elevator, which does not have elevator access control. Exterior doors are easily compromised, and need replacing.

• Medical Office Buildings (Building 80 and 9, 30, and 40) are not equipped with card readers. The San Francisco Sheriff Department’s unlock schedule opens the clinics 3 hours prior to the start of business, to accommodate early arriving employees, which allows unauthorized access to the clinics, which is a daily occurrence.

KEY RECOMMENDATIONS

• Increase annual maintenance and service budget to a level that is sufficient to repair and maintain all dysfunctional devices and systems.

• All buildings should incorporate access control, alarm monitoring, and closed circuit television.

• All future cameras, card readers, and alarms should be connected to the new systems.

• Remove/replace all existing equipment that is non-functional.

• All alarms are to be tested at least monthly, and reported to the Environment of Care Committee quarterly, include action plans to addressing malfunctioned equipment.

• All cameras should be “called up” and tested for proper view of intended area as well as quality of picture. Inadequate images should be identified and trouble-shooting should be conducted. Any dysfunctional cameras should be replaced immediately.

• All emergency phones should be equipped with camera call up availability at the responding SOC.

• All perimeter doors should be alarmed and monitored by the security system.

• All emergency exit doors and/or stairwell doors that can be opened from the exterior of the building should be locked from the outside and equipped with local internally mounted sounders.

• All exterior stairwell exit doors should be equipped with cameras which monitor the doors with automatic camera call-up if the local sounder is activated.

• All interior doors to employee areas should be closed and secured.

2015-2016 PERFORMANCE METRICS

• Employee Security Awareness will be monitored to determine employee’s security knowledge.

During EOC rounds, hospital staff be tested on 10 security awareness questions. [Sample size: 300 employees per quarter]

Target 90% or higher (Knowledgeable rating) on the total questions answered correctly by the total employees surveyed.

The results of the above countermeasures will be reported quarterly in the Security EOC Report under Significant Reporting.
<table>
<thead>
<tr>
<th>SECURITY ASSESSMENT KEY FINDINGS</th>
<th>KEY RECOMMENDATIONS</th>
<th>2015-2016 PERFORMANCE METRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The rear entry doors to the Medical Office Buildings are often propped open, and access into the clinics can be accomplished through window ledges where windows are often left unlocked/open.</td>
<td>• Push button locks should be standardized and codes changed regularly.</td>
<td></td>
</tr>
<tr>
<td>• The hospital’s ground floor is accessible to the public. Several exterior doors, windows, and air-vents are compromised to gain access. During the facility walk-through, there was evidence of habitation in the hospital ground floor.</td>
<td>• All Help Buttons should be consistent in design and application. Testing of working help buttons should be completed at least monthly.</td>
<td></td>
</tr>
<tr>
<td>• Several buildings have no electronic security systems whatsoever. Others have installed monitoring equipment that is inoperable. Alarm monitoring is inconsistent in its application with different system manufactures, including the pharmacies, and buildings where there is no access control system installed.</td>
<td>• Improve the current communications system, including help-buttons so that is capable of radio and telephone communications between all DPH facilities.</td>
<td></td>
</tr>
<tr>
<td>• Most of the cash handling areas are not equipped with safes, and cash drawers, and cash transactions are not monitored by an alarm system or video surveillance.</td>
<td>• Improve lighting at Building 3, 80, 90, 100, and increase evening and night security patrols.</td>
<td></td>
</tr>
<tr>
<td>• Production of ID badges is the function of the Human Resources Department, and the programming of badges is the function of the Facilities Department. There is no collaboration or communication between the departments, resulting in terminated employees with active badges in the proximity card system.</td>
<td>• All ID Badge Services, including production, programming, and producing badge audit-history reports to be performed by the Security Services Department, in the SOC.</td>
<td></td>
</tr>
</tbody>
</table>

**Alarm Systems**

**ID Badge System**

**Hospital Employee Security Awareness Recommendations**

- During the security portion of the orientation, employees should receive information about the following:
  1. A description of the Security department
  2. Security services provided
  3. Prudent security practices
  4. Violence in the Workplace Policy
  5. ID Policy
  6. Emergency procedures to be followed during security incidents
  7. Processes to minimize security risks in sensitive areas
  8. Reporting a security incidents or suspicious activity
  9. Security command structure
  10. Facility response to infant and pediatric abductions/drills
  11. Facility response to “At Risk” patient incidents/drills
<table>
<thead>
<tr>
<th>SECURITY ASSESSMENT KEY FINDINGS</th>
<th>KEY RECOMMENDATIONS</th>
<th>2015-2016 PERFORMANCE METRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The CCTV system technology is outdated and needs replacing. The camera coverage is also inadequate. The CCTV System cannot fully contribute to customer service objectives due to inherent limitations of information provided.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The SFGH Security Operations Center is equipped with an audio recorder that records all SOC operator phone communication. The system has exceeded its product life cycle, is dysfunctional, and needs replacement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support and Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Contract technicians are equipped with the proper system knowledge for trouble-shooting; however, proprietary oversight to manage the system vendor is limited.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hospital Employee Security Awareness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The security awareness of the hospital staff is marginal. Historically, the hospital has solely depended upon SFSD to develop, implement, and manage the security operation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The existing security awareness program for employees consists of monthly SFSD security alerts, and periodic SFSD community policing events.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The security information in New Employee Orientation Program is limited, and should be presented by a representative of the Security Department to ensure that all employees will receive basic information related to the Security Department and its Security Management Plan.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. Security locations and phone numbers
### III. SECURITY STAFFING

The San Francisco Sheriff's Department (SFSD) is the contract security provider. Formal Security Operations Center (SOC) staff, systems training for access control, alarm response, and CCTV systems do not currently exist. As a result, only limited employees have SOC system’s knowledge, while others adopted a "learn as you go" procedure in using the systems.

- All security incident reports are entered into a SFSD database, which SFGH has no access. Copies of incident reports require a written request to the Office of the Sheriff. In the incident is under criminal investigation, SFGH may not be provided a copy.

- Security incident data for trending, risk mitigation, and performance metrics, which is reported to SFGH’s Executive and Environment of Care Committees, cannot be validated for accuracy. The data is a combination of crime stats provided by SFSD, and Unusual Occurrence Reports (UO) provided by Risk Management. The UO data is not properly categorized to determine incident frequency.

- The SFSD are responsive to security emergencies; however, hospital staff have expressed concern regarding security visibility, cooperation during state survey audits, knowledge regarding Joint Commission, state and federal regulations, and Crisis Response Training.

<table>
<thead>
<tr>
<th>SECURITY ASSESSMENT KEY FINDINGS</th>
<th>KEY RECOMMENDATIONS</th>
<th>2015-2016 PERFORMANCE METRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SFSD performance as it relates to the elements of the MOU between DPH and SFSD will be monitored in the 2015-2016 EOC Security Report. SFSD is expected to maintain scores in the 3-5 range. A score of 1 to 2 indicates that a problem or issue exists that needs to be immediately addressed. A score of 0 indicates a substantive problem or issue that requires immediate correction or resolution. Each category receives points as achieved per line item. A final numerical score is calculated at the end of the report.</td>
<td>Hire a full-time proprietary Security Systems Administrator with overall responsibility for the oversight of the implementation of hospital’s security systems and technology integration, including responsibility for the following: 1. Consulting 2. Assisting and tracking master system architecture for DPH facilities in order to achieve logical collective implementation. 3. Provide Contractor/Local support for programming or bringing systems into operations. 4. Maintain Security System Server Software Licensing. 5. Provide liaison for Local Security and Systems designers and manufactures. 6. Ensure design/construction projects are consistent with industry best practices as well as industry design standards, scope, schedule and budgets. 7. Reinforces the direction of hospital facility systems, and develops relationships with IT, Facilities, the SFSD, and Contractors in order to maintain system efficiencies. 8. Conducts monthly inspections of the hospital security system to ensure functionality 9. Implementing the security operation center’s program, including producing audit reports, and forensic evidence during investigations.</td>
<td>Use of Force will be monitored to determine track activity for trending and analysis. On a monthly basis, data to track SFSD incidents at SFGH that involve the use of force will be broken down as follows: 1. Type of Force 2. Number of incidents. 3. Demographics The results of the above countermeasures will be reported quarterly in the Security EOC Report under Significant Reporting.</td>
</tr>
<tr>
<td>SECURITY ASSESSMENT KEY FINDINGS</td>
<td>KEY RECOMMENDATIONS</td>
<td>2015-2016 PERFORMANCE METRICS</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>• Hire a full-time proprietary Security Administrative Specialist with responsibility for administrative functions including:</td>
<td></td>
<td>EOC Security Report.</td>
</tr>
<tr>
<td>1. ID Badge producing, programing, and producing badge audit-history reports.</td>
<td></td>
<td>On a monthly basis, a sample size of 100 customers, consisting of patients, visitors, employees, and physicians that had a recent contact with Security, will be surveyed on their experience.</td>
</tr>
<tr>
<td>2. Incident Report processing, record keeping, and filing, reception, compilation of data for reports, and tracking statistics</td>
<td></td>
<td>The Security Department will be measured on its ability to achieve the following:</td>
</tr>
<tr>
<td>3. Data entry</td>
<td></td>
<td>Threshold - 80% Somewhat Satisfied</td>
</tr>
<tr>
<td>4. Other miscellaneous and/or ancillary tasks as assigned by the Director of Security</td>
<td></td>
<td>Target - 90% Satisfied</td>
</tr>
<tr>
<td>• Ensure that baseline SFSD security staffing levels assigned to SFGH can accommodate account management, administrative level supervision, basic security patrolling requirements of the hospital’s interior, campus exterior, and provide for mutual back up.</td>
<td></td>
<td>Stretch – 98% Very Satisfied</td>
</tr>
<tr>
<td>• Additional security staffing considerations to address the following:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### SECURITY ASSESSMENT KEY FINDINGS

<table>
<thead>
<tr>
<th>NEW HOSPITAL (BUILDING 25)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Electronic Security Systems – ID Badge Programming</strong></td>
</tr>
<tr>
<td>• Data Integration – Currently attempts to integrate existing data has resulted in corrupt data, which creates a barrier for badge programming.</td>
</tr>
<tr>
<td>• Database Touchpoints – Once the database was transferred existing touchpoints to the previous database were lost, which will impact regulatory training requirements.</td>
</tr>
<tr>
<td>• Terminated Staff Protocols – There is no method in place to remove a terminated employee from the database. Thus the existing database is littered with entries that need to be deactivated.</td>
</tr>
</tbody>
</table>

**Electronic Security Systems – Commissioning and Acceptance**

The following security system components have yet to be completely installed in Building 25:

• Installation of all video surveillance cameras, including proper aiming, map locations of cameras, event programming, and viewing capability in the Security Operation Center.
• Activation of badge readers
• HUGS installation
• AeroScout Installation

### KEY RECOMMENDATIONS

An ID Badge Task Force, which includes representatives of Human Resources, Information Systems, Facilities, Security, and Patient Safety was developed to discuss remedies, and develop a plan that addresses the badge programming concerns.

• According to Facilities, the data integration and database touchpoint issues are 90% completed.
• The removal of corrupt data, and a DPH-wide off-boarding process is still outstanding.

Conduct regular meetings with the security system vendor to receive installation and testing status updates.

• The first meeting was held on 9/10/2015. The vendor reported that 98% of the video surveillance cameras were installed. A meeting to address proper system functionality is scheduled for 9/9/16/2015.

### 2015-2016 PERFORMANCE METRICS

Weekly meetings with the President and CEO of Black Bear Security Inc. to
SECURITY ASSESSMENT KEY FINDINGS | KEY RECOMMENDATIONS | 2015-2016 PERFORMANCE METRICS
--- | --- | ---
Hospital Transition Security
- There have been five security breaches within six weeks. Each involving unauthorized access into the building, and three incidents involving the removing of hospital property. | - On August 27, 2015, Black Bear Security Inc. submitted an action plan to improve security, which includes securing and alarming all perimeter doors. | |